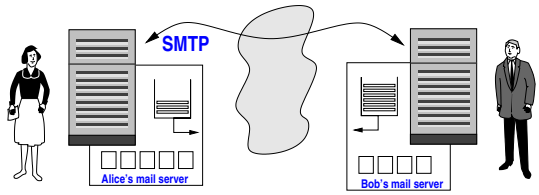
ARes - Lab n°3

Couche application (2) : Messagerie, DNS et SNMP

Ce support est le second consacré à la couche application. Il propose quelques exercices à réaliser sans machine et l'étude des protocoles des applications suivantes : SMTP, POP, IMAP, DNS et SNMP. Pour illustrer nos propos, le trafic réseau de chacune de ces applications sera capturé et analysé avec l'outil `wireshark`.



1 Messagerie

Nous allons détailler les différents mécanismes et protocoles associés à l'émission et à la réception d'un message électronique. En particulier, nous étudierons deux approches qui diffèrent au niveau de la proximité du client : soit basée sur SMTP/POP/IMAP (client local), soit sur HTTP *(web-mail)*.

1.1 Quelques exercices (sans-machine)

1. Bob accède à sa messagerie par le web. Il envoie un message à Alice. Cette dernière rapatrie ses messages sur son ordinateur de bureau lorsque celui-ci est allumé. Décrivez les échanges d'informations ainsi que les protocoles mis en jeu.

2. Rappelez la structure du message échangé par les serveurs de courrier électronique.

3. Pouvez-vous décoder ce champ d'en-tête ?
   `Subject: =?iso-8859-1?B?Qydlc3QgcGFzIGZhY2lsZSAhCg==?=`

4. Vous envoyez un courrier électronique avec un message en texte et en HTML, accompagné de quelques pièces jointes : une image au format PNG, du son encodé en MP3 et un fichier WAD pour Doom. Quelles lignes d'en-tête devrait-on observer dans le message ?

1.2 Services de messagerie sur la plateforme d'experimentation

La plateforme permet d'accéder aux services de messagerie via les protocoles SMTP, POP, IMAP et HTTP *(web-mail)*.

Nous supposons que vous êtes sur le poste ARI **N**. L'envoi d' *e-mail* se fait par le biais du protocole SMTP qui contacte le MTA localisé sur la VM "serveur". Ce dernier peut être identifié grâce à son nom (`mail.etu`**N**`.plateforme.lan`) ou son adresse IPv4 (`10.`**N**`.1.`**N**3). Vous pouvez utiliser la boîte *e-mail* `etudiant` sur le MTA afin de pouvoir recevoir des messages[1].

Vous pouvez alors envoyer des messages à partir d'un premier compte dédié local au client (par exemple "`Test SMTP`") simplement en configurant votre agent de messagerie (`evolution` ou autre UA disponible). Cette configuration doit comprendre comme serveur de messagerie `mail.etu`**N**`.plateforme.lan` et SMTP (ou ESMTP) comme protocole d'envoi des *e-mails*.

Concernant la récupération des messages, vous pouvez accéder à votre boîte `etudiant@etu`**N**`.plateforme.lan` avec les deux protocoles suivant : POP ou IMAP. Pour cela, un deuxième compte local "`Test POP`" est a configurer pour un accès et un retrait des messages par le protocole POP. Un troisième compte local, "`Test IMAP`", est également à configurer pour un accès via le protocole IMAP aux messages présents sur le serveur.

1.2.1 Configuration des serveurs

Voici les 3 serveurs utilisés pour le lab :

- `smtpd` : C'est le serveur **Postfix**[2], MTA alternatif à Sendmail. Pour éviter de changer la configuration du serveur, il est nécessaire d'utiliser la boîte associée au compte UNIX `etudiant`.

