Assignment 1 Part 2

1 Network Traffic Analysis

1.1 Data Collection

We collected network traffic data from a series of 2-person, 1-minute Microsoft Teams calls using **Wireshark** as our primary network protocol analyzer. To ensure the accuracy and relevance of our captured data, we implemented a controlled environment by closing all applications except Microsoft Teams and Wireshark. The traffic capture was performed on the WiFi router's WLAN interface, allowing us to record all pertinent network packets. We conducted multiple 1-minute calls, systematically capturing data for all four combinations of audio and video settings: audio on/video on, audio on/video off, audio off/video on, and audio off/video off. This comprehensive approach enabled us to gather diverse data representing various call configurations. Moreover, both of us recorded it separately on two computers, which led to a total of 8 data sets for analysis.

1.2 Protocol Analysis

1.2.1 Protocols and Packet Distribution

Network Layer : We observed packets from three protocols in the network layer. These have been listed below. Some of them may have been due to some background traffic.

- **IP (Internet Protocol):** The fundamental protocol for routing and addressing packets across the internet.
- **IPv6 (Internet Protocol version 6):** The next generation of IP, designed to replace IPv4 with a much larger address space.
- **ARP (Address Resolution Protocol):** A protocol to map IP addresses to MAC addresses in a local network.

Protocol	Number of Packets	Percentage of Total Packets
IP	65649	99.9 %
IPv6	56	0.08 %
ARP	10	0.015 %
Total	65715	100 %

Table 1: Distribution of Protocols in Network Layer

Transport Layer : We observed packets from four protocols in the transport layer. These protocols are in the table below.

- **UDP (User Datagram Protocol):** A connectionless transport protocol for sending messages with minimal overhead.
- **TCP (Transmission Control Protocol):** A connection-oriented protocol ensuring reliable data delivery.
- **ICMP (Internet Control Message Protocol):** Used to send error messages and operational information about IP network conditions.
- **ICMPv6:** The implementation of ICMP for IPv6, providing error reporting, diagnostics & neighbor discovery.

Protocol	Number of Packets	Percentage of Total Packets
UDP	64393	98.0 %
TCP	1303	2.0 %
ICMP	4	0.006 %
ICMPv6	9	0.013 %
No Transport layer header	10	0.015 %
Total	65715	100 %

Table 2: Distribution of Protocols in Network Layer

This shows that most communication in Microsoft team calls occurs over the UDP protocol, and some handshakes and data transfers occur on the TCP protocol. UDP (User Datagram Protocol) dominates Teams calls because it prioritizes speed over reliability, crucial for real-time audio and video streaming. Its lightweight nature allows for quick packet transmission, which is essential in maintaining low latency during calls. UDP (User Datagram Protocol) prioritizes speed over reliability through its streamlined, connectionless approach to data transmission. UDP doesn't require a pre-established connection before sending data, eliminating the time-consuming handshake process that TCP uses. UDP doesn't wait for received packet acknowledgments, allowing it to continue sending data without pausing.UDP doesn't attempt to resend it, avoiding delays but potentially losing some data.

On the other hand, TCP (Transmission Control Protocol) does handshakes and some data transfers where reliability and ordered delivery are more important than speed, such as chat messages, file transfers, or establishing the initial connection.

UDP protocols are more suitable for video and audio calls due to their tolerance for packet loss. Maintaining a smooth, continuous data flow in real-time communication is often more important than ensuring every packet arrives. If some packets get lost during transmission, UDP sends new data without attempting to recover the lost information. This approach is acceptable in video and audio calls as Human perception can often fill in small gaps in audio or video. Momentary glitches are less disruptive than the delays caused by re-transmitting lost packets. The continuous stream of new data quickly supersedes any lost information. This "best-effort" delivery model of UDP allows for lower latency and more fluid communication, which is crucial for the natural feel of video and audio calls, even at the cost of occasional minor quality issues.

Application Layer : We observed packets from various protocols at the Application layer level. These are listed in the table below.

- **RTP (Real-time Transport Protocol):** Used for delivering audio and video over IP networks in real-time applications like VoIP.
- **RTCP (RTP Control Protocol):** Provides out-of-band statistics and control information for RTP flows.
- **Skype:** A proprietary protocol used by Skype for voice calls, video chats, and instant messaging.
- **STUN (Session Traversal Utilities for NAT):** Allows devices behind NAT to discover their public IP address and port mappings.
- **TLS (Transport Layer Security):** Cryptographic protocol designed to provide communications security over a computer network.
- **Data:** Generic term for various data transfer protocols not explicitly identified.
- **DNS (Domain Name System):** Translates human-readable domain names to IP addresses.
- **MDNS (Multicast DNS):** Resolves hostnames to IP addresses within small networks without a local name server.

- **SSDP (Simple Service Discovery Protocol):** Protocol for advertisement and discovery of network services and presence information.
- **DVB-S2 Baseband:** Digital Video Broadcasting - Satellite - Second Generation, a standard for satellite television broadcasting.

