Laboratoires services

Rapport laboratoire 6

BULLONI Lucas & WERMEILLE Bastien

20 juin 2018

Table des matières

1 Introduction

Dans le cadre d'un laboratoire du cours "Réseau et application", les services de base d'un réseau informatique sont mis en pratiques. Les protocoles à mettre en place sont le DHCP, DNS, serveur web et optionnellement le protocole NTP. La partie NTP a été réalisée. Le but principal est de créer un petit réseau, et ensuite 4 réseaux connectés, composé uniquement de machine GNU/Linux. Tout le laboratoire se fera sur NetKit, simulation d'environnement réseau virtuel.

1.1 Prérequis

— Un PC Linux avec NetKit

— Laboratoire netkit "qos"

1.2 Réseau du laboratoire

1.2.1 Réseau initial

Le réseau est composé de deux PC, dont un qui est un serveur web, ainsi qu'un serveur qui fait office de DNS et de DHCP.

Le nom du réseau est net1.mylan.ch.

[Image sous-réseau]

1.2.2 Réseau final

L'objectif final est de dupliquer le premier réseau 3 fois et d'interconnecter les 4 sous-réseaux.

[Image réseau final]

2 Déploiement d'un sous-réseau

La première étape du laboratoire est la configuration du serveur DNS et DHCP. Toutes les manipulations de configurations ont été faites dans le fichier "n1-router.startup" afin que les modifications soient préservées lors du redémarrage du laboratoire.

2.1 DHCP

La configuration DHCP se trouvent dans la section du fichier .startup du serveur DHCP/DNS après la ligne :

cat » /etc/dhcp3/dhcpd.conf « EOF

2.1.1 Plage d'adresses dynamiques

La première étape est la configuration de la plage d'adresse IP dynamique. Toutes les machines configurées avec une adresse IP dynamique prendront une adresse entre 192.168.1.100/24 et 192.168.1.199/24.

L'adresse de broadcast est 192.168.1.255 et la passerelle est 192.168.1.1. Nous avons également ajouté le serveur DNS en prévoyance. Le serveur étant la même machine que le DHCP, l'adresse est également 192.168.1.1, de ce fait, le serveur sera en adresse statique.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
   range 192.168.1.100 192.168.1.199;
   option routers 192.168.1.1;
   option broadcast-address 192.168.1.255;
   option domain-name-servers 192.168.1.1;
   option domain-name "net1.mylan.ch";
}
```

2.1.2 Adresses statiques

le serveur DNS/DHCP est configuré en IP statique, un serveur DHCP ne peut en effet pas s'attribuer une adresse dynamique. Il faut également faire attention à ne pas mettre une adresse statique dans la plage d'adresse dynamique pour ne pas créer de conflit. La configuration du serveur DHCP est faite dans la définition de la zone de la partie précédente

Le serveur web est également configuré avec une adresse IP statique. En effet, un serveur Web ne va que très rarement changer d'adresse IP afin d'éviter des problèmes de mise à jour DNS. Nous avons décidé de donner l'adresse 192.168.1.42 pour ce serveur. La configuration est la suivante :

```
host tournedix {
   hardware ethernet 00:00:00:01:00:00;
   fixed-address   192.168.1.42;
}
```

2.2 DNS

La configuration DNS est également faite dans le fichier .startup du serveur.

2.2.1 Définition de la zone

Comme énoncé précédemment, la zone (sous-réseau) est composé d'un serveur web et d'un PC simple, et d'un serveur DHCP/DNS. Comme le protocole l'énonce, les entrées DNS sont de type NS, les entrées simples A (pour IPv4), les alias CNAME et les serveurs mails MX. [1]

Certaines entrées doivent être configurées dans les deux sens, du passage de l'hostname à l'adresse IP et de l'adresse IP à l'hostname.

la configuration hostname vers adresse ip est faite après la ligne :
'cat > /var/lib/bind/net1.mylan.ch.zone « EOF'

Et la configuration hostname vers adresse IP est faite après la ligne :
'cat > /var/lib/bind/1.168.192.in-addr.arpa.zone « EOF'

Serveur DNS/DHCP Comme énoncé précédemment, le serveur DNS doit être de type NS. Mais cet enregistrement ne permet pas de spécifier son hostname, il faut donc également ajouter une adresse de type A pour pouvoir y accéder via son hostname. Un alias a également été fait pour que la machine puisse être accédé avec le nom 'routeur' et 'dns'.

La configuration est donc la suivante :

```
@  IN NS dns.net1.mylan.ch.
dns   IN A  192.168.1.1
@  IN A  192.168.1.1
```

```
routeur IN CNAME dns
```

et dans l'autre zone :