[1] En configuration de base, un serveur UNIX associe ses comptes utilisateur UNIX a des boîtes *e-mail*.
[2] `http://www.postfix.org/`

- `imapd` : C'est le serveur **Courier-IMAP**[3] qui assure le service POP et IMAP.
- `apache2` : C'est le serveur HTTP, sur lequel repose **Squirrelmail**[4] (écrit complètement en PHP, sortie en pur HTML).

1.2.2 Configuration des clients

Sur votre machine client, l'utilisation du UA `evolution` nécessite quelques configurations pour rajouter des comptes locaux ("`Test SMTP`", "`Test POP`" et "`Test IMAP`"). Après avoir lancé l'application, dans le menu Edition, sélectionnez Preférence puis utilisez le bouton + Ajouter pour ajouter un nouveau compte. **Attention, les comptes sont peut-être déjà configurés,** dans ce cas effacez les *e-mails* présents et vérifiez les paramètres utilisés.

"Test SMTP" Les étapes pour ajouter dans `evolution` le compte local "`Test SMTP`" pour émettre des messages en SMTP sont les suivantes :

- Ne restaurez pas la session si ce choix vous est proposé
- Configurez le nom "`etudiant sur la VM3`" et l'adresse *e-mail* "`etudiant@mail.etu`**N**`.plateforme.lan`" (vous pouvez préciser que c'est le compte par défaut)
- Ne configurez pas de serveur de réception (choisir "Aucun")
- Configurez le serveur SMTP (sélectionnez le type SMTP, précisez le serveur "`mail.etu`**N**`.plateforme.lan`" et ne sélectionnez aucune authentification)
- Terminez en configurant le nom "`Test SMTP`"

"Test POP" Les étapes pour ajouter dans `evolution` le compte local "`Test POP`" pour récupérer via POP les messages de la boîte `etudiant` du serveur sont les suivantes :

- Utilisez à nouveau le nom "`etudiant sur la VM3`" et l'adresse *e-mail* "`etudiant@mail.etu`**N**`.plateforme.lan`"
- Configurez le serveur POP (sélectionnez le type POP, préciser le serveur "`mail.etu`**N**`.plateforme.lan`", le nom d'utilisateur "`etudiant`" et ne modifiez aucun mécanismes de sécurité ou d'authentification)
- Indiquez que vous souhaitez conserver les messages sur le serveur et laissez les valeurs par défaut des autres options de réception
- Ne configurez pas de serveur SMTP (sélectionnez "`Sendmail`")
- Terminez en configurant le nom "`Test POP`"

"Test IMAP" Les étapes pour ajouter dans `evolution` le compte local "`Test IMAP`" pour accéder via IMAP aux messages de la boîte `etudiant` du serveur sont les suivantes :

- Utilisez à nouveau le nom "`etudiant sur la VM3`" et l'adresse *e-mail* "`etudiant@mail.etu`**N**`.plateforme.lan`"
- Configurez le serveur IMAP (sélectionnez le type IMAP, préciser le serveur "`mail.etu`**N**`.plateforme.lan`", le nom d'utilisateur "`etudiant`" et ne modifiez aucun mécanismes de sécurité ou d'authentification)
- Laisser les valeurs par défaut des autres options de réception
- Ne configurez pas de serveur SMTP (sélectionnez "`Sendmail`")
- Terminez en configurant le nom "`Test IMAP`"

Pour le service de messagerie par *web-mail*, vous devez accéder aux comptes via le navigateur web en vous connectant au serveur à travers **SquirrelMail** via l'URL `http://mail.etu`**N**`.plateforme.lan/squirrelmail`. Entrez alors le nom du compte (`etudiant`) sans spécifier le domaine du serveur mail.

