Contrôle d'accès : TP - DHCP, NAT & Syslog

BLUEM Juliette - SEZNEC Lucas - MAIMBOURG Gaston

31 mai 2022

1 Introduction

Dans le cadre du cours de contrôle d'accès réseaux et authentification, nous allons dans ce TP mettre en place les protocoles DHCP et NAT puis les superviser avec le protocole Syslog.

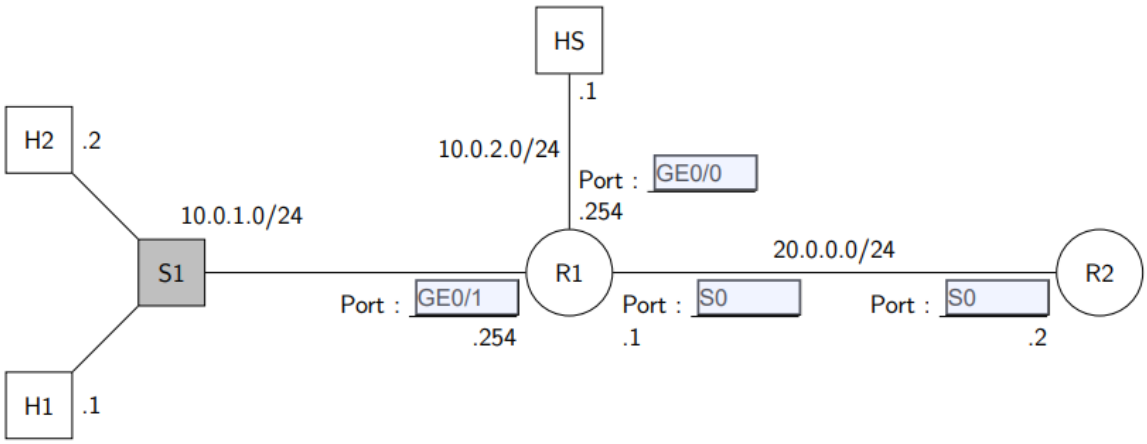
Le protocole Dynamic Host Configuration Protocol (DHCP - RFC 2132) permet d'attribuer dynamiquement des adresses IP à des hôtes. Il permet également de configurer d'autres paramètres des hôtes passerelle, DNS, proxy...

Le protocole Network Address Translation (NAT - RFC 2663) est une méthode qui permet de faire correspondre des adresses IP à d'autres adresses. Généralement, le protocole NAT est utilisé pour permettre à des réseaux privés de communiquer avec Internet, en translatant les adresses IP internes en adresse IP publique associée à un port.

Sur un LAN connecté à Internet, on trouvera généralement une association des protocoles DHCP et NAT au niveau de la passerelle. Étant donné qu'il s'agit du point d'entrée et de sortie du réseau, il est important de superviser le déroulement de ces protocoles. Pour cela, différentes méthodes existent, notamment le Syslog.

Syslog est un standard (RFC 5424) pour l'envoi et la réception de messages d'enregistrement d'évènements. Grâce au Syslog, un équipement peut émettre des messages à chaque évènement vers un serveur qui les enregistre. Le serveur peut alors les analyser et au besoin émettre des alertes. Les messages syslog contiennent un champ "Facility" qui indique le type et un niveau de sévérité.

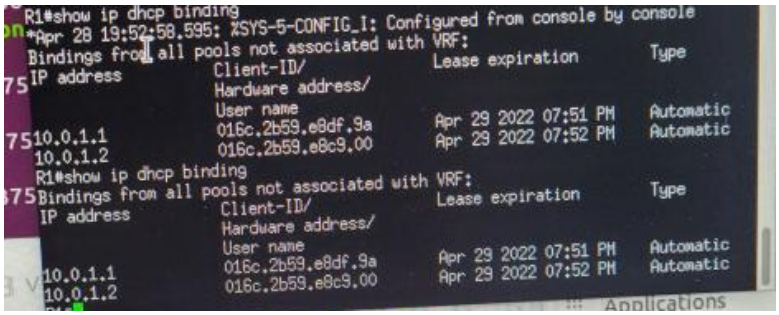
Voici la topologie de notre réseau :



2 Mise en place du protocole DHCP

Pour commencer, nous créeons un pool IP DHCP que nous nommons "LAN". Ensuite, nous faisons en sorte que notre pool distribue des adresses IP dans le sous réseau 10.0.1.0/24 et on configure l'adresse de passerelle distribuée par le DHCP. Nous avons maintenant nos hôtes qui sont bien configurés pour recevoir une configuration via DHCP.

