Lab Work 06 Report:

Wireshark. Network Traffic Capture and Analyze.

|  |  |  |
| --- | --- | --- |
| **Student Name Surname:** | **Student ID:** | **Date:** |
|  |  | DD.MM.YYYY |

Use **smallFlows.pcap** from the archive <http://net.academy.lv/soft/pcap.zip>

|  |  |  |
| --- | --- | --- |
| 3.1. Capture File Properties  Fill in the table. For initial data use the **Statistics/Capture File Properties**. | | |
| **Nr** | **Parameters** | **Value** |
| 1 | Time of capture, min |  |
| 2 | Packets |  |
| 3 | Bytes, МiB |  |
| 4 | Average packet size, B |  |
| 5 | Average packets per seconds, pps |  |
| 6 | Average bytes per seconds, B/s |  |
| 7. Determine the relative network load L (in%) for the control period T by formula: L = (Traffic [Mbits] / T [sec]) / (Bandwidth [Mbits/sec]), if Bandwidth=100 Mbits/sec | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 3.2. Ethernet Traffic Distribution by Protocols  Fill in the table. For initial data use the **Statistics/Protocol Hierarchy**. | | | |
| **Nr** | **Protocol** | **Traffic, МiB** | **Traffic, %** |
| 1 | IPv6 |  |  |
| 2 | IPv4 |  |  |
| 3 | --UDP |  |  |
| 4 | --TCP |  |  |
| 5 | --ICMP |  |  |
| 6 | ARP |  |  |
| 7 | 802.1X |  |  |
|  | **SUMM** |  |  |
| 8. What is the ratio of the numbers of application (http, mail, ftp, …) to numbers of service (dns, icmp, arp, …) protocols?  Anr / Snr = Your Ansver | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3.3. Ethernet Traffic Distribution by Nodes  Fill in the table (for the 5 most active network nodes by Bytes). For initial data use the **Statistics/Endpoints/Ethernet**. | | | | | | | | |
| **Nr** | **MAC-address** | **IP- address** | **Traffic** | | | | | |
| **Rx input** | | **Tx output** | | **Overall** | |
| **МiB** | **%** | **МiB** | **%** | **МiB** | **%** |
| 1. |  |  |  |  |  |  |  |  |
| 2. |  |  |  |  |  |  |  |  |
| 3. |  |  |  |  |  |  |  |  |
| 4. |  |  |  |  |  |  |  |  |
| 5. |  |  |  |  |  |  |  |  |
|  | **SUM** | |  |  |  |  |  |  |
| 6. Which IP nodes are the most loaded, given the direction of traffic?  Incoming –  Outgoing –  Overall – | | | | | | | | |

|  |  |  |
| --- | --- | --- |
| 3.4. Display Filters  Fill in the table. Write and test in Wireshark 5 simple search filters (Display Filters) using AND, OR, NO to display packets from (to) a specific node generated by ICMP, DNS, ARP requests (responses) when accessing any server of your choice. | | |
| **Nr** | **Display Filter** | **Description** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 3.5. Network Problem Analyze.  Analyze the 5 note/warning/error problems existing on the network. Find and read information about network problems on the Internet.  For initial data use the **Analyze/Expert Information**. | | | |
| **Nr** | **Expert Information** | **Severity** | **Your Short Description (Problem Analyse)** |
| 1 |  | Warning |  |
| 2 |  | Note |  |
| 3 |  | Error |  |
| 4 |  |  |  |
| 5 |  |  |  |

|  |
| --- |
| 3.6. Network Problem Analyze.  **Tasks.**  You need to find and export the N-th (by size) JPEG file, where N is your number in the class list (the 1st by number takes the largest file, the 2nd takes the next, etc.).  Determine the starting packet number, source IP, destination IP, Jpeg file size.  Paste this image into your Report  **Instruction.**  For initial data use **File / Export Object / HTTP ...** / sort information by file size (large to small) / find the N-th file content-jpeg / read interesting information / save this file.  **Answer.**  1. Your variant Nr: ??  2. Starting packet number:  3. Source IP:  4. Destination IP, jpeg file size:  5. Jpeg file size:  6. Picture  Jpeg-file Picture |