Université de Tamanrasset

Faculté des Sciences et de la Technologie

Département de Mathématiques et Informatique

05/11/2025

Réalisé par : Dr. gattal elhachemi

Email : elhachmig@gmail.com

TP 6 — Protocoles de transmission (Wireshark + Python + GNS3)

Objectif général
Travail pratique simple mais formateur pour découvrir les protocoles de transmission à travers trois outils complémentaires :
1) GNS3 pour construire un mini-réseau et injecter des conditions de lien (latence/perte/QoS).
2) Wireshark pour observer les en-têtes (TCP/UDP/QUIC/RTP) et le comportement du contrôle de flux/congestion.
3) Python pour analyser des traces (pcap) et extraire des métriques (RTT, retransmissions, gigue, débit effectif).

À la fin, l'étudiant comprend quoi il fait et pourquoi : il relie la théorie (framing, ARQ, rwnd/cwnd, QoS, PMTUD, NAT) à la pratique.

Compétences visées (Learning Outcomes)
- Distinguer TCP, UDP, QUIC et RTP en pratique.
- Lire les champs d'en-tête dans Wireshark (Ports, Seq/Ack, Flags, Options, DSCP, SACK…).
- Observer Sliding Window, rwnd/cwnd et l'effet de l'AQM/QoS sur la gigue.
- Diagnostiquer PMTUD/MSS et le HoL d'HTTP/2 vs le multiplexage QUIC.
- Exploiter Python (pyshark/scapy) pour produire un mini-rapport chiffré.

Pré-requis
- GNS3 + GNS3 VM, images Linux/Alpine/Ubuntu (hôtes) et/ou VyOS/FRR (routeur).
- Outils : Wireshark, iperf3, tc/netem, curl (HTTP/3), (optionnel : ffmpeg/gstreamer, coturn).
- Python 3 + pyshark ou scapy, pandas, matplotlib.

Topologie minimale
Host A —— Routeur (Linux/VyOS) —— Host B
Deux liaisons Ethernet : (A–R) et (R–B). Sur le routeur, on injecte du délai/perte (netem) et on peut activer fq_codel (AQM).

Partie A — Comparer TCP vs UDP (Wireshark)

1) Sur Host B : iperf3 -s
2) Sur Host A : iperf3 -c <B> -u -b 2M -t 30 puis iperf3 -c <B> -t 30 -i 1
3) Capture Wireshark (A–R) : filtres udp / tcp.
4) Tableau : UDP (8 octets) vs TCP (20–60) avec champs.

Questions : Pourquoi pas d'ordre/ARQ en UDP ? Où apparaît le Window Scaling ?

Partie B — Sliding Window et Throughput ≈ min(rwnd, cwnd)/RTT

1) Routeur : tc qdisc add dev <iface> root netem delay 40ms loss 0.5%
2) Host A : congestion CUBIC puis BBR (sysctl …)
3) iperf3 TCP avec capture.
4) Estimer RTT et relever Window/WS dans Wireshark.
5) Comparer le débit iperf3 avec l'estimation.
Livrable : graphe simple CUBIC vs BBR.

Partie C — PMTUD et MSS Clamping

1) ping -M do -s 1472 <B> (varier taille)
2) Observer ICMP Fragmentation Needed/Too Big.
3) (Option) MSS clamping : iptables TCPMSS --clamp-mss-to-pmtu
4) Noter la taille maximale sans fragmentation.
Question : Pourquoi VPN/PPPoE posent plus de soucis MTU ?

Partie D — QoS/AQM : voix (UDP) vs téléchargement (TCP)

1) Routeur : tc qdisc replace dev <iface> root fq_codel
2) Générer flux UDP (DSCP=EF) + gros flux TCP
3) Comparer gigue/latence avant/après fq_codel.
Attendu : baisse de la gigue et de la latence du flux temps réel.

Partie E (option) — HTTP/2 vs HTTP/3 (QUIC)

1) Serveur supportant les deux ; alterner H2/H3 sous 1–2% pertes.

2) Wireshark : udp.port == 443 vs tcp.port == 443.
Observation : HoL en H2 vs multiplexage H3 sans HoL.

Partie E' (option) — RTP/RTCP & Jitter Buffer

1) Émettre RTP (ffmpeg/gstreamer) de A vers B.
2) Injecter delay 20ms + loss 2%.
3) Lire RTCP SR/RR/Jitter et tester FEC léger.

Partie F — Analyse Python (mini-lab)

Tâches TCP : RTT moyen, retransmissions, out-of-order, goodput.
Tâches UDP : jitter approximatif, taux de pertes.
Exemple de code (à compléter) : pyshark + impression Goodput par flux.
Étendre : export CSV + graphiques matplotlib.

Livrables
1) Tableaux en-têtes TCP/UDP (captures Wireshark).
2) Graphe/Tableau CUBIC vs BBR + lien avec min(rwnd,cwnd)/RTT.
3) PMTUD : taille max avant/après MSS clamping + explication.
4) QoS/AQM : gigue/latence UDP avant/après fq_codel.
5) Rapport Python : goodput, retrans, jitter + 1 graphique.
6) (Option) HTTP/2 vs HTTP/3 ou RTP/RTCP.

ملاحظة للطلبة

من جَدَّ وجد، ومن تَعب تعلَّم .ومع كلّ تعمّقٍ ستبدو المسائل أوضح فأبسط؛ فالصعوبة كثيرًا ما تكون غلافًا للفهم لم يُفتح بعد.

- **أنتم في مرحلة التعلّم :اغتنموا كلَّ فرصةٍ للتجربة والسؤال والنقاش المؤدّب.**
- **اجتهدوا وابحثوا، وامارسوا الشكّ البنّاء والنقد العلمي، ودوّنوا أخطاءكم قبل صوابكم.**
- **حدِّدوا لكل حصةٍ هدفًا قابلاً للقياس، وطبِّقوا ما تتعلّمونه بأدوات حقيقية (Wireshark/iperf3/GNS3/Python).**
- **تعلّموا أن تربطوا النظرية بالتطبيق :جرّبوا، لاحظوا، قارنوا، ثم لخِّصوا ما توصّلتم إليه.**