UNIVERSITÉ DE SHERBROOKE
Faculté de génie
Département de génie informatique

RAPPORT APP4

Réseaux et protocoles de communication
GIF332

Présenté à
Équipe de formateurs de la session S3

Présenté par
Raphael Bouchard – bour0703
Alexis Guérard – guea0902

Sherbrooke – 28 juin 2023

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

1. ANALYSE DES PDUS

1.1 PDU 1

Le premier champ est l'adresse MAC de destination de 6 octets (FF FF FF FF FF FF). L'adresse de destination utilisée dans ce cas est une adresse de diffusion (broadcast). L'appareil émetteur envoie une requête à toutes les machines du réseau pour déterminer laquelle possède l'adresse IP de destination spécifiée. En d'autres termes, il interroge toutes les machines du réseau pour trouver celle qui correspond à l'adresse IP recherchée.

Le deuxième champ est l'adresse MAC source de 6 octets (F8 B1 56 A3 64 50). C'est l'adresse physique unique de l'émetteur de ce PDU.

Le protocole est le protocole ARP (Address Resolution Protocol) qui est désigné par les deux octets suivant la source, soit les octets 08 06. (Type Ethernet)

Le type de composant réseau qui devrait répondre à ce PDU est la machine qui a l'adresse IP C0 A8 01 01, qui sont les 4 derniers octets du PDU.

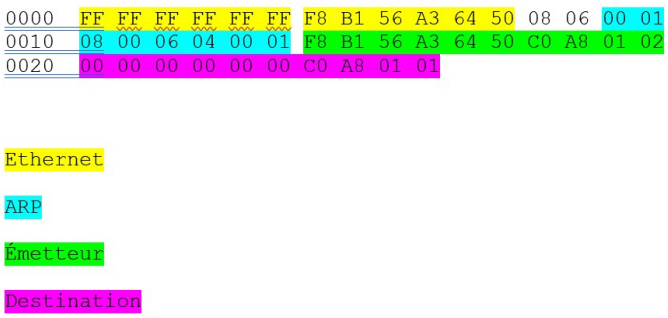

Figure 1 : PDU 1

1.2 PDU 4

Le premier champ est l'adresse MAC de destination de 6 octets (F8 B1 56 A5 90 E1).

Le deuxième champ est l'adresse MAC source de 6 octets (F8 B1 56 A3 59 E0).

Le protocole est le protocole IPv4, qui est désigné par les deux octets suivant la source, soit les octets 08 00. (Type Ethernet)

Les octets 01 DC dans le PDU fourni correspond au type de service dans le protocole IPv4. Il indique la priorité et le traitement spécifique que le paquet devrait recevoir lors de sa transmission sur le réseau.

Les octets 40 00 dans le PDU fourni correspond à la longueur totale du paquet dans le protocole IPv4. Il indique la taille totale du paquet, y compris l'en-tête et les données, en octets. Cela correspond à une longueur totale de 16384 octets.

Les octets 80 06 dans le PDU fourni correspond à l'identification dans le protocole IPv4. L'identification est un champ utilisé pour identifier de manière unique chaque paquet IPv4.

Les octets 68 C2 dans le PDU fourni correspondent aux "Drapeaux et décalages de fragment" dans le protocole IPv4. Ce champ est utilisé pour gérer les fragments des paquets IP lorsque la taille dépasse la capacité maximale autorisée pour une transmission sur le réseau.

Les octets 84 D2 dans le PDU fourni correspondent à la "Durée de vie" dans le protocole IPv4. Ce champ indique le nombre maximal de sauts (routage) qu'un paquet peut effectuer avant d'être éliminé du réseau. Cela correspond à une durée de vie de 33954.

Les octets 4A A2dans le PDU fourni correspondent au champ "Protocole" dans le protocole IPv4. Ce champ indique le protocole utilisé dans la partie de données du paquet. Dans ce cas, les octets "4A A2" indiquent que le protocole utilisé est le TCP (Transmission Control Protocol).