```
@ IN   NS dns.net1.mylan.ch.
```

Serveur Web Le serveur web sera accessible avec le nom www et pc1. Deux enregistrement de type A ont donc été fait :

```
pc1   IN A  192.168.1.42
www   IN A  192.168.1.42
```

3 Déploiement de 4 sous-réseaux

4 Autres services

PTP text du cours : Le protocole PTP (Precision Time Protocol), coupe a du support dans les équipements de commutation permettant de modifier les datagrammes couche 4 en transit (transparent clock) et d'y insérer des informations de délais effectifs, peut atteindre la précision requise, dans la mesure ou les délais peuvent être estimées symétriques et constants durant les fenêtres de synchronisation. Un des avantages du PTP est la possibilité, si les équipements de commutation le supportent (boundary clock), de pouvoir supporter la synchronisation en phase.

5 Questions

1. Quel est le rôle du mot clé authoritative dans la configuration du serveur DHCP ?

Dans le cas où l'on a configuré le sous-réseau "'aa.bb"' dans le DHCP, une requête venant d'un sous-réseau "non identifié" "'aa.bb.cc"' sera ignorée si ce mot clé n'est pas activé, s'il est activé, le serveur répondra avec un NACK

2. Pour quelle raison aurait-on tendance à configurer une durée de bail DHCP courte (p.ex. 1h) ? ou longue ? (p.ex. 1 semaine)

- bail court : quand il y a beaucoup de clients et pas beaucoup d'adresses IP disponibles dans la plage
- bail long : quand il y a de grandes plages d'adresses IP et pas beaucoup de clients

3. Peut-on imaginer un réseau dans lequel aucune adresse de type hard static n'existe ?

Non, il faut au moins que le routeur ait une adresse hard static, afin que les différents périphériques puissent joindre le serveur. TODO check

4. Quel est l'avantage de configurer des imprimantes, machines virtuelles ou éventuellement serveurs en adresse de type DHCP static ?

Ces périphériques sont toujours censés être disponibles ! Les mettre en adresse dynamique n'apporte rien. Ces périphériques doivent être en adresse statique afin de toujours pouvoir être atteint de la même manière. Certains programmes par exemple sauvegardent l'adresse IP de certains serveurs au lieu du nom, ce qui poserait des problèmes peur ceux-ci. La configuration statique permet également de limiter le nombre de requêtes inutiles à chaque changement d'adresse des ces différents serveurs/imprimantes/...

5. Peut-on mettre les plages d'adresses DHCP dynamiques là où se trouvent des adresses hard static ?

Non, le serveur DHCP risquerait d'allouer dynamiquement une adresse statique déjà allouée. Si nous voulions pouvoir faire cette manipulation qui n'apporte pas grand-chose, il faudrait que le serveur DHCP sache que ces adresses sont déjà allouées ce qui revient à modifier la plage d'adresses DHCP disponible pour allocation.

6. Qu'est-ce que Cisco appelle des manual bindings ?

Ce sont des adresses IP (un pool) liées à certaines adresses MAC connues par le serveur DHCP.
TODO completer

7. Expliquez le concept derrière la configuration DNS suivante (faites abstraction du CNAME, mais tenez compte du TTL et du fait qu'il y a 2 champs A différents) :

“‘ $ dig -t a www.yahoo.com www.yahoo.com. 216 IN CNAME fd-fp3.wg1.b.yahoo.c fd-fp3.wg1.b.yahoo.com. 38 IN A 46.228.47.114 fd-fp3.wg1.b.yahoo.com. 38 IN A 46.228.47.115
#lancez plusieurs fois la commande pour voir si quelque chose change “‘ on a un serveur dupliqué donc deux serveurs à disposition. Cela permet de répartir la charge sur plusieurs serveurs différents et d'avoir de la redondance en cas de panne.

8. Consultez sur un serveur DHCP le fichier “‘/var/lib/DHCP/dhcpd.leases“‘ : que contient-il ? qu'en déduisez-vous sur la volatilité des adresses IP dynamiques ?

Contiens les bails DHCP. Les adresses IP dynamiques qui ont été allouées possèdent une "durée de vie" limitée qui expire au bout d'un certain moment. Une fois le bail expiré, celui-ci est supprimé et le périphérique qui possédait e bail doit en redemander un.

9. Capturez et expliquez ce qui se passe avec : “‘host big-entry.alphanet.ch“‘ (sur machine réelle, ou “‘nslookup“‘)

Il y de nombreuses adresses IP qui s'affichent : “‘ big-entry.alphanet.ch has address 192.168.24.25 “‘
il y a plusieurs serveurs physiques qui répondent à ce nom (plusieurs entrées avec le même nom dans la résolution d'adresses directe DNS)
TODO ...

10. Expliquez la résolution inverse (adresse IP vers nom)