À l'aide de la commande "show ip dhcp binding", on observe que nos hôtes ont reçu les adresses 10.0.1.1 et 10.0.1.2 et qu'elles ont été attribuées automatiquement.



Ces adresses appartiennent donc aux hôtes H1 et H2 que nous avons configurés afin qu'ils reçoivent une configuration avec DHCP.

3 Mise en place du protocole NAT/PAT

Nous souhaitons mettre en place le protocole NAT car lorsque H1 essaie de ping R2, R1 encapsule son IP sur le ping donc R2 reçoit le ping et répond à R1. Mais lorsque que R1 reçoit le ping contenant la réponse de R2, il ne sait pas quel hôte à envoyé le ping et donc ne peut pas translater pour que H1 reçoive la réponse.

On crée un pool d'adresses IP publiques pour R1 avec une seule adresse qui est celle de son interface.

À partir de là, à l'aide d'une seule commande, on configure le NAT IP intérieur pour utiliser la liste 10 comme source et l'interface de sortie de R1 avec le pool d'IP publiques. L'option "overload" permet au NAT de faire correspondre plusieurs adresses à son adresse publique en utilisant le PAT, qui permlet de faire de la translation de ports.

Après cela, la connexion entre les hôtes du réseau local et le routeur distant R2 est possible. À l'aide de la commande "show ip nat translation", on observe que R1 associe le port 13 à H1 lorsqu'il ping R2 :

4 Syslog

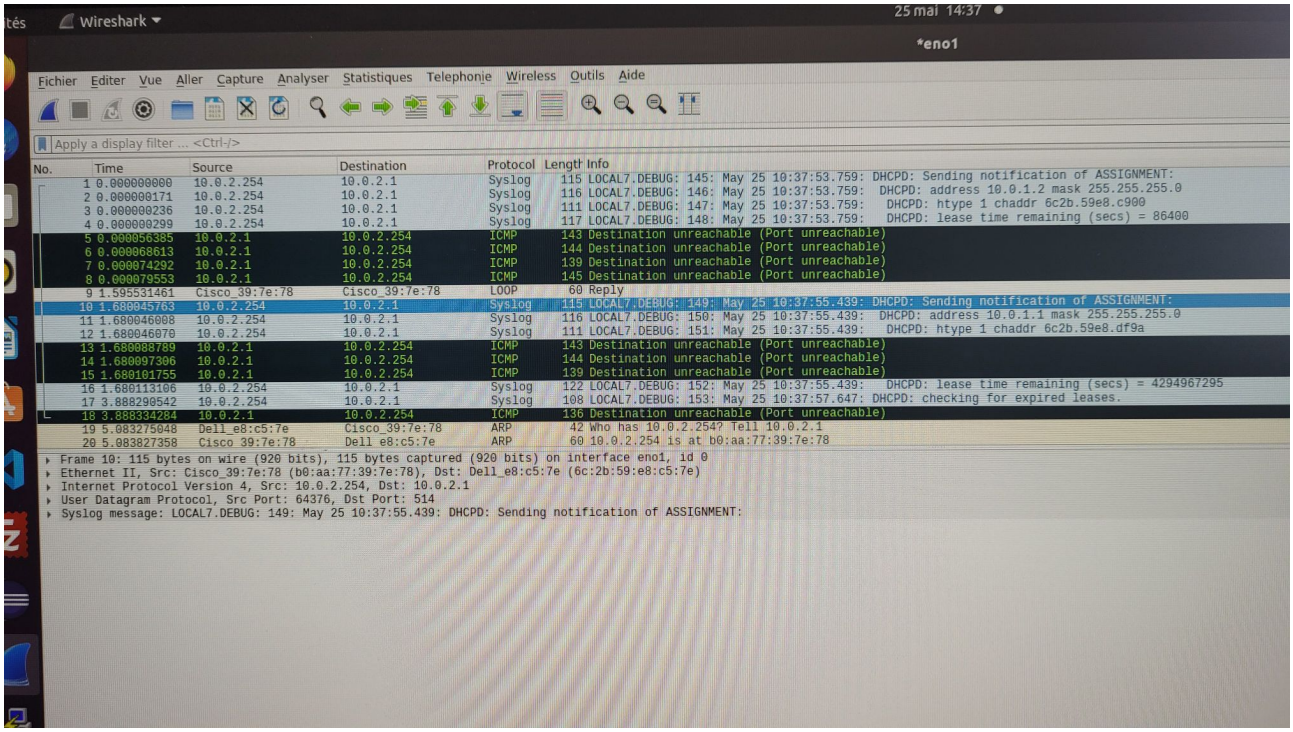
Dans cette partie, nous allons configurer sur notre routeur R1 l'envoi de messages Syslog afin d'enregistrer toute attribution ou translation d'adresse.