Les octets C0 A8 01 03 dans le PDU fourni correspond à la "Somme de contrôle de l'en-tête" dans le protocole IPv4. Ce champ est utilisé pour vérifier l'intégrité de l'en-tête du paquet IPv4. Il s'agit d'une valeur calculée en fonction des informations de l'en-tête et utilisée pour détecter les éventuelles erreurs de transmission ou de manipulation des données.

L’adresse IP source est représenter par les octets 0B E1 04 20.

Le type de composant réseau qui devrait répondre à ce PDU est la machine qui a l’adresse IP 6F F5 0F 95. (Adresse IP de destination)

Les 12 derniers octets (68 6F 77 20 61 72 65 20 79 6F 75 3F) représentent le message « how are you? » en hexadécimal.

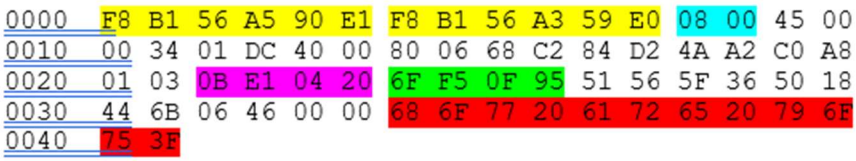

Figure 2 : PDU 4

2. EXPLICATION DU DÉTOURNEMENT DE LA SESSION TCP

Au cours de l'analyse, il a été identifié que l'attaque a été réalisée en usurpant l'adresse IP du développeur. Les détails de l'attaque sont les suivants :

Le développeur (adresse MAC : 00:00:c0:29:36:e8) a établi une communication avec le serveur (adresse MAC : 00:06:5b:d5:1e:e7) en utilisant le protocole TELNET. Cependant, un attaquant (adresse MAC : 00:01:03:87:a8:eb) a réussi à prendre le contrôle de l'adresse IP du développeur (192.168.1.103) et a envoyé un message au serveur. Nous avons pu trouver s'il y avait des trames qui n'étaient pas des adresses du développeur et du serveur avec le filtre « !(eth.src eq 00 :00 :c0 :29 :36 :e8) and !(eth.src eq 00 :06 :5b :d5 :1e :e7) ». Cela a donc confirmé qu'il y avait une attaque.

L'attaquant a été en mesure de s'insérer à la bonne séquence, soit la 233^{e} à la transaction 461. Si le numéro de séquence avait été trop bas, l'attaquant aurait reçu un accusé de réception (ACK) du serveur, indiquant que le message avait déjà été reçu. D'autre part, si le numéro de séquence avait été trop élevé, le serveur n'aurait pas reçu les messages dans l'ordre attendu et aurait sollicité l'envoi des paquets manquants au développeur.

Lorsque le développeur a envoyé la véritable séquence 233 au serveur, celui-ci a répondu en indiquant au développeur qu'il avait déjà reçu le paquet 233 et qu'il attendait le paquet 234. Cependant, le développeur n'était pas préparé à cette réponse inattendue et a répété l'envoi du paquet 233 de manière répétée, créant ainsi une boucle infinie de cette séquence.

En conséquence, l'attaquant a réussi à prendre le contrôle de la communication vers le serveur. Une fois le contrôle établi, l'attaquant a commencé par effacer le contenu de la ligne de commande actuelle en utilisant des caractères d'échappement (\b). Par la suite, il a inséré la

commande "echo HACKED" dans le profil du développeur sur le serveur à la séquence 243 à la transaction 243.