Protocol	Number of Packets	Percentage of Total Packets
RTP	17744	27.0 %
RTCP	91	0.1 %
STUN	40	0.07 %
TLS	662	1.0 %
Skype	28633	43.6 %
Data	17606	26.8 %
DVB-S2 Baseband	167	0.3 %
DNS	50	0.1 %
MDNS	53	0.1 %
SSDP	5	0.007 %
No Application Level Header	664	1.0 %
Total	65715	100 %

Table 3: Distribution of Protocols in Network Layer

The Skype protocol accounts for 43.6 % of the traffic, while RTP accounts for 27.0 %. The packet distribution shows significant communication between audio/video packets over these two protocols. We don't see any communication on RTP protocol with other applications closed in the audio-off video-off file. But we do see Skype protocol, which means that there is some background traffic that is using Skype protocol. The analysis also shows a similar result for the files recorded on my partner's laptop. But when we analyzed the files for my partner and me on his wire shark, the result showed stun and RTP protocol for both files. So, there are some differences between the Wireshark versions we are using. My wireshark version is Version 4.2.6 (v4.2.6-0-g2acd1a854bab), and libpcap is 1.10.1.

1.2.2 Connection Analysis

We didn't observe a direct connection between two hosts during a Microsoft Teams call, and this may be likely due to how Teams handles network connections. There was a common endpoint with which both my partner's devices communicated. The source IP for my device is 192.168.18.144, which connects to the router with IP 192.168.18.1; my router communicated to endpoint 52.115.237.150, a Microsoft server in the US. Similarly, my partner's IP was 192.168.31.198, talking to the same end-point 52.115.237.150.

Thus, a Microsoft server acted as common ground for communication. We considered how Microsoft would do this; here's a thought process.

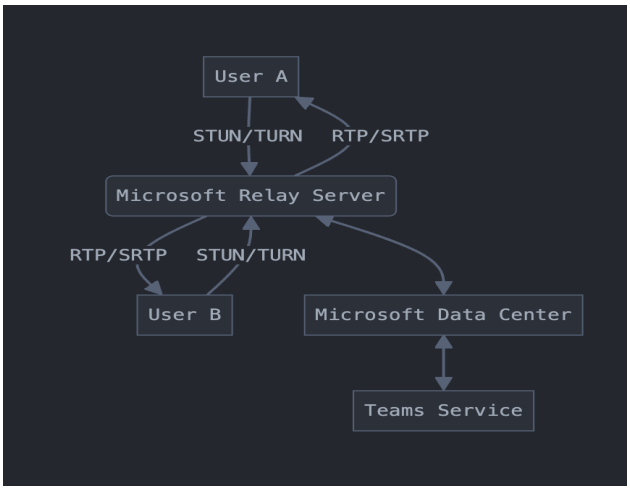

Figure 1: Microsoft Teams Connection Process

Figure 1 illustrates the connection process in Microsoft Teams calls. The diagram shows how User A and User B connect to the Microsoft Relay Server using STUN/TURN protocols and how the audio/video data (RTP/SRTP) is relayed through this server. It also depicts the connection between the Relay Server, the Microsoft Data Center, and the Teams Service.

- **User A and User B:** The end users participating in the Teams call.
- **Microsoft Relay Server:** Facilitates the connection between users, especially when direct peer-to-peer communication is impossible.
- **Microsoft Data Center:** Houses the infrastructure that supports the Teams service.
- **Teams Service:** The core service manages calls, meetings, and other Teams functionalities.

Process : Users A and B initiate connections to the Microsoft Relay Server using STUN/TURN protocols. These protocols help overcome NAT and firewall restrictions. Audio and video streams (RTP/SRTP packets) are sent from each user to the Microsoft Relay Server. The Microsoft Relay Server communicates with the Microsoft Data Center. The Data Center houses the Teams Service, which manages the overall call process, user authentication, and other service-related functions.

1.2.3 Audio and Video Packet Analysis

Protocol	Number of Packets	Percentage of Total Packets
Audio	65649	99.9 %
Video	56	0.08 %
Total	65715	100 %

Table 4: Distribution of Protocols in Network Layer

Logic : We have used the Wireshark display filter to capture specific types of RTP (Real-time Transport Protocol) packets for audio and video streams. We used the following filters:

Audio : `(rtp.p_type == 120 or rtp.p_type == 108)`
Video : `(rtp.p_type == 122 or rtp.p_type == 123 or rtp.p_type == 124 or rtp.p_type == 125)`

For audio, it filters RTP packets with payload types 120 or 108. It captures RTP packets with payload types 122, 123, 124, or 125 for video. The filter uses logical operators to combine these conditions: 'or' to allow multiple payload types for each media type.

