TP Protocoles d'Application

Dino Lopez Pacheco dino.lopez@univ-cotedazur.fr

1 Introduction

Ce TP a pour objectif de vous permettre d'observer et comprendre, le fonctionnement de certains protocoles que vous utilisez de manière courante. Ces protocoles sont tellement utilisés que leurs exécutions passent souvent inaperçus. Être conscient de la manière dont ils fonctionnent est un premier pas vers la résolution des potentiels problèmes des applications réparties.

2 Le protocole DHCP

Comme on l'a vu en cours, le protocole DHCP permet d'obtenir de manière automatique des informations nécessaires pour devenir un membre actif du réseau.

1. Nous allons « jouer » avec le protocole DHCP.
    - Téléchargez le fichier topo-test-dhcp.imn et déployé le réseau (click sur bouton « start »)
    - Vérifiez que les clients c1 et c2 ne possèdent pas d'adresse IPv4. Quelle commande utiliser ?

    ip a s

    - Sur chaque client, ouvrez un terminal et exécutez tcpdump avec un filtre permettant de capturer uniquement le trafic DHCP. Tcpdump doit garder les paquets *sniffés* dans le fichier « cx.pcap » (où « x » correspond au numéro du client). Quelle commande tcpdump utiliser ? **Laissez tcpdump tourner.**

    tcpdump -i eth0 "udp and (port 67 or port 68)" -w c1.pcap

    - Dans une nouvelle fenêtre pour c1, exécutez la commande « dhclient -v eth0 » (il y a toujours 4 tcpdump's en cours d'exécution dans le réseau). A la fin de l'exécution de la commande dhclient, fermez toutes les commandes tcpdump avec « Ctrl + c ». Vérifiez que le nombre de paquets capturés par tcpdump est > 0. **Expliquez également à quoi sert la commande « dhclient » que vous venez d'exécuter.**

    La commande permet d'exécuter un client DHCP qui cherche à obtenir une adresse IPv4 pour l'interface donné en argument. « -v » est le paramètre « verbose » (exécution d'une commande « bavarde », qui explique tout ce qui se passe).
    Les clients ont dû capturer 2 paquets, à l'exception de « c1 » qui capture 4 paquets.

2. Ouvrez les fichiers pcap de c2, c3 et c4 avec Wireshark (i.e. exécutez « wireshark c2.pcap » si on est dans le client « c2 »).
    - Quels sont les paquets qui ont été capturés par c1, c2 et c3 (voir colonne « Info » de la division supérieure de la fenêtre wireshark) ? Pourquoi ces paquets ont été capturés ?

    Ce sont les paquets « DHCP Discover » et « DHCP Request ». Ils ont été capturés car les paquets ont été envoyé en mode broadcast.

- Comment peut-on identifier la machine à l'origine des messages reçus par c2, c3 et c4 ? Astuce : vérifiez l'adresse MAC de votre suspect principale (commande « ip a s », ligne « link/ether ») et l'adresse MAC source des paquets capturés (sous-fenêtre au milieu, ligne « Ethernet II », champ « Src »). N'hésitez pas à demander l'aide de votre encadrant si vous n'arrivez pas à identifier ces élements.

Vérification faite, on voit sur wireshark que l'émetteur possède une adresse MAC « 00:00:00:00:00:01 », qui est l'adresse MAC de « c1 ». La machine « c1 » est donc à l'origine de ces paquets.

3. Quels paquets ont été envoyés à la suite de votre commande dhclient ? voir fichier pcap sur c1.

DHCP Discover, DHCP Offer, DHCP Request, DHCP Ack

- Quels paquets ont été envoyé en mode broadcast (paquets dont la destination est l'adresses « 255.255.255.255 ») et quels paquets ont été envoyé en unicast ? Expliquez brièvement l'objectif de chaque paquet DHCP capturé.

DHCP Discover – Broadcast. Paquet envoyé pour détecter tous les serveur DHCP du réseau.
DHCP Offer – unicast. Paquet utilisé par le serveur pour offrir une adresse valable à un client.
DHCP Request – Broadcast. Si plusieurs serveur DHCP font une offre, ce paquet permet de faire comprendre à tous quel serveur/adresse a été choisi
DHCP Ack – Unicast. Confirme l'assignation de l'adresse IP par le serveur.