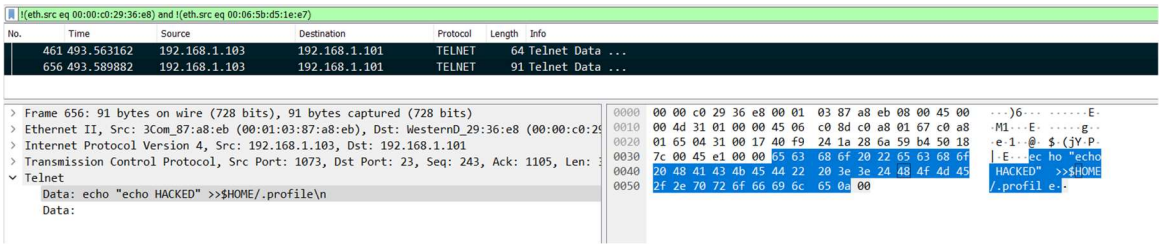

Figure 3 : Trames provenant de l'attaquant

3. CHEMINS PAR LESQUELS PASSE LE TRAFIC IP

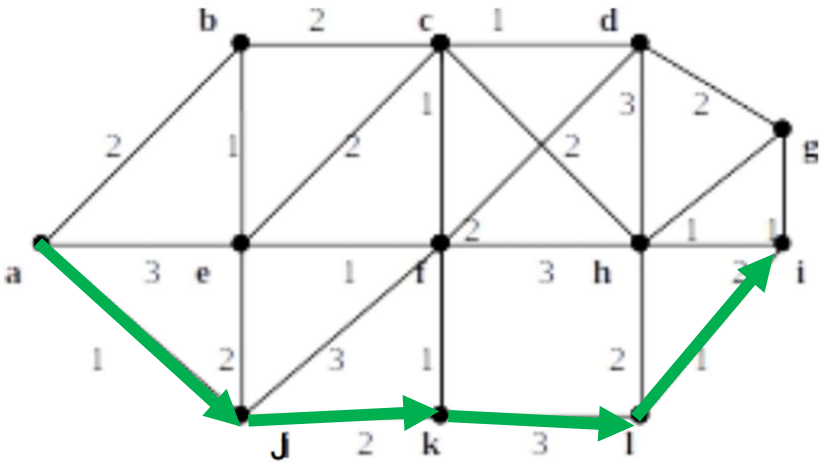

Figure 4 : Diagramme d'interconnexion

En utilisant l'algorithme de Dijkstra, il a été possible de déterminer la distance minimale entre chaque point et le routeur principal de l'entreprise (routeur A). À l'aide du tableau complété ci-dessous, il a été constaté que le coût des connexions entre le routeur de sortie (routeur I) et le routeur principal de l'entreprise est de 7. Il a été possible de trouver ce « cout » en commençant du point A et en cherchant la distance minimale de ses nœuds adjacents. L'algorithme a procédé de manière itérative en sélectionnant à chaque étape le nœud ayant la distance la plus courte par rapport à A parmi ceux qui n'ont pas encore été traités. Cette étape consistait à mettre à

jour le tableau des distances en enregistrant la distance minimale pour chaque nœud visité. Ensuite, pour trouver le chemin, il suffisait de se référer au tableau en partant du nœud I et en suivant les lettres correspondantes jusqu'à atteindre le nœud A. Le chemin obtenu de cette manière représentait le trajet avec la distance minimale entre I et A selon l'algorithme de Dijkstra.

Tableau 1 : Étape de l'algorithme de Dijkstra

Sommet	A	B	C	D	E	F	G	H	I	J	K	L
A	0a	2a	∞_a	∞_a	3a	∞_a	∞_a	∞_a	∞_a	1a	∞_a	∞_a
J		2a	∞_a	∞_a	3a	4j	∞_a	∞_a	∞_a	1a	3j	∞_a
B		2a	4b	∞_a	3a	4j	∞_a	∞_a	∞_a		3j	∞_a
E			4b	∞_a	3a	4j	∞_a	∞_a	∞_a		3j	∞_a
K			4b	∞_a		4j	∞_a	∞_a	∞_a		3j	6k
C			4b	5c		4j	∞_a	6c	∞_a			6k
F				5c		4j	∞_a	6c	∞_a			6k
D				5c			7d	6c	∞_a			6k
H							7d	6c	8h			6k
L							7d		7l			6k
G							7d		7l			
I									7l			

Chemin le plus court de A à I : A → J → K → L → I

4. AVANTAGES ET INCONVÉNIENTS DE LA SOLUTION DE ROUTAGE STATIQUE, AVEC RIP ET AVEC OSPF

4.1 EXTENSIBILITÉ DE LA SOLUTION

La solution de routage statique avec RIP présente des limitations en termes d'extensibilité lorsque de nouveaux routeurs sont ajoutés au réseau. La mise à jour des tables de routage doit être effectuée manuellement, ce qui peut devenir fastidieux et source d'erreurs. Dans les réseaux de grande envergure, où le nombre de routeurs et de sous-réseaux est élevé, cette approche peut entraîner des problèmes d'évolutivité et une charge administrative importante.

