Data Networks WS 18/19
INTERNET ARCHITECTURE:
Assignment 10

Chirag Bhuvaneshwara - 2571703
Florena Raja – 2566418

Question 1: (1 + 1 + 1 = 1 points) VoIP over TCP Please answer in 3-5 sentences per question.

(a) Describe briefly how TCP reacts to packet loss.

When the sender running TCP detects a packet loss, it'll retransmit the packets that were not acknowledged and due to the nature of IP(on which TCP runs) these retransmitted packets might be lost again. Also, due to congestion control in TCP, the rate of transmission at the sender side will be reduced as a packet loss is interpreted as the link being congested. The extent of the reduction is determined by the particular variant of TCP. This means that the receiver should expect delays not only due to the unpredictability of IP but also due to TCP's behaviour on packet loss.

(b) Assume a VoIP session was established over TCP, how would the user experience be affected in case of a packet loss?

When there is a packet loss, TCP sender will try to retransmit the lost packets which might be lost again and this might result in the retransmitted packets being received at the receiver side with some amount of delay. And if this delay exceeds 400ms, the quality of the VoIP session will be bad. Basically, some parts of the audio will never be heard on the receiver side as the delay caused by TCP might be greater than the playout delay being used by the VoIP session.

(c) In your opinion, is TCP the best choice for VoIP?

For a real time application such as VoIP, TCP is not the best choice as it does not guarantee timely delivery of the audio data. In VoIP, there is no need for exact reconstruction on the receiver side. A good enough reconstruction which ensures that most of the audio data is delivered without going over the playout delay in the VoIP session would perform much better than TCP.

Question 2: (.5 + .5 = 1 points) Video Streaming

Please provide a short answer for the questions below.

(a) TCP is not ideal for audio and video playback (or "conversational"-type applications). Please cite three brief reasons why not.

1. TCP retransmits lost packets which might get lost again making the receiver wait till it receives those particular packets. For example, in a scenario where the receiver buffer is filled except for 1 particular missing packet and the sender can ensure delivery of this particular packet in the 10th retransmission, a large amount of delay is introduced which just halts the playback at the receiver.
2. Congestion control reduces throughput upon detecting packet loss which also might introduce too much delay.
3. TCP prevents the use of IP multicast. Such an IP multicast could potentially help reduce bandwidth requirement for a large audience of the same video/audio data.

(b) Why is UDP not a good replacement for TCP in the above scenario? Briefly cite two reasons.

1. The amount of available bandwidth between server and client varies with time. In such a scenario, constant rate UDP streaming can fail to provide continuous playout as it may lead to congestion on the link.
2. As such an overflow of UDP packets might lead to congestion, many firewalls are configured to block UDP traffic. This prevents the users behind such firewalls from receiving any UDP video.

Question 3: (0.5 + 0.5 + 1 + 1 = 3 points) RTP

Please provide a short answer for the questions below.

(a) Does the word "real-time" in Real-time Protocol imply that RTP guarantees "real-time" delivery?

The word "real-time" does ***not*** imply that RTP guarantees real-time delivery. It just implies that when UDP is used to transfer real-time(streaming) data, RTP provides some additional functionality by providing port numbers, IP addresses, time stamping etc in its header field. RTP is implemented on the end-systems and the routers in between, will not be unpacking the RTP headers.

(b) Is RTP a transport protocol?

RTP is not part of the transport layer but instead part of the application layer. It provides additional information for UDP which is a transport layer protocol.

(c) Does RTP provide reliable data transport? How?

RTP typically runs on top of UDP and as a result, does not provide reliable data transfer. But it does provide ways of detecting packet loss and out of order delivery and facilities to compensate against jitter.

(d) Do routers prioritize audio and video playback data delivered using RTP? If your answer is yes", (briefly) state how such prioritization schemes are implemented. If your answer was "no", (briefly) explain why not.

Within a particular network, a network administrator may implement a scheme which ensures that RTP messages are prioritized within his network. This can be implemented by having dedicated queues at the routers for RTP packets. The routers can then be programmed to process this RTP queue first leading to an RTP prioritized scheme. But outside this particular network, such a priority might not be given to RTP as another scheme which does not prioritize any particular messages might be implemented.

Question 4: (1 + 1 = 2 points) SIP

(a) Is SIP a reliable protocol? What happens when a SIP INVITE request is lost?

SIP alone doesn't guarantee reliability as SIP can work on both TCP and UDP. If we run SIP on TCP, we get reliability and on UDP, we do not get reliability. When a SIP INVITE request is lost, the sender's device may choose to terminate the call or it might choose to retransmit the invite.

(b) What is a SIP registrar and why do we need them?

A SIP registrar acts like an endpoint providing a location service which means that the registrar redirects the SIP invite request obtained for "bob@somewebsite.com" to the IP address it has stored for that particular email address. This registrar obtains the email address to IP address mapping by accepting SIP REGISTER requests and records the email address and associated IP address of each user.

Question 5: (0.5 + 1 + 0.5 + 1 = 3 points) Traffic Policing

(a) What does traffic policing mean?

Traffic policing allows one to control the maximum rate of traffic that is transmitted or received on an interface.

(b) What fields of a packet header are used to "mark" a packet for offering differentiated services?

Packet is marked in the Type of Service (TOS) field in IPv4, and Traffic Class field in IPv6

(c) Cite one use for differentiated services.

With differentiated services being deployed, Emergency call/dialled numbers maybe prioritised and this ensures that the person having an emergency is attended sooner.

(d) DiffServ provides a framework to allow classification and differentiated treatment of packets. Classification refers to "packet marking" and differentiated treatment refers to scheduling and queue-management policies at routers. Where does traffic policing come into play in the DiffServ architecture? Do we need policing to support DiffServ? Why (or why not)?

Traffic policing comes into play at the routers that perform differentiated service because even though certain types of data will be given higher priority, it does not mean that the whole bandwidth will be assigned to this particular type of data. So Traffic policing would ensure that, the high priority data uses only the relatively larger amount of bandwidth assigned to it and does not go beyond that limit.

We do need policing to support differentiated service because we need to ensure that each class has a maximum rate imposed on it and if it goes above this limit, it should be penalized so that it is not allowed to take up the whole bandwidth as that might block all other traffic.