מעבדת תקשורת

Table of Contents

1.The Goals 2
2.Preparations 2

3. Introduction to Wireshark 2
4. TOS – Type of service at the 3rd layer 5
5. Live capture 6
6. Call flow analysis 7
7. Wireshark quiz 8

 All rights reserved

1. The Goals

- The student will be able to use Wireshark for real-time captures
- To analyze Ethernet (MAC and LLC), IP , UDP and TCP Layers
- To present the Call flow
- To record media and replay it
- To analyze network impairments by using Wireshark such as Jitter and Packet-loss

2. Preparations

1. Get your Laptop/Desktop connected to the campus LAN/WLAN
2. Ping to your own IP address (Start-Run-CMD)
3. Run ipconfig to show your own IP address
4. Ping to our own IP Address (ping _____) and verify that an echo is received

3. Introduction to Wireshark

- Free and open-source packet and protocol analyzer
  http://www.wireshark.org
  https://www.wireshark.org/download.html version 1.10.13.
- Available for various of operating systems (e.g. Linux, Windows, OS X, Unix, etc.)
- Wireshark provides statistics and analyzing tools
- Allows filtering for easy analysis (e.g. view network messages and filter out internal server messages)
- Allows examining & playing RTP data
- Contains graphical tools to make debugging easier
- Open source software

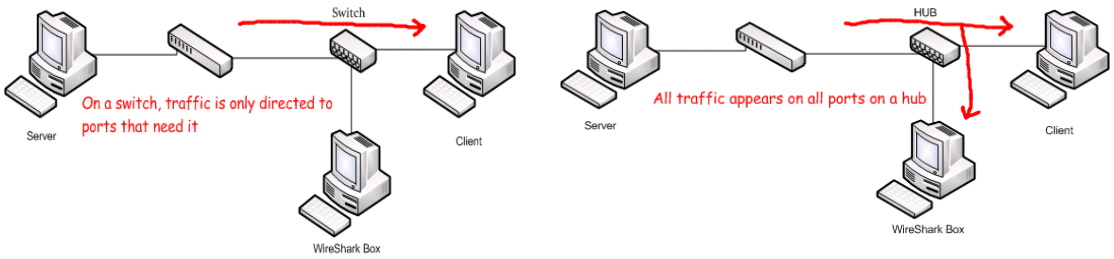
Some TIPs

- In order to capture (sniff) the right data, it is important to understand the traffic flow of the network

 All rights reserved

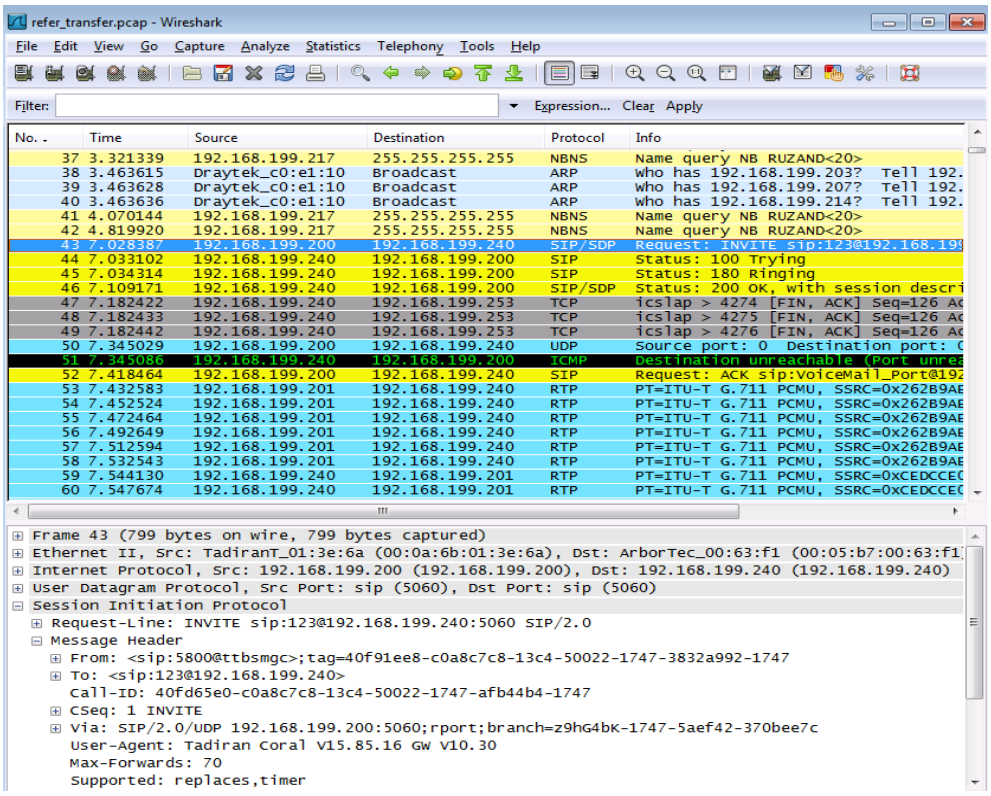
- Data captured over the IP Network
  - Signaling packets
  - RTP (Media): P2P between end points or via Proxy