En revanche, la solution de routage statique avec OSPF offre une meilleure extensibilité lorsqu'il s'agit d'ajouter de nouveaux routeurs. Grâce à l'utilisation de domaines de routage (areas), les nouveaux routeurs peuvent être facilement intégrés à un domaine existant, ce qui réduit la

charge administrative lors de l'extension du réseau. Les mises à jour de routage sont propagées efficacement au sein de chaque domaine, permettant ainsi une gestion plus efficace des réseaux de grande taille.

4.2 TOLÉRANCE AUX PANNES

En ce qui concerne la tolérance aux pannes, la solution de routage statique avec RIP présente des limites. Bien qu'elle utilise un mécanisme de compte à rebours pour éviter les boucles de routage, cela peut prendre du temps pour que les mises à jour de routage se propagent à l'ensemble du réseau. Pendant cette période, des chemins de routage incorrects peuvent être utilisés, entraînant des temps d'indisponibilité du réseau en cas de panne.

En revanche, la solution de routage statique avec OSPF est conçue pour être hautement résiliente aux pannes. Elle utilise des mécanismes de détection rapide des pannes et de convergence rapide pour rétablir les chemins de routage en cas de défaillance d'un lien ou d'un routeur. Grâce à ces mécanismes, OSPF ajuste rapidement les tables de routage en fonction des changements du réseau, ce qui permet de minimiser l'impact des pannes sur la connectivité globale.

4.3 FACILITÉ DE CONFIGURATION DES ROUTEURS

En ce qui concerne la facilité de configuration pour privilégier une route plutôt qu'une autre, la solution de routage statique avec RIP présente des limitations. RIP utilise le protocole de vecteur de distance, où la décision de routage est principalement basée sur le nombre de sauts. Cette approche offre une configuration limitée des préférences de routage, ce qui peut rendre difficile la mise en place de politiques de routage avancées.

D'un autre côté, la solution de routage statique avec OSPF offre une plus grande flexibilité dans la configuration des préférences de routage. En utilisant l'état de lien, OSPF permet aux administrateurs de définir des métriques plus précises telles que la bande passante, le coût ou la charge pour influencer les décisions de routage. Cette flexibilité accrue offre un contrôle plus précis sur la sélection des routes préférées, en fonction des besoins spécifiques du réseau.

4.4 Recommandation du choix de routage pour l'entreprise

La recommandation de choix de routage pour l'entreprise serait d'opter pour le routage dynamique avec OSPF. Cette solution offre une meilleure extensibilité en permettant une intégration aisée de nouveaux routeurs grâce à la segmentation en domaines de routage. De plus, OSPF garantit une tolérance aux pannes élevée grâce à ses mécanismes de détection rapide et de convergence rapide. Enfin, OSPF offre une plus grande flexibilité dans la configuration des préférences de routage, permettant ainsi de mettre en place des politiques de routage avancées. En choisissant OSPF, l'entreprise bénéficiera d'un réseau évolutif, fiable et adapté à ses besoins spécifiques.