Correspond à la résolution inverse, d' adresse IP vers nom.

11. Comment un serveur de nom trouve-t-il quels serveurs gèrent la racine “‘.“‘ ?

Le nombre de serveurs racines est limité dans le monde et ceux-ci sont codés en dur.
TODO Check

12. A quoi sert l'option DNS (bind/named) “‘forwarders“‘ ?

L'option “forwarders” permet de rediriger les requêtes qui ne sont pas résolues par notre serveur vers un serveur DNS distant (serveurs DNS de votre FAI par exemple).
Cela permet d'utiliser le cache d'un serveur déjà existant et donc d'obtenir des temps d'accès plus rapides. Si la requête DNS n'est pas résolue par le serveur DNS “distant” alors la requête sera envoyée aux serveurs DNS racine.

13. Vous modifiez une zone gérée par un master et un slave DNS, que devez-vous absolument changer ?

Il est nécessaire de mettre à jour les informations des 2 serveurs DNS, du master et du slave.

14. Que pensez-vous de la sécurité du protocole DNS ? Quelles possibilités existent pour l'améliorer ?

Ce protocole n'est pas sûr et possède plusieurs problèmes de sécurité tel le "DNS Spoofing", qui permet de rediriger les requêtes vers des "faux sites". Il existe une version sécurisée de ce protocole, DNSSEC qui est comme DNS, mais qui inclut du cryptage.

15. Vous venez de configurer deux serveurs DNS pour la zone "'mondomaine.ch"', et ils sont associés à un registrar : expliquez ce que le registry 1 doit faire pour que cela fonctionne, techniquement (indication : "'whois alphanet.ch"' ; de plus, voir les entrées "'NS"' sur "'n1-routeur"' de "'mylan.ch"' vers les sous-domaines)

Faire remonter l'existence de ce réseau au DNS supérieur qui s'occupe de la zone.

16. Pourquoi est-ce important d'avoir des champs PTR existants et cohérents ?

— Faciliter le changement de configuration
— Sécurité

TODO développer

17. A quoi servent les champs de type SRV ? et TXT ? et NAPTR ? (donnez un exemple pour chacun)

— SRV : indique quel serveur s'occupe d'un service spécifique : SIP
— TXT : texte libre. Exemple : notification de règles SPF (Shortest Path First)
— NAPTR : conversion de valeurs. Exemple : n°de téléphone en URI SIP

18. A-t-il été nécessaire de changer le protocole DNS pour supporter les domaines accentués, ou seule une modification du client a suffi ? (indication : punycode, exemple : "'linux-neuchâtel.ch"' dans votre navigateur)

— Aucune modification du DNS 1,tem Mais utilisation de punycode

19. A quoi sert le DNSSEC ?

Sécuriser le protocole 'DNS' avec l'ajout d'un chiffrement des données.

6 Questions pour le rapport

1. Expliquez ce que l'on doit faire sur le maître et le secondaire pour activer un secondaire (slave)

Il est nécessaire de référencer le serveur DNS slave dans le fichier de configuration du routeur principal et référencer le serveur maître dans le secondaire.

2. Sécurité d'un serveur de nom

Indications, `http://docstore.mik.ua/orelly/networking_2ndEd/dns/ch11_02.htm`

(a) Pourquoi les serveurs récursifs sont-ils dangereux ?

Car un attaquant peut faire une attaque de type "DNS Spoofing" sans avoir à se trouver dans le réseau. Il peut faire une requête DNS au roteur vers site dont il veut détourner le trafic et immédiatement après envoyer des réponses DNS au serveur DNS avec une réponse pour ce site avec l'adresse IP de son site malveillant.
Cela lui permet de faire croire à l'utilisateur qu'il se trouve sur le site qu'il a demandé alors qu'il ne l'est pas.

(b) Pourquoi est-ce une bonne pratique de séparer les serveurs autoritaires d'une zone sur Internet d'un serveur récursif pour un sous-réseau ?

Afin que le serveur récursif ne soit accessible que depuis le sous-réseau et pas depuis l'extérieur. Cela permet de limiter les attaques par spoofing.

(c) Qu'est-ce qu'une attaque de trafic amplification sur le DNS ? Comment l'éviter ?

Il s'agit d'envoyer des paquets DNS à des serveurs récursifs ouverts avec comme provenance l'adresse du serveur à attaquer. La requête DNS pourrait être *dig ANY isc.org @x.x.x.x*. Cette requête de 64 bytes peut retourner environ 3'223 bytes, ce qui correspond à une multiplication du trafic(amplification) par 50.

Le comble de ce problème et que la requête en question est possible grave au protocole DNSSEC qui permet d'améliorer la sécurité des réseaux. Cette requête permet de retourner la liste des clés DNSSEC.

Une manière d'éviter cette problématique est de fermer l'accès des serveurs DNS récursif afin d'empêcher les attaquants de les détourner.