[3] `http://www.courier-mta.org/imap/`
[4] `http://squirrelmail.org/`

1.2.3 Préparation pour réaliser les captures

Les captures que vous allez réaliser dans la prochaine section ont pour but de percevoir la nature des trafics de messagerie. Sur la plateforme d'expérimentation, la topologie 1 a été configurée (postes clients et serveur sur le même LAN). Vous réaliserez ces captures de trafic à l'aide du logiciel `wireshark` :

- A partir du poste ARI **N**, connectez-vous sur les 3 VM correspondantes de la plateforme à l'aide de 3 fenêtres textuelles
  - fenêtre 1 (hôte "client") : tapez `ssh -X etudiant@10.0.7.`**N**1
  - fenêtre 2 (hôte "sonde") : tapez `ssh -X root@10.0.7.`**N**2 (attention, vous êtes administrateur)
  - fenêtre 3 (hôte "serveur") : tapez `ssh -X etudiant@10.0.7.`**N**3
- Vérifiez que les serveurs Postfix, Courier-IMAP et HTTP tournent sur `10.0.7.`**N**3 (fenêtre 3)
  - rechercher les processus des serveurs, tapez `ps aux | grep postfix` ou `imapd` ou `apache2`
  - visualisez la configuration des interfaces, en particulier celle sur le LAN d'étude (`/sbin/ifconfig eth1`) pour vérifier l'adresse IPv4 du serveur pour la connexion du client (devrait être `10.`**N**`.1.`**N**3)
- Démarrez la capture en lançant l'analyseur sur `10.0.7.`**N**2 (fenêtre 2)
  - lancez l'analyseur, tappez : `wireshark`
  - initier la capture sur l'interface `eth1`, comme indiqué précédemment
- Démarrez un UA, `telnet` ou un navigateur sur `10.0.7.`**N**1 (fenêtre 1)
  - soit tapez `evolution` et utilisez-le en fonction des captures demandées relatives à SMTP/POP/IMAP
  - soit tapez `telnet mail.etu`**N**`.plateforme.lan 25`
  - soit tapez `firefox` et entrez l'URL `http://mail.etu`**N**`.plateforme.lan/squirrelmail`
- Observez la capture se réaliser dans la fenêtre de `wireshark`
- Terminez les captures. **Filtrez les trafics afin de ne conserver que ceux relatifs à SMTP, POP, IMAP ou HTTP** (filtre = `smtp`, `pop`, `imap` ou `http`). Enregistrez les traces filtrées pour pouvoir les ré-utiliser ultérieurement.

1.3 Emission du message

1.3.1 Envoi avec le protocole SMTP

Réalisez une capture en utilisant l'UA `evolution` pour envoyer un *e-mail* à partir du compte local par défaut ("`Test SMTP`") vers la boîte (`etudiant`) du serveur.

1. Quelles sont les commandes du protocole SMTP observées lors de l'émission d'un courrier ? Pouvez-vous indiquer leur utilité et le type de réponse produite ?
2. Quelles sont les contraintes imposées à la forme du courrier ? Expliquez la structure de ce dernier et détaillez les champs qui composent son en-tête.
3. Que pensez-vous des possibilités d'identification du protocole SMTP ?

Sans la plateforme... En cas de problème d'accès à la plateforme d'expérimentation ou si vous souhaitez réviser sur une autre machine, vous pouvez télécharger la trace `tme3-smt.dmp` (similaire à celle capturée précédemment) soit à partir du répertoire `/Infos/lmd/2014/master/ue/ares-2014oct`, soit sur la page web `http://www-rp.lip6.fr/~fourmaux/Traces/labV6.html`, puis l'analyser avec le logiciel `wireshark` (sans avoir besoin des droits d'administrateur).

1.3.2 Envoi avec le protocole TELNET

Une alternative, moins attractive mais très efficace, est l'accès au serveur SMTP par le client `telnet`. Il suffit de taper la commande : `telnet mail.etu`**N**`.plateforme.lan 25`.

1. Vérifiez que vous pouvez envoyer un *e-mail* de cette manière.
2. Si vous réalisez une capture, quels filtres allez-vous utiliser ?

1.3.3 Envoi avec le protocole HTTP

Réalisez une capture en utilisant le *web-mail* pour envoyer un *e-mail* vers votre boîte (`etudiant`) sur le serveur.