Differences when going through network Hubs and Switches



- When using a computer for sniffing, it is recommended to disable your local FW.

Wireshark GUI

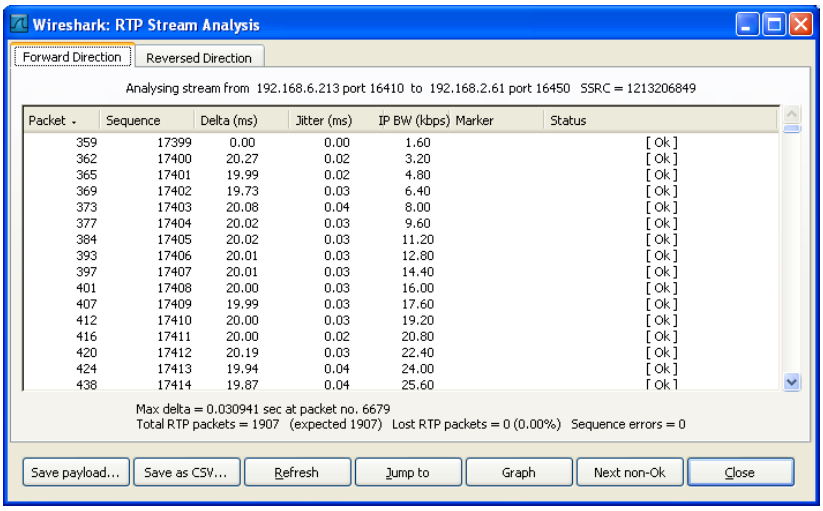


Wireshark Capabilities: Audio

- When analyzing RTP streams the media can be saved to file
- When verifying audio problems the saved media file can be played back using media player

 All rights reserved

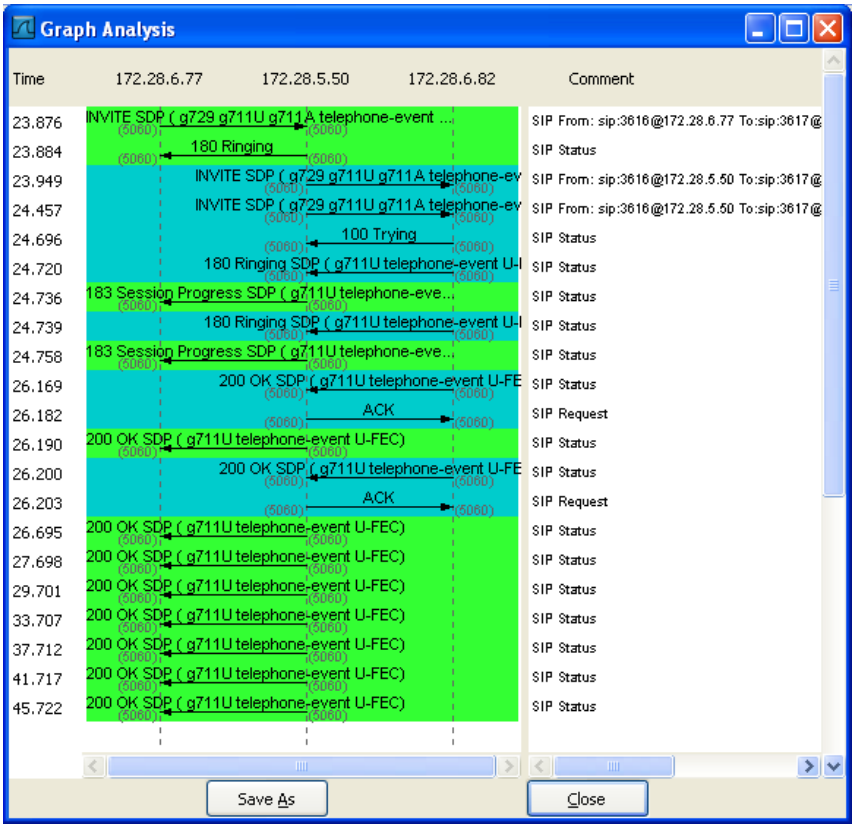
- Analyzing a stream
  - In Wireshark use: ***Statistics->RTP->show all streams***
  - Select the stream and press the Analyze button
  - In the new opened window press Save Payload…