- Expliquez brièvement comment une communication en mode unicast est possible alors que la machine « c1 » ne possédait pas une adresse IPv4.

Même si le client ne possède pas d'adresse IP, sa carte réseau possède une adresse matérielle (l'adresse MAC), qui permet de l'identifier.

- Comment trouver, grâce à wireshark l'adresse IP proposée par le serveur ?

On le trouve dans le champ « your (client) IP address » du paquet DHCP Offer et DHCP Ack.

- Combien de temps pouvons-nous garder cette adresse IP (trouver l'option « IP Address Lease Time ») ?

La période d'utilisation de cette offre est de 10 minutes. « IP Address Lease Time » donne cette période en nombre de secondes.

- Quel routeur, serveur DNS et nom de domaine sont fourni par le serveur DHCP, si jamais ces informations ont été envoyés par notre serveur ?

Pour trouver cette information, sur wireshark : « Routeur », c'est l'option 3 du protocole DHCP, « serveur DNS » option 6. Le « nom de domaine » n'est pas fourni par notre serveur.

4. Quels sont les ports d'écoute du client et du serveur ? Analyser les lignes « User Datagram Protocol » des paquets sur Wireshark (sous-fenêtre centrale).

Client 68, Serveur 67

5. Expliquez comment les mécanismes du protocole DHCP peuvent être utilisés pour introduire de sérieux problèmes de sécurités dans un LAN.

   Vu qu'aucun mécanisme d'identification du serveur n'est pas implémenté côté client, c'est assez simple de mettre un serveur DHCP dans un réseau donnant des adresse IP des serveurs DNS et routeurs compromis. De plus, rarement les utilisatreurs·ices des ordinateurs vérifient ou peuvent vérifier que les informations données par le serveur DHCP sont celles attendues.

6. En capturant à nouveau le trafic DHCP sur c1, exécutez la commande « dhclient -r *nom_interface* » où « *nom_interface* » est le nom de l'interface réseau de c1 connecté au LAN. Quel paquet à été envoyé suite à votre commande ?

   DHCP Release. C'est le paquet qui indique au serveur que le client efface la configuration fournie

7. Arrêtez le réseau virtuel et quittez CORE complètement.

3 Le protocole DNS

Nous avons vu en cours que le protocole DNS permet la traduction des noms canoniques de machines en adresse IP. Cependant, le service DNS permet d'autres opérations très courantes également, comme l'obtention du serveur SMTP d'un domaine. Nous allons illustrer maintenant avec quelques exercices les principaux services fournis par le protocole DNS.

Les prochains exercices se font directement dans la VM.

8. Avec la commande « dig -t a www.google.com » obtenez l'adresse IPv4 du serveur www.google.com

   - Donnez l'adresse IPv4 du serveur

   172.217.21.4

   - Avez-vous trouvé que la réponse provient d'un serveur avec autorité sur le domaine ? regardez la ligne « ;; flags … » et « ;; SERVER … » (ce dernier donne l'adresse et port du serveur DNS que nous avons contacté). Voyez ici la significations du champ flags de dig https://kiwix.ounapuu.ee/serverfault.com_en_all_2019-02/A/question/729025.html

   La réponse provient d'un serveur sans autorité dans le domaine. Nous voyons bien que l'adresse IP sur serveur DNS et la 127.0.0.53 (machine locale). Ceci veut dire que la requête exécutée par nslookup est répondu par l'information DNS en cache de notre machine locale.

9. Avec dig et le type de requête (-t) approprié, essayez d'obtenir l'adresse IPv6 du serveur www.google.com. Y a-t-il une adresse IPv6 associé à ce serveur ? essayez aussi de trouver l'adresse IPv6 de www.univ-cotedazur.fr

   -t aaaa. Il est possible de trouver une adresse IPv6 pour www.google.com (2a00:1450:4007:818::2004). En revanche, pas d'adresse IPv6 pour www.univ-cotedazur.fr.

10. Pour obtenir le serveur DNS d'un domaine, on utilise une requête NS. Expliquez pourquoi les commandes « dig -t ns www.google.com. » et « dig -t ns google.com. » produisent des résultats distincts.

    www.google.com. est un FQDN d'une machine. Une machine ne possède pas de serveur DNS. Ce sont les domaines qui possèdent (sont administrées avec) un DNS. « google.com » est un domaine qui possède donc un serveur DNS mais pas « www.google.com ».