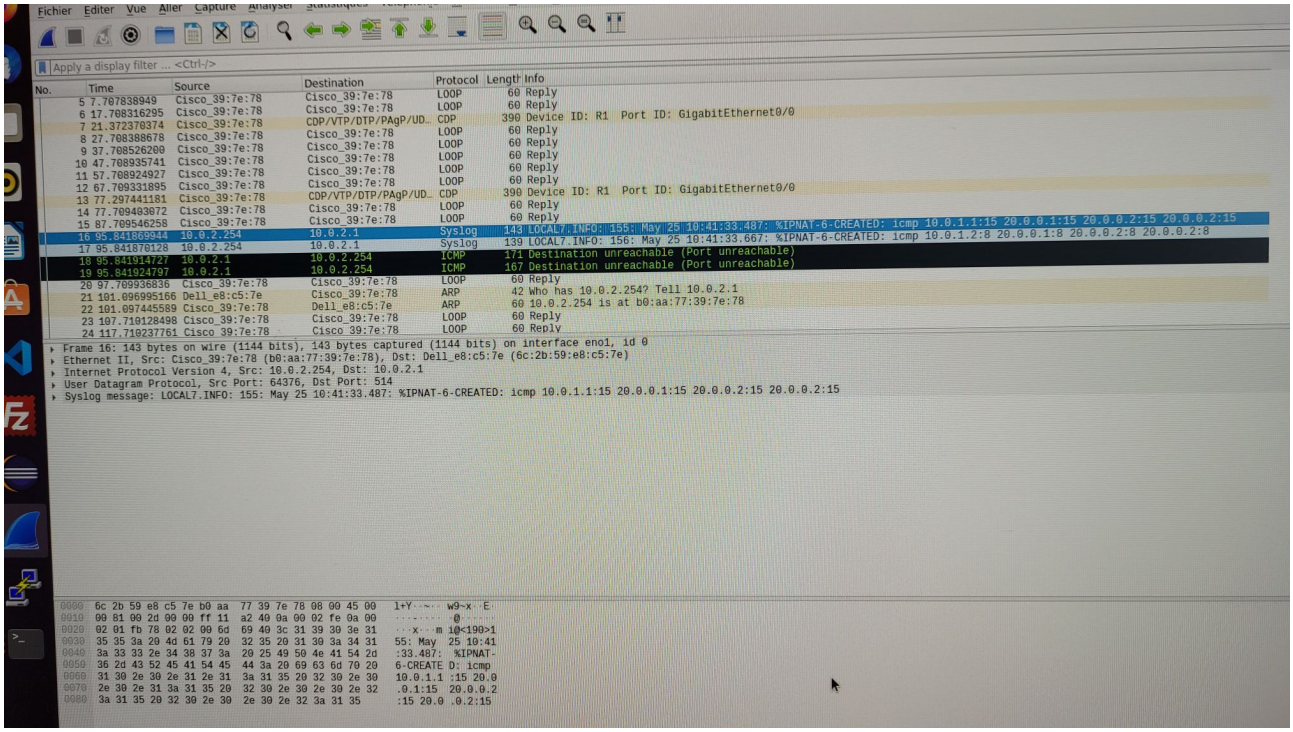
Tout d'abord, nous vérifions sur le switch HS que le serveur Rsyslog est lancé afin qu'il puisse recevoir les messages.