1. Pouvez-vous retrouver le message original dans la réponse du serveur ?
2. Que pensez-vous de la confidentialité lorsque vous consultez votre courrier de cette manière ?

Sans la plateforme... En cas de besoin, vous pouvez télécharger et analyser la trace `tme3-wm1.dmp` (similaire à celle capturée précédemment) des localisations habituelles (voir la partie 1.3.1).

1.4 Réception du message

1.4.1 Réception avec le protocole POP

Réalisez une capture en utilisant le UA `evolution` pour recevoir un *e-mail* sur le compte local "`Test POP`" (assurez-vous qu'un *e-mail* a bien été reçu sur ce compte précédemment).

1. Quelles sont les commandes utilisées par le protocole POP lors de la récupération d'un courrier ? Pouvez-vous indiquer leur utilité et le type de réponse produit ?
2. A votre avis, quelles seraient les réponses du serveur POP s'il y avait plusieurs messages en attente ?
3. Quelles sont les différences entre le message envoyé précédemment et celui reçu ici ?

Sans la plateforme... En cas de besoin, vous pouvez télécharger et analyser la trace `tme3-pop.dmp` (similaire à celle capturée précédemment) des localisations habituelles (voir la partie 1.3.1).

1.4.2 Réception acec le protocole IMAP

Réalisez une capture en utilisant le UA `evolution` pour recevoir un *e-mail* sur le compte local "`Test IMAP`" (assurez-vous qu'un *e-mail* a bien été reçu sur ce compte précédemment).

1. Quels types d'échanges sont réalisés entre le client et le serveur IMAP ?
2. Quelles différences protocolaires observez-vous entre POP et IMAP ?
3. Quelles sont les différences entre le message envoyé précédemment et celui reçu ici ?
4. Pensez vous que l'authentification soit plus sécurisée avec IMAP ?

Sans la plateforme... En cas de besoin, vous pouvez télécharger et analyser la trace `tme3-ima.dmp` (similaire à celle capturée précédemment) des localisations habituelles (voir la partie 1.3.1).

1.4.3 Réception acec le protocole TELNET

POP et IMAP étant des protocoles textuels, le client `telnet` est utilisable pour se connecter vers les serveurs POP ou IMAP. Il suffit de taper la commande : `telnet mail.etu`**N**`.plateforme.lan <portnum>`. Le `<portnum>` correspond au numéro de port serveur du protocole utilisé : 110 pour POP et 143 pour IMAP.

1. Vérifiez les actions que vous pouvez réaliser de cette manière avec POP.
2. Vérifiez les actions que vous pouvez réaliser de cette manière avec IMAP.
3. Si vous réalisez une capture, quels filtres allez-vous utiliser ?

1.4.4 Réception acec le protocole HTTP

Réalisez une capture en utilisant le *web-mail* pour consulter un *e-mail* sur le compte du serveur (assurez-vous qu'un *e-mail* a bien été reçu sur ce compte précédemment).

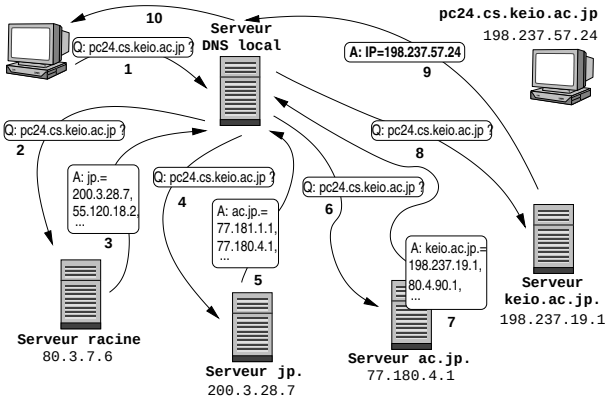
1. Pouvez-vous retrouver le message original dans la réponse du serveur ?
2. La consultation du message retourne beaucoup de trafic HTTP. Discutez des performances d'une consultation à travers le web.