11. Vous êtes le serveur SMTP du domaine « gmail.com », et vous avez un email à transférer vers l'adresse ab123456@etu.univ-cotedazur.fr. Comment devez-vous faire pour obtenir l'adresse IPv4 du serveur à qui retransmettre l'email ? utilisez nslookup pour vérifier votre procédure.

    - Vous devez transmettre l'email au serveur SMTP de « etu.univ-cotedazur.fr ».

    On utilise un -querytype=MX pour trouver le nom du serveur SMTP du domaine etu.univ-cotedazur.fr. Puis, -querytype=A pour trouver l'adresse IP du serveur obtenu avec la requête de type MX.

12. Faite le nécessaire pour trouver l'adresse IPv4 de www.google.com depuis un serveur avec autorité sur le domaine. Pour indiquer à dig quel serveur DNS interroger, utilisez le caractère « @ ». Ex. « dig @192.168.1.10 www.unice.fr »

    On trouve les serveurs DNS de google.com avec « dig -t ns google.com », puis on prend l'un de ces serveurs pour retrouver l'adresse IPv4 de www.google.com « dig @ns1.google.com -t a www.google.com »

4 Configuration d'un serveur DHCP

Nous allons maintenant procéder à la configuration d'un serveur DHCP. Pour cela, nous utiliserons le serveur DHCP le plus utilisé dans le monde : ISC DHCP.

13. Téléchargez le fichier test-dhcp-conf.imn et déployez le réseau virtuel.
14. Vous configurerez le serveur DHCP sur le nœud « svr ».
    - Notez que le fichier de configuration se trouvera dans le fichier /etc/dhcp/dhcp.conf de « svr »
    - Avant de modifier le fichier de configuration, pensez à arrêter le serveur avec la commande « killall dhcpd »
    - Après avoir modifiez le fichier de configuration, lancez le serveur DHCP pour le tester : « # dhcpd »
15. Modifiez le fichier de configuration dhcp.conf avec un éditeur de texte simple (e.g. gedit) et déclarez à la fin du fichier le réseau pour lequel vous configurerez ce serveur. Nous écrirons un bloque « subnet ». La syntaxe est la suivante :
    - subnet *net_addr* netmas *net_msk* {}
    - E.g. "subnet 192.168.1.0 netmask 255.255.255.0"
    - Quel réseau devez-vous déclarer avec quel netmask ?

    subnet 10.0.1.0 netmask 255.255.255.0 {}

16. A l'intérieur du bloque « subnet », déclarez un intervalle d'adresses disponibles avec la directive « range ». Un intervalle qui marcherait bien pour le bloque « subnet » donné en exemple ci-dessous :
    - range 192.168.1.100 192.168.1.200;
    - Modifiez votre « dhcp.conf » pour déclarer un intervalle de votre choix. Pensez à finir la ligne « range » par le caractère « ; »

    range 10.0.1.100 10.0.1.200;

    - Après avoir sauvegardé le fichier « dhcp.conf », et avoir lancé le serveur DHCP, vous aurez un serveur DHCP minimal.

17. Testez votre serveur grâce au client « c1 ».
    - Quelle commande avez-vous donné ? est-ce que votre intervalle d'adresses a été bien respecté ?

    dhclient -v eth0

    - Est-ce que votre client a reçu l'adresse IP de la passerelle ? exécutez la commande « ip r s » et si vous n'obtenez pas une ligne commençant par « default », vous n'avez pas une passerelle.

    non

    - Est-ce que votre client a reçu l'identité du serveur DNS ? liste le contenu du fichier « /etc/resolv.conf » et vérifiez si y figure l'adresse d'un serveur DNS.

    Le fichier doit être vide.