Ensuite sur R1, nous allons configurer l'envoi en règlant l'horloge système via la commande "clock" et en affectant HS comme hôte de reception avec la commande "logging". Une fois cela fait, nous allons utiliser la commande "logging trap debugging" pour envoyer les alarmes de niveau débug.

Enfin, nous allons activer les messages DHCP avec la commande "ip dhcp server events" et en renouvelant le bail DHCP sur H1 et H2. Avec cela, nous activons les messages NAT avec la commande "ip nat log translations syslog".

Maintenant que nous avons terminé la configuration des messages Syslog, nous allons pouvoir à présent effectuer des requêtes depuis H1 et H2 vers R2. Nous pouvons observer les messages Syslog transmis avec Wireshark comme ci-dessous :

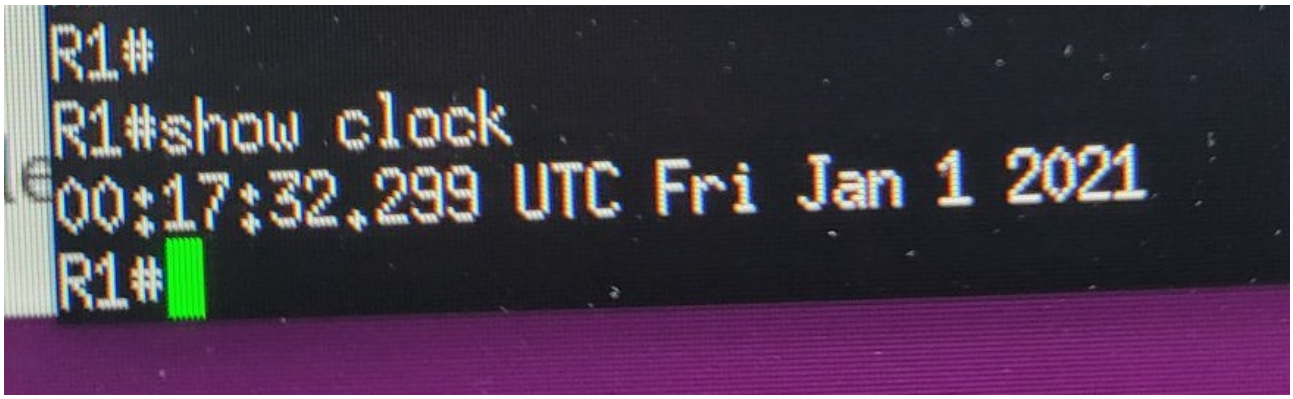



Fichier Editer Vue Aller Capture Analyser
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
5 7.707838949 Cisco_39:7e:78 Cisco_39:7e:78 LOOP 60 Reply
6 17.708316295 Cisco_39:7e:78 Cisco_39:7e:78 LOOP 60 Reply
7 21.372370374 Cisco_39:7e:78 CDP/VTP/DTP/PAgP/UD... CDP 390 Device ID: R1 Port ID: GigabitEthernet0/0
8 27.708388678 Cisco_39:7e:78 Cisco_39:7e:78 LOOP 60 Reply
9 37.708526200 Cisco_39:7e:78 Cisco_39:7e:78 LOOP 60 Reply
10 47.708935741 Cisco_39:7e:78 Cisco_39:7e:78 LOOP 60 Reply
11 57.708924927 Cisco_39:7e:78 Cisco_39:7e:78 LOOP 60 Reply
12 67.709331895 Cisco_39:7e:78 Cisco_39:7e:78 LOOP 60 Reply
13 77.297441181 Cisco_39:7e:78 CDP/VTP/DTP/PAgP/UD... CDP 390 Device ID: R1 Port ID: GigabitEthernet0/0
14 77.709403072 Cisco_39:7e:78 Cisco_39:7e:78 LOOP 60 Reply
15 87.709546258 Cisco_39:7e:78 Cisco_39:7e:78 LOOP 60 Reply
16 95.841869944 10.0.2.254 10.0.2.1 Syslog 143 LOCAL7.INFO: 155: May 25 10:41:33.487: %IPNAT-6-CREATED: icmp 10.0.1.1:15 20.0.0.1:15 20.0.0.2:15 20.0.0.2:15
17 95.841870128 10.0.2.254 10.0.2.1 Syslog 139 LOCAL7.INFO: 156: May 25 10:41:33.667: %IPNAT-6-CREATED: icmp 10.0.1.2:8 20.0.0.1:8 20.0.0.2:8 20.0.0.2:8
18 95.841914727 10.0.2.1 10.0.2.254 ICMP 171 Destination unreachable (Port unreachable)
19 95.841924797 10.0.2.1 10.0.2.254 ICMP 167 Destination unreachable (Port unreachable)
20 97.709936836 Cisco_39:7e:78 Cisco_39:7e:78 LOOP 60 Reply
21 101.096995166 Dell_e8:c5:7e Cisco_39:7e:78 ARP 42 Who has 10.0.2.254? Tell 10.0.2.1
22 101.097445589 Cisco_39:7e:78 Dell_e8:c5:7e ARP 60 10.0.2.254 is at b0:aa:77:39:7e:78
23 107.710128498 Cisco_39:7e:78 Cisco_39:7e:78 LOOP 60 Reply
24 117.710237761 Cisco_39:7e:78 Cisco_39:7e:78 LOOP 60 Reply