Sources :
- `https://www2.e-xpertsolutions.com/attention-aux-attaques-dns/`
- `https://blog.cloudflare.com/65gbps-ddos-no-problem/`
- `https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/`

(d) Avancés : évaluez la résistance d'une configuration BIND9 de base face aux attaques de spoofing basées sur le devinage du champ ID de la requête ?

Indications :
- Est-ce que le numéro de port de la requête est également devinable ? si oui, quel est l'impact sécurité et comment corriger le problème ?
- Que peut-il se passer si l'on met un serveur BIND9 avec numéro de port variable et aléatoire derrière un firewall NAT/PAT, par exemple un routeur ADSL ?

TODO

Sources :
-
-
-
-

3. Qu'est-ce que la configuration de views BIND ?

Permets de présenter une configuration du serveur DNS selon la provenance de la requête. Certains périphériques auront accès à une version et d'autres à une tout autre configuration.

Source :
- https://kb.isc.org/article/AA-00851/0/Understanding-views-in-BIND-9-by-example.html

4. Comparez les protocoles de routage interne OSPF et RIPv2

OSPF se base sur la rapidité d'un chemin alors que RIP fonctionne avec les "hop count". OSPF envoie des messages "link-state advertisement" (lsa) qui contiennent la liste des routeurs atteignable par lui-même à tous ses voisins, propagé ensuite à tous les routeurs du réseau. Cet ensemble de LSA permet de connaître la structure du réseau. Chaque routeur utilisant finalement l'algorithme de Djikstra afin de trouver le chemin le plus court vers chaque réseau.

RIP quant à lui ne prend en compte que le nombre de sauts en chaque routeur. Il envoie des messages toutes les 30 secondes à tous ses voisins avec de leur communiquer la liste des distances qui le sépare des différents réseaux connus. L'avantage de ce protocole est qu'il est simple à mettre en place et supporté par un grand nombre de routeurs. D'un autre côté, celui-ci a une très lente convergence dans de grands réseaux et peut être inefficace dans certains cas, car il ne prend pas en compte la vitesse des lignes.

RIP consomme une partie de la bande passante en continu alors que OSPF lui en consomme principalement lors de l'initialisation du réseau, jusqu'à ce que tout soit calculé puis très peu de paquets sont envoyés par la suite.

Sources :
- https://fr.wikipedia.org/wiki/Open_Shortest_Path_First
- https://en.wikipedia.org/wiki/Routing_Information_Protocol
- http://resources.intenseschool.com/rip-vs-ospf-which-is-better-for-your-network/

5. La délégation de zone inverse est par classe A-C, qui sont obsolètes : des délégations de granularité inférieure à /24 sont aujourd'hui nécessaires : consultez le RFC 2317 pour expliquer la solution moderne

La solution "Moderne" consiste a faire déléguer la résolution inverse de ces réseaux par le FAI à notre propre serveur DNS. Pour ce faire, nous allons en collaboration avec le FAI définir un label pour nommer la zone. Le FAI va ainsi déléguer la résolution-inverse pour la zone contenant nos sous-réseaux à notre propre serveur DNS. Le FAI va également créer un CNAME pour chacun de nos sous-réseaux.

Ainsi, la résolution DNS standard nom vers adresse se sera disponible du côté du FAI et la résolution inverse sera effectué sur notre propre serveur DNS.
Sources :
- https://tools.ietf.org/html/rfc2317
- http://dloads.infoblox.com/direct/kb_attach/1441_Tech_Note_RFC2317.pdf

6. Quand est-ce qu'un CNAME est impossible ? (indication : peut-il coexister avec un même noeud ou une feuille du même niveau) quelles sont les limitations supplémentaires sur CNAME ?

La première limitation est la suivante, un CNAME doit toujours pointer sur un autre nom domaine et jamais sur une adresse. La seconde est qu'aucun autre enregistrement ne doit redéfinir le label du CNAME ! Il ne faut pas nom plus

utiliser de CNAME pour la racine du domaine, mais plutôt utiliser un ALIAS.

Un CNAME ne devrait en théorie pas pointer sur un autre CNAME, cela pourrait causer une boucle DNS non résolvable dans le cas ou les deux CNAME se pointent l'un l'autre.

Sources :

- https://en.wikipedia.org/wiki/CNAME_record <item https://blog.dnsimple.com/2014/01/why-alias-record/
- http://top100opinions.com/2016/09/usability-and-limitations-of-a-cname-record/

7 Conclusion

Références

[1] Marc SCHAEFER. *Protocoles et Réseaux*. 2017. ISBN : 978-2-940387-09-0.