    - Arrêtez votre serveur DHCP et continuons sa configuration.

    killall dhcpd

    - Si votre client obtient une adresse IP, faite en sorte que ce premier l'efface grâce à l'option RELEASE.

    dhclient -v -r eth0

18. Maintenant, déclarons un serveur DNS et la passerelle que chaque client recevant une adresse IP de notre serveur devra utiliser. Pour cela, vous déclarerez les options « router » et « domain-name-servers » à l'intérieur du bloc « subnet ».
    - « option router @ip_passerelle; » où @ip_passerelle est donc l'adresse IP du routeur de votre réseau.
    - « option domain-name-servers @ip_dns; » où @ip_dns est l'adresse IP d'un serveur DNS. Supposez que le serveur DNS de votre réseau est « c11 ».
    - Faites les modifications pertinentes sur « dhcp.conf ». Pensez à arrêter le serveur et à le relancer dans les bons moments.

    option router 10.0.1.1;
    option domain-name-servers 10.0.1.11;

    - Testez votre nouvelle configuration avec « c1 ».

- Prouvez que vous avez bien reçu l'identité d'un serveur DNS et que la passerelle fonctionne correctement.

On la preuve en regardant le contenu de resolv.conf sur c1 pour le serveur DNS (qui doit bien correspondre à ce qu'on a donné en conf) et avec un ping simplement pour la partie « passerelle ».

- Si tout va bien, faite oublier à « c1 » la configuration obtenue depuis le serveur.

19. Souvent, il est nécessaire que l'une des machines obtienne toujours la même adresse IP suite à la demande d'une adresse à notre serveur DHCP. Par exemple, si vous êtes chez orange, vous pouvez demander que votre Livebox obtienne toujours la même adresse IP, ce que vous permettra d'y installer un serveur. En ISC, ceci se fait facilement en déclarant un bloc « host ». La syntaxe est :
    - host *hostname* { hardware ethernet *hostname_mac_addr*; fixed-address *@IP_to_assign*; }
    - Modifiez la configuration de votre serveur pour que votre client « c1 » possède une adresse fixe différente aux adresses qu'il est lors de vos tests précédents.
    - Prouvez que tout fonctionne correctement.

```
host c1 {
 hardware ethernet 00:00:00:00:00:01;
 fixed-address 10.0.1.99;
}
```

5 Interaction inter-protocolaire

Avant de finir avec ce TP, nous souhaitons vous montrer par une expérience rapide comment le protocole DNS est mise en œuvre pour permettre l'exécution d'autres protocoles applicatifs.

20. Sur votre VM
    - utilisez tcpdump pour enregistrer dans le fichier « /tmp/trace.pcap » uniquement le trafic TCP et UDP (notez que vous devez bien indiquer le nom de l'interface connectée à Internet et que vous devez être « root » pour lancer tcpdump). Laissez tourner tcpdump.

```
# tcpdump "udp or tcp" -i enp0s3 -w /tmp/trace.pcap
```

    - Dans un autre terminal, effacez la cache locale DNS avec la commande « # systemd-resolve --flush-caches »
    - Puis, exécutez la commande « wget http://www.i3s.unice.fr/ --max-redirect=0 ». A la fin de l'exécution de wget, arrêtez la collecte de trafic et analysez la trace avec wireshark
    - Décrivez l'échange qui a lieu à la suite de votre commande, entre votre VM et les serveurs Internet.

On retrouve des requêtes DNS de type A et/ou AAAA pour retrouver l'adresse IPv4 ou IPv6 du serveur. L'adresse IPv4 est bien retrouvée pour la machine niouze.i3s.unice.fr, www.i3s.unice.fr étant un alias de la machine niouze (analyser le paquet « standard query response pour « A www.i3s.unice.fr »), mais il n'y a pas d'adresse IPv6 associée

à niouze.i3s.unice.fr. Après l'obtention de l'adresse IPv4 de www.i3s.unice.fr, on établit une connexion TCP avec ce serveur pour télécharger une ressource.

21. Identifiez le délai introduit par le protocole DNS. En d'autres termes, calculez le temps écoulé entre la transmission de la première requête DNS capturée et le temps de la connexion vers le serveur (transmission du paquet TCP SYN).

    84 ms dans mon expérience.

22. Quel pourcentage de temps représente l'exécution du protocole DNS sur le total de temps pris par wget pour récupérer une réponse du serveur ? considérez que la réponse du serveur est complètement reçu lorsque les derniers paquets FIN / ACK de TCP sont échangés.

    Dans mon expérience, wget prend au total 210ms. 84ms représente donc 40% du temps total pour l'exécution de notre requête avec wget.