Wireshark Capabilities: Sequence Diagram

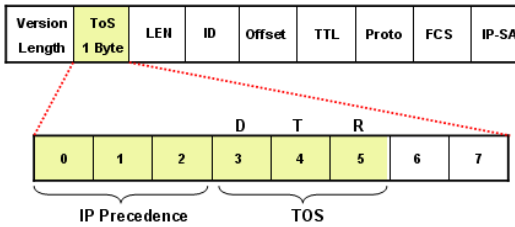
- A sequence diagram represents the messages between entities in the system during a call
- Viewing a sequence diagram:
  - Open: ***Statistics->VOIP calls***
  - Select the participants of the call
  - Select the Graph button
- When the graph is opened:
  - Clicking the diagram will display the specific packet
  - Clicking a stream will mark it and will display the first packet

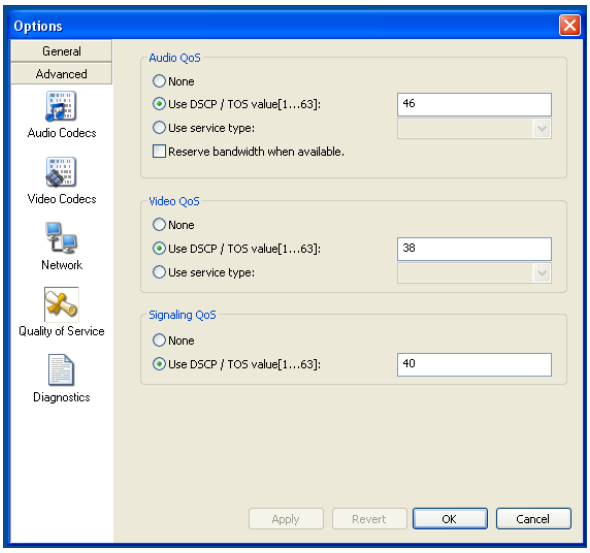
 All rights reserved



4. TOS – Type of service at the 3rd layer

a. QoS Setting





- Precedence
  - 111 = Network

 All rights reserved

- 110 = Internetwork
- 101 = Critic (mainly used for Voice RTP)
- 100 = Flash Override
- 011 = Flash (mainly used for Voice Signaling or for Video)
- 001 = Immediate
- 000 = Routing (best effort)

- TOS
  - D = Request low delay
  - T = Request high throughput
  - R = Request high reliability

5. Live capture

1. Activate the **Wireshark** (setup the proper interface and define in promiscuous mode)
2. Define the Wireshark filter for analyzing the traffic to your computer : ip.addr=={our address} and MAC

3. Lab report
   a. What are the source and destination MAC addresses?
   b. Identify the parameters in the LEN, Type and FCS fields.
   c. Analyze and Identify the manufacturer and the MAC address type (Unicast, Multicast or Broadcast)
   d. Analyze and indicate the IP Address Class and type (Private or Global)?
   e. Indicate the parameters of the IP Header as follow:
      i. IP version
      ii. Header length
      iii. Type of Service (RFC 791)
      Or
      DS (Differentiated Services) and ECN (Explicit Congestion Notification) - RFC 2474