Sans la plateforme... En cas de besoin, vous pouvez télécharger et analyser la trace `tme3-wm2.dmp` (similaire à celle capturée précédemment) des localisations habituelles (voir la partie 1.3.1).

1.5 Trace longue distance (*facultatif... à traiter de manière autonome si vous êtes nettement en avance par rapport au reste du groupe*)

A partir d'une trace contenant une heure de trafic longue distance entre le *Lawrence Berkeley Laboratory* et le reste du monde en janvier 1994, retrouvez des exemples de communications SMTP, POP et IMAP.

Chargez la trace `tme2-lbl.txt.gz`, soit à partir du répertoire `/Infos/lmd/2014/master/ue/ares-2014oct`, soit sur la page `http://www-rp.lip6.fr/~fourmaux/Traces/labV6.html`, vers un répertoire **local** (ex : `/tmp`)[5]. Puis à l'aide des outils UNIX standard (`awk`, `perl`, `sed`...), isolez un des flots intéressants (SMTP, POP et IMAP) et identifiez leurs caractéristiques typiques. **Ne demandez pas à votre encadrant d'aide sur ces outils, il est là pour répondre à vos questions liées au réseau**.



2 Service d'annuaire

2.1 Le système DNS (sans machine)

1. Chaque machine de l'Internet est généralement associée à un serveur de nom local et un serveur de nom de référence (*authoritative*). Quel est le rôle joué par chacun d'eux au sein du système DNS ?

2. A partir d'une machine utilisateur qui comporte un navigateur (client web) et agent de messagerie (client mail), vous souhaitez surfer sur le site web d'une institution (par exemple votre université), puis envoyer un *e-mail* vers le serveur mail de celle-ci. Quelles entités vont avoir à recourir au système DNS, et en particulier, à demander des résolutions qui impliquent le serveur de référence de l'institution ? Le serveur web et le serveur de courrier de cette institution peuvent-ils partager le même nom (par exemple `server.upmc.org`) ?

3. En surfant sur le Web, vous cliquez sur un lien menant à une page qui vous intéresse. Votre machine ne connaît pas l'adresse IP correspondant à l'URL de la page demandée et celle-ci ne se trouve pas dans le cache de votre navigateur. Si n serveurs DNS sont visités de manière **itérative** avant d'obtenir l'adresse IP recherchée, en combien de temps peut-on escompter voir apparaître la page (le temps de transmission de l'objet est négligeable) ? Faites un chronogramme pour illustrer vos réponses.

2.2 Etude manuelle d'un échange DNS (sans machine)

Le système DNS repose sur un échange de messages en mode non connecté. Voici un exemple composé de deux trames que nous vous proposons d'étudier à la main (sans Wireshark). Utilisez directement le support du lab pour entourer les différents champs sur les traces. Attention au codage des noms avec renvoi (code `0xC0`+n indiquant sur un octet la distance n en octet du début du message DNS).

2.2.1 Requête DNS

Voici une trame observée sur le réseau :

```
0000  00 07 e9 0c 90 62 00 20  ed 87 fd e6 08 00 45 00   .....b.  ......E.

0010  00 39 00 00 40 00 40 11  a9 71 84 e3 3d 7a 84 e3   .9..@.@. .q..=z..
```

[5] La taille de la trace étant particulièrement importante, si vous travaillez sur votre compte qui est monté par NFS vous obtiendrez des temps de réponse très mauvais.

```
0020  4a 02 85 05 00 35 00 25  c0 74 a0 71 01 00 00 01   J....5.% .t.q....
0030  00 00 00 00 00 00 03 77  77 77 04 6c 69 70 36 02   .......w ww.lip6.
0040  66 72 00 00 01 00 01                              fr.....
```

1. Analysez manuellement la trame ci-dessus à l'aide du support de cours.
2. Quel est le but du message contenu dans cette trame ? Quelle action de l'utilisateur a pu déclencher cette requête ?