Frame 16: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface eno1, id 0
Ethernet II, Src: Cisco_39:7e:78 (b0:aa:77:39:7e:78), Dst: Dell_e8:c5:7e (6c:2b:59:e8:c5:7e)
Internet Protocol Version 4, Src: 10.0.2.254, Dst: 10.0.2.1
User Datagram Protocol, Src Port: 64376, Dst Port: 514
Syslog message: LOCAL7.INFO: 155: May 25 10:41:33.487: %IPNAT-6-CREATED: icmp 10.0.1.1:15 20.0.0.1:15 20.0.0.2:15 20.0.0.2:15
0000 6c 2b 59 e8 c5 7e b0 aa 77 39 7e 78 08 00 45 00 l+Y..~.. w9~x..E.
0010 00 81 00 2d 00 00 ff 11 a2 40 0a 00 02 fe 0a 00 ...-.... .@......
0020 02 01 fb 78 02 02 00 6d 69 40 3c 31 39 30 3e 31 ...x...m i@<190>1
0030 35 35 3a 20 4d 61 79 20 32 35 20 31 30 3a 34 31 55: May 25 10:41
0040 3a 33 33 2e 34 38 37 3a 20 25 49 50 4e 41 54 2d :33.487: %IPNAT-
0050 36 2d 43 52 45 41 54 45 44 3a 20 69 63 6d 70 20 6-CREATE D: icmp
0060 31 30 2e 30 2e 31 2e 31 3a 31 35 20 32 30 2e 30 10.0.1.1 :15 20.0
0070 2e 30 2e 31 3a 31 35 20 32 30 2e 30 2e 30 2e 32 .0.1:15 20.0.0.2
0080 3a 31 35 20 32 30 2e 30 2e 30 2e 32 3a 31 35 :15 20.0 .0.2:15

5 Partie Bonus : NTP

Network Time Protocol (« protocole de temps réseau ») ou NTP est un protocole qui permet de synchroniser, via un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure. Cette fonctionnalité est donc cruciale pour l'horodatage des évènements.

Dans la topologie du TP, R2 sera la référence, c'est-à-dire le serveur NTP. Ensuite sur R1, on déclare l'adresse de R2 comme étant le serveur NTP. Après quelques minutes, afin d'actualiser l'horloge de R1, on remarque qu'avec la commande "show clock" que R1 utilise bien la date du premier Janvier 2021 fixée à minuit sur R1 comme référence d'horloge :



6 Conclusion

Ce TP nous a apprit le fonctionnement de différents protocoles tel que DHCP pour distribuer des adresses aux hôtes au sein d'un réseau local ainsi que NAT/PAT qui permettent de faire de la translation d'IP et de port entre le réseau local et distant. Afin de pouvoir surveiller l'activité de ces protocoles sur le réseau, nous avons mis en place un serveur Syslog, réccupérant les logs des évènements sur le routeur R1. L'observation et l'analyse des logs d'équipements réseau tel que des serveurs ou des routeurs permet de surveiller leur activité, d'y détecter des comportements anormaux voir frauduleux mais également d'avoir des informations utiles lors d'un dépannage de ces équipements. Finalement, la mise en place du protocole NTP vient assurer l'horotage des logs puisque le timestamp d'un log est une information précieuse lors de son analyse.