

TP – ADMINISTRATION RÉSEAU

AGBENONZAN KOSSIVI JACQUES JUNIOR
SANOGO SOULEYMANE

LICENCE 3 – RIST – UFHB

2025 - 2026

Introduction

L'objectif de ce TP est de mettre en pratique les notions d'**administration réseau** en observant et comparant le fonctionnement du protocole DHCP en **IPv4** et en **IPv6**. À travers des captures réalisées avec **Wireshark** et des expérimentations dans un environnement simulé avec **Kathará**, nous cherchons à :

- Forcer et analyser les requêtes DHCP générées par un client.
- Identifier les différentes étapes du cycle **DORA** (Discover, Offer, Request, Ack) en IPv4 et du cycle **SARR** (Solicit, Advertise, Request, Reply) en IPv6.
- Comprendre les types de diffusion utilisés (broadcast en IPv4, multicast/unicast en IPv6).
- Vérifier les adresses sources et destinations réelles dans les échanges.
- Automatiser la mise en place et la capture des paquets via des scripts pour garantir un environnement reproductible.

Ce TP s'inscrit dans une démarche pédagogique visant à relier la théorie des protocoles réseau à leur observation concrète, tout en développant des compétences pratiques en diagnostic et en administration réseau.

1. Mise en place du labo

- **Sur Mon OS Windows:**
 - J'Active/Désactive mon interface réseau pour forcer une requête DHCP.
 - On tape les commandes suivantes dans cmd

"cmd"
ipconfig /release
ipconfig /renew

- Lance **Wireshark** sur l'interface Wi-Fi.

Filtre : dhcp (IPv4).

No.	Time	Source	Destination	Protocol	Length	Info
11...	-563.702548	10.230.93.90	10.230.93.132	DHCP	342	DHCP Release - Transaction ID 0xd280
24...	-434.588672	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa3cd
24...	-434.559762	10.230.93.132	10.230.93.90	DHCP	352	DHCP Offer - Transaction ID 0xa3cd
24...	-434.554455	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0xa3cd
24...	-434.543513	10.230.93.132	10.230.93.90	DHCP	352	DHCP ACK - Transaction ID 0xa3cd
49...	-181.527956	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x1fc3
49...	-181.501785	10.230.93.132	10.230.93.90	DHCP	352	DHCP ACK - Transaction ID 0x1fc3

Etape	Norme	Diffusion réelle	Ip Source	Ip Destination
Discover	Broadcast	Broadcast	0.0.0.0	255.255.255.225
Offer	Unicast/ Broadcast	Unicast	10.230.93.132	10.230.93.90
Request	Broadcast	Broadcast	0.0.0.0	255.255.255.225
Ack	Broadcast /Unicast	Unicast	10.230.93.132	10.230.93.90

- **Wireshark** sur l'interface Wi-Fi.

Filtre : dhcpv6 (IPv6).

Etape	Norme	Diffusion réelle	Ip Source	Ip Destination
Solicit	Multicast		fe80::d107:337a:6f6d:6cb7	ff02::1:2
Advertise	Unicast/ Multicast			
Request	Unicast/ Multicast		fe80::d107:337a:6f6d:6cb7	ff02::1:2
Reply	Unicast/ Multicast			

- **Sur Kathara**

Après avoir configuré les labs

Nous nous rendons directement à l'emplacement du fichiers lab.conf et nous lançons fichier .bat, ce fichier me sert a automatiser la saisie des commandes suivantes :

- Nettoyage de tous les conteneurs et réseaux Kathara précédents

"bat"
kathara wipe Kathara lclean

Ces commande supprime tous les conteneurs Docker et réseaux virtuels précédents pour garantir un environnement propre.

- Démarrage du lab...

"bat"
kathara lstart

Crée et démarre les conteneurs Docker (client) avec la configuration réseau spécifiée. Charge et exécute le fichier **client.startup**

- Attente de 30 secondes pour la génération des paquets DHCPv4 et DHCPv6

"bat"
timeout /t 30 /nobreak

Donne le temps au script Python dans le conteneur de générer tous les paquets DHCPv4 et DHCPv6.

- Récupération capture

#Crée le dossier de destination si nécessaire mkdir ..\rapport\captures_pcap 2>nul #Copie le fichier .pcap depuis le conteneur vers l'hôte kathara copy client /shared/dhcp_complet.pcap ..\rapport\captures_pcap\

Le dossier ████████ dans Kathara est un volume partagé entre l'hôte et le conteneur. Cette commande transfère la capture réseau.

On a alors les captures suivantes

```
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/d6:f2:dd:36:0a:a6
Sending on      LPF/eth0/d6:f2:dd:36:0a:a6
Sending on      Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 15
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 12
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 14
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 8
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 5
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x0
2	2.038223	10.0.0.1	10.0.0.100	DHCP	286	DHCP Offer - Transaction ID 0x0
3	4.096004	0.0.0.0	255.255.255.255	DHCP	286	DHCP Request - Transaction ID 0x0
4	6.133077	10.0.0.1	10.0.0.100	DHCP	286	DHCP ACK - Transaction ID 0x0
5	10.568028	fe80::	ff02::1:2	DHCPv6	76	Message Type 68 XID: 0x484350
6	12.613045	2001:db8::1	2001:db8::100	DHCPv6	78	Message Type 68 XID: 0x484350
7	14.646704	fe80::	ff02::1:2	DHCPv6	76	Message Type 68 XID: 0x484350
8	16.708405	2001:db8::1	2001:db8::100	DHCPv6	74	Message Type 68 XID: 0x484350

Filtre : dhcp(IPv4)

Etape	Norme	Diffusion réelle	Adresse Mac / ip Source	Ip Destination
Discover	Broadcast	Broadcast	d6:f2:dd:36:0a:a6/0.0.0.0	255.255.255.255
Offer	Unicast/Broadcast	Unicast	10.0.0.1	10.0.0.100
Request	Broadcast	Broadcast	d6:f2:dd:36:0a:a6/0.0.0.0	255.255.255.255
Ack	Broadcast/Unicast	Unicast	10.0.0.1	10.0.0.100

Filtre : dhcpv6(IPv6)

Etape	Norme	Diffusion réelle	Ip Source	Ip Destination
Solicit	Multicast	Multicast	fe80::d107:337a:6f6d:6cb7	ff02::1:2

Advertise	Unicast/Multicast	Unicast	2001:db8::1	2001:db8::1
Request	Unicast/Multicast	Multicast	fe80::d107:337a:6f6d:6cb7	ff02::1:2
Reply	Unicast/Multicast	Unicast	2001:db8::1	2001:db8::1

Bilan

Ce TP montre que, même si DHCPv4 et DHCPv6 poursuivent le même objectif (attribuer des paramètres réseau aux clients), leurs mécanismes diffèrent :

- **IPv4** repose sur le broadcast et le cycle DORA.
- **IPv6** introduit le multicast et le cycle SARR, avec en plus la possibilité d'utiliser **SLAAC** pour l'autoconfiguration.

En conclusion, cette mise en pratique nous a permis de comprendre les différences normatives et techniques entre les deux protocoles, de les observer dans des captures réelles, et de renforcer notre maîtrise des outils d'administration réseau.