2.2.2 Réponse DNS

Peu de temps après, on peut observer la trame suivante sur le réseau :

```
0000  00 20 ed 87 fd e6 00 07  e9 0c 90 62 08 00 45 00   . ...... ...b..E.
0010  00 cf 2a 2d 00 00 3f 11  bf ae 84 e3 4a 02 84 e3   ..*-..?. ....J...
0020  3d 7a 00 35 85 05 00 bb  a1 3b a0 71 85 80 00 01   =z.5.... .;.q....
0030  00 02 00 03 00 03 03 77  77 77 04 6c 69 70 36 02   .......w ww.lip6.
0040  66 72 00 00 01 00 01 c0  0c 00 05 00 01 00 00 54   fr...... .......T
0050  60 00 08 05 68 6f 72 75  73 c0 10 c0 29 00 01 00   `...horu s...)...
0060  01 00 00 54 60 00 04 84  e3 3c 0d c0 10 00 02 00   ...T`... .<......
0070  01 00 00 54 60 00 07 04  69 73 69 73 c0 10 c0 10   ...T`... isis....
0080  00 02 00 01 00 00 54 60  00 09 06 6f 73 69 72 69   ......T` ...osiri
0090  73 c0 10 c0 10 00 02 00  01 00 00 54 60 00 0e 06   s....... ...T`...
00a0  73 6f 6c 65 69 6c 04 75  76 73 71 c0 15 c0 4d 00   soleil.u vsq...M.
00b0  01 00 01 00 00 54 60 00  04 84 e3 3c 02 c0 60 00   .....T`. ...<..`.
00c0  01 00 01 00 00 54 60 00  04 84 e3 3c 1e c0 75 00   .....T`. ...<..u.
00d0  01 00 01 00 01 16 cb 00  04 c1 33 18 01           ........ ..3..
```

1. Analysez manuellement la trame ci-dessus.
2. Quelles informations sont renvoyées par le serveur DNS local ? Correspondent-elles à celles attendues par le client ?

2.2.3 Vérification des analyses manuelles

Seulement après avoir effectué les deux analyses manuelles ci-dessus, vérifiez les résultats à l'aide du logiciel `wireshark` sur votre poste ARI. Chargez la trace `tme3-dn1.dmp` soit à partir du répertoire `/Infos/lmd/2014/master/ue/ares-2014oct`, soit sur la page `http://www-rp.lip6.fr/~fourmaux/Traces/labV6.html`.

2.3 Le système DNS de la plateforme

Pour les besoins de la plateforme, nous avons installé un serveur DNS sur chaque VM "serveur". Celui-ci joue le rôle de serveur local, de serveur de référence et de relais. Vous trouverez ainsi sur celui-ci les informations relatives à la zone `etu`**N**`.plateforme.lan` (si vous êtes sur du poste ARI **N**) et la résolution inverse.

2.3.1 Configuration du client et du serveur DNS

1. Comment un hôte peut-il accéder au système DNS ? Faut-il utiliser un programme client ? Quels paramètres faut-il configurer ? Etudiez le fichier `/etc/resolv.conf` sur la machine client (`10.0.7.`**N**`1`) et explicitez-en les paramètres.
2. La configuration du serveur **BIND**[6] sur la VM "serveur" (`10.0.7.`**N**`3`) est visible dans le fichier `/etc/bind/named.conf.local`. Celui-ci indique les deux zones contrôlées localement :
   - **etuN.plateforme.lan** décrite dans le fichier `/etc/bind/db.etu`**N**`.plateforme.lan`
   - **N.10.in-addr.arpa** pour la résolution inverse, aussi dans le fichier `/etc/bind/db.etu`**N**`.plateforme.lan`

   Analysez le contenu de ces deux fichiers et expliquez leur utilité. Précisez ce qu'il est nécessaire de modifier si l'on souhaite déclarer une nouvelle machine sur le serveur.
3. Comment générer des échanges DNS ? Citez au moins 4 possibilités que vous testerez dans la capture suivante.