5. Protocole de transfert de fichier

5.1 Définition de chaque couche

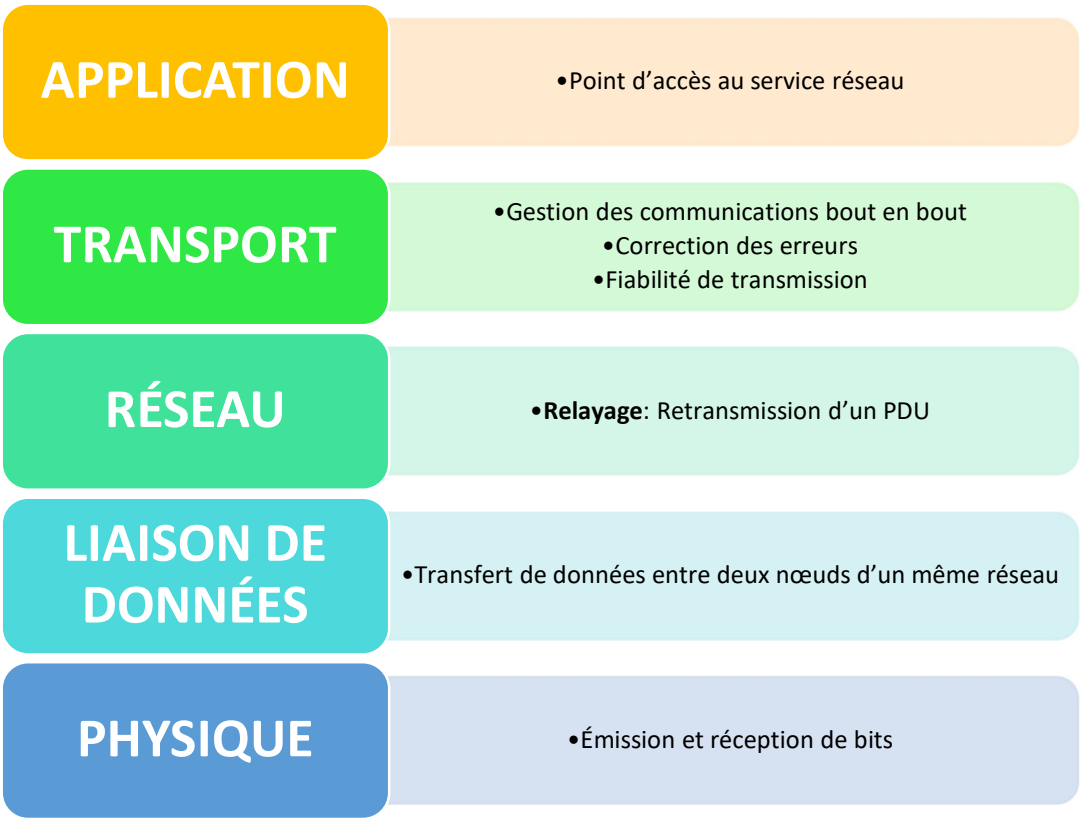

Figure 5 : Modèle OSI (Chain of responsability)

Le fonctionnement de notre protocole de transfert de fichier se fait avec une partie du modèle OSI. Cela est donc une chaine de responsabilité singleton. Lorsque le client est lancé, le thread écoute sur le port et est prêt à recevoir les informations. Lorsque le client envoie un fichier, cela commence par la couche application. Cette dernière lit le type de fichier envoyé et le transforme en octet et elle lit le contenu du fichier envoyé et le transforme également en octet. Ceci est ensuite envoyé à la couche transport. Cette couche sépare les octets en PDU de 200 octets et l'envoie ensuite à la couche réseau, qui sert seulement d'auxiliaire entre la couche transport et la couche liaison de données. La couche liaison de données vérifie s'il y a des erreurs à l'aide de CRC en ajoutant 4 octets aux PDUS. Ceci est maintenant envoyé à la couche physique. Cette dernière décale les données si le paramètre pour ajouter des erreurs est activé. Elle envoie également les octets au bon endroit à l'aide de l'adresse IP de destination et au bon port.

5.2 DIAGRAMME DE CLASSES DU PROTOCOLE DE TRANSFERT

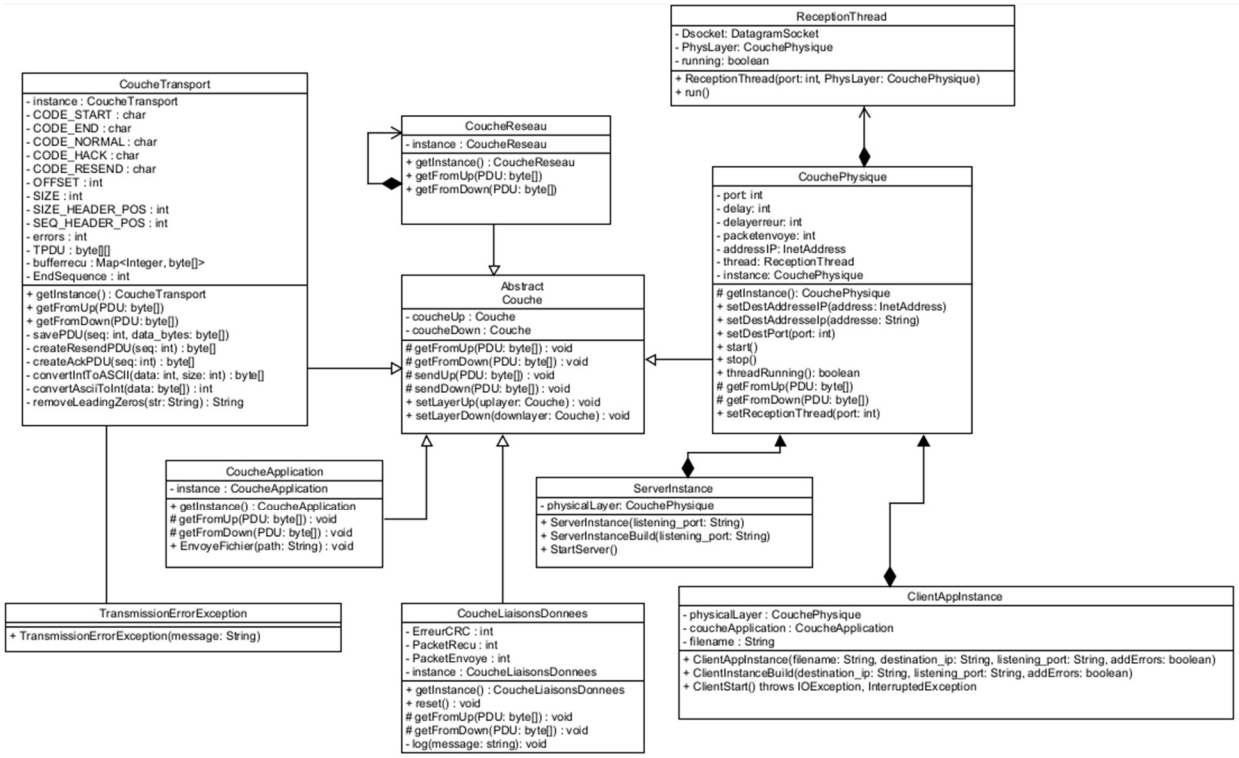

Figure 6 : Diagramme de classes

*Le diagramme est également disponible en pièce jointe

5.3 PLAN DE TEST

Tableau 2 : Plan de tests

Test	Résultat attendu
Lancer le serveur et le client en passant en paramètre pour le client un petit fichier existant, l'adresse IP de destination 127.0.0.1, le port 25002 et false.	Le fichier se retrouve dans le dossier « dest », il n'y a aucune erreur dans la console qui a été détectée.
Lancer le serveur et le client en passant en paramètre pour le client un petit fichier existant, l'adresse IP de destination 127.0.0.1, le port 25002 et true.	Il y a une erreur dans le terminal et le fichier ne s'est pas rendu dans le dossier « dest ».
Lancer le serveur et le client en passant en paramètre pour le client un gros fichier existant, l'adresse IP de destination 127.0.0.1, le port 25002 et false	Le fichier se retrouve dans le dossier « dest », il n'y a aucune erreur dans la console qui a été détectée.
Lancer le serveur et le client en passant en paramètre un fichier qui n'existe pas, l'adresse IP de destination 127.0.0.1, le port 25002 et false.	Met l'exception « NoSuchFileException » dans le terminal.
Lancer le serveur et le client en passant en paramètre un fichier existant, une adresse IP incorrecte, le port 25002 et false.	Le fichier ne se rend pas dans le dossier « dest ».
Lancer le serveur et le client en passant en paramètre un fichier existant, l'adresse IP de destination 127.0.0.1, le port 4443 et false.	Le fichier ne se rend pas dans le dossier « dest ».
Lancer le serveur et appuyer sur la touche q et ensuite sur la touche « enter » dans le terminal.	Le serveur arrête de fonctionner.