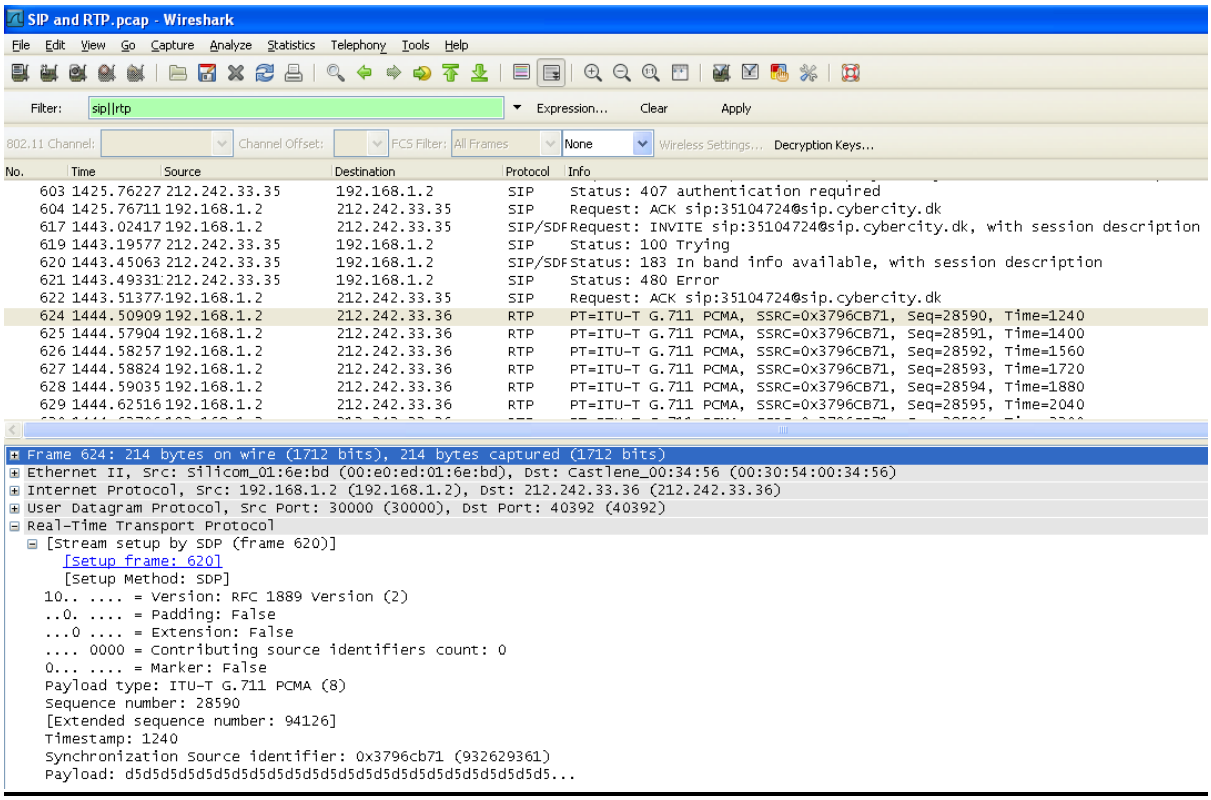
      iv. Total length
      v. Identification

 All rights reserved

vi. Flags
vii. Fragmentation offset
viii. Time To Live (TTL)
ix. Protocol
x. Header checksum
xi. Source address
xii. Destination address
xiii. Options

6. Call flow analysis

1. Open the .cap file by using the Wireshark and analyze the audio (RTP protocol)
2. Present the network impairments (Jitter and Packet-Loss)
3. Replay the Audio (non compressed using G.711 coder)
4. Analyze the IP layer (source and destination IP addresses, and other parameters including the flags (DF and MF)



 All rights reserved

7. Wireshark quiz

1. Your network consists of managed switch and multiple hosts that are connected to this switch. In case that you need to monitor the overall traffic flowing through this switch, where will you connect the Wireshark to fulfill this mission?
2. In case you need to capture traffic from specific IP Address: 192.168.0.1, what should be defined in the Wireshark filter?
3. Please define the proper filter that will capture traffic from the 4th Layer: UDP or from TCP and only from IP Address 192.168.0.32
4. As part of your tasks, you need to present the call flow. Please describe what are the required actions for that?
5. If you need to capture and replay audio based capture (running over RTP- Real Time Transport Protocol) from/to your Softphone, what will be the filter to be defined and specify the actions to fulfill this task.
6. As part of the troubleshooting process you need to analyze the network impairments such as Jitter and Packet Loss. Please specify the required actions in order to present these parameters measured by the Wireshark.

 All rights reserved