2.3.2 Capture d'échanges DNS locaux

Cette troisième capture a pour but de percevoir la nature du trafic DNS. Sur la plateforme d'expérimentation, toujours sur la topologie 1 (postes client et serveur sur le même LAN), réalisez la capture de trafic DNS à l'aide du logiciel `wireshark` :

- A partir du poste ARI **N**, connectez-vous sur les 3 VM correspondantes de la plateforme à l'aide de 3 fenêtres textuelles.
- Vérifiez que le serveur BIND (`named`) tourne sur `10.0.7.`**N**`3` (fenêtre 3)
- Démarrez la capture en lançant l'analyseur sur sur l'interface `eth1` de l'hôte `10.0.7.`**N**`2` (fenêtre 2)
- Sur la VM "client", vérifier la configuration locale du DNS et réalisez les différentes actions permettant de déclencher des requêtes DNS proposées précédemment (fenêtre 1)
- Observez la capture se réaliser dans la fenêtre de `wireshark`
- Terminez la capture. **Filtrez le trafic afin de ne conserver que celui relatif au DNS** (filtre = `dns`). Enregistrez la trace filtrée pour pouvoir la ré-utiliser ultérieurement. Ne quittez pas l'application afin de pouvoir démarrer les analyses qui suivent.

2.3.3 Analyse des échanges DNS locaux

1. Analysez les trames échangées.
2. La résolution locale modifie-t-elle les échanges DNS ?

2.4 Accès au DNS de l'Internet

Le serveur DNS de chaque PC serveur joue le rôle de serveur local pour les zones autres que **etuN.plateforme.lan**. Ce serveur n'ayant pas accès au reste de l'Internet, les requêtes vers les autres zones de l'Internet doivent être relayées vers le serveur DNS de la baie (qui a un accès vers le système DNS global).

[6] BIND *(Berkeley Internet Name Daemon)* : http ://www.isc.org/software/bind

2.4.1 Capture d'échanges DNS externe

Cette troisième capture a pour but de percevoir la nature d'un autre trafic DNS. Sur la plateforme d'expérimentation, toujours sur la topologie 1 (postes client et serveur sur le même LAN), réalisez la capture de trafic DNS à l'aide du logiciel `wireshark` :

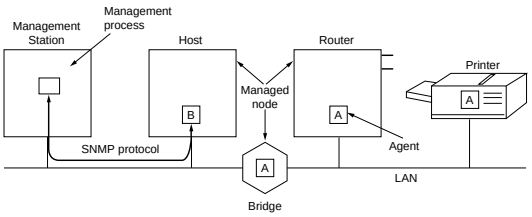
- A partir du poste ARI **N**, connectez-vous sur les 3 VM correspondantes de la plateforme à l'aide de 3 fenêtres textuelles.
- Vérifiez que le serveur BIND (`named`) tourne sur `10.0.7.`**N**3 (fenêtre 3)
- Démarrez la capture en lançant l'analyseur sur sur l'interface `eth1` de l'hôte `10.0.7.`**N**2 (fenêtre 2)
- Sur la VM client, vérifier la configuration locale du DNS, puis tapez `dig www.apple.com` (fenêtre 1)
- Observez la capture se réaliser dans la fenêtre de `wireshark`
- Terminez la capture. **Filtrez le trafic afin de ne conserver que celui relatif au DNS** (filtre = `dns`). Enregistrez la trace filtrée pour pouvoir la ré-utiliser ultérieurement. Ne quittez pas l'application afin de pouvoir démarrer les analyses qui suivent.

2.4.2 Analyse de l'échange DNS externe

1. Analysez rapidement les deux trames contenues dans la trace.
2. Expliquez le but de cet échange.
3. A votre avis, pourquoi la résolution