The table below presents the payload types and their common usage in Microsoft Teams:

Payload Type	Common Usage
108	G.722 audio codec
120	SILK audio codec (older versions of Skype/Teams)
122	H.264 video codec (primary video codec in Teams)
123	H.264 video codec (alternative configuration)
124	H.264 video codec (another variation)
125	H.264 video codec (high quality/resolution)

Considerations : It's crucial to note that the exact usage of these payload types can vary depending on the specific version of Teams and the call configuration. I have used Version 24193.1707.3028.4282 (24193.1707.3028.4282) of Microsoft Teams.
Packet Distribution : We observed a significant disparity between video and audio packet volume. Specifically, we captured 15172 video packets, constituting 23.1% of the total 65715 packets. In contrast, audio packets were considerably less prevalent, with only 2572 packets detected, accounting for a mere 3.9% of the overall traffic.

1.2.4 Analysis of Wireshark I/O Graphs: Audio and Video Bandwidth Utilization

We used the Wireshark I/O graph to plot the bandwidth utilization patterns of audio and video traffic. The plot is shown below.

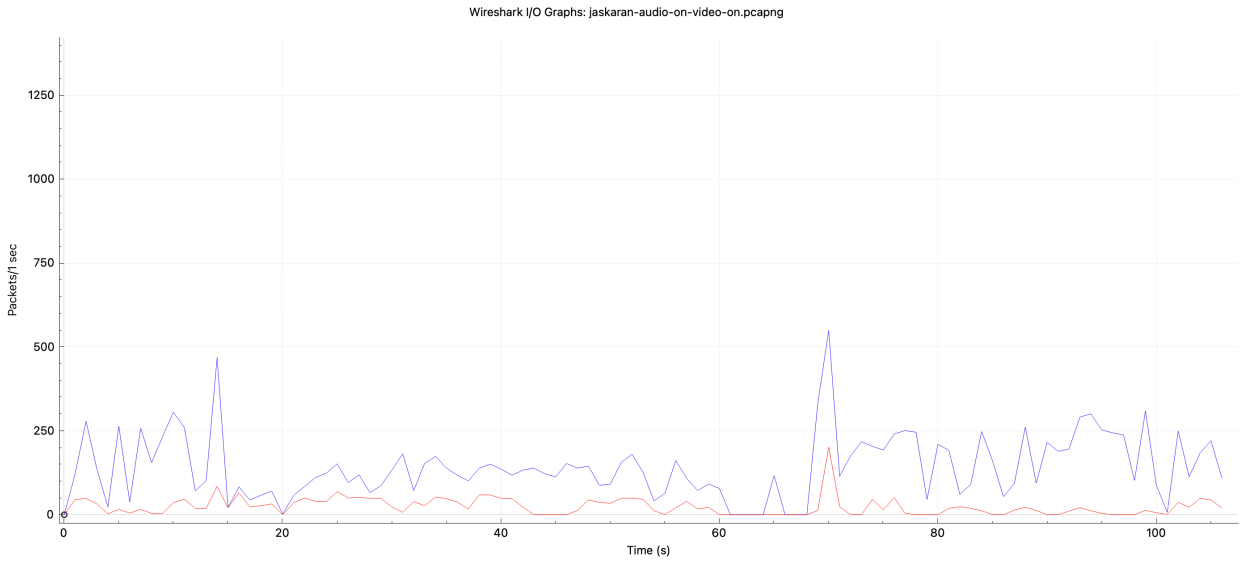

Figure 2: Wireshark I/O Graphs: Audio and Video Bandwidth Utilization

- The x-axis represents time in seconds, while the y-axis shows the packet rate in packets per second.
- The graph displays two distinct lines representing audio (red line) and video (blue line) traffic.
- The overall trend shows fluctuations in bandwidth usage for both media types throughout the recorded period. The bandwidth usage for video is higher than audio.

Video Traffic Analysis

- Video traffic (blue line) shows higher variability and generally higher bandwidth usage.
- Peak video traffic reaches about 550 packets/sec around the 65-second mark.
- Video bandwidth usage fluctuates significantly, with several peaks and troughs throughout the session.
- There's a noticeable drop in video traffic around the 60-second mark, followed by a sharp increase.

Audio Traffic Analysis

- Audio traffic (red line) shows more consistent and lower bandwidth usage compared to video.
- Audio bandwidth generally stays below 100 packets/sec throughout the session.
- There are small fluctuations in audio traffic, but they are less pronounced than video fluctuations.
- A slight increase in audio bandwidth is observable around the 65-second mark, coinciding with the video traffic peak.

2 Conclusion

The analysis of Microsoft Teams call traffic reveals a predominant use of UDP for real-time communication, with RTP and Skype protocols handling most of the audio and video data. Video traffic consistently demands higher bandwidth and exhibits greater variability compared to audio, which maintains a lower, more stable bandwidth usage, reflecting the distinct requirements of these media types in digital communications.

3 Appendix

3.1 PCAP File

Below is the list of Pcap files attached to this report :

- basil-audio-off-video-off.pcapng
- basil-audio-off-video-on.pcapng
- basil-audio-on-video-off.pcapng
- basil-audio-on-video-on.pcapng
- jaskaran-audio-off-video-off.pcapng
- jaskaran-audio-off-video-on.pcapng
- jaskaran-audio-on-video-off.pcapng
- jaskaran-audio-on-video-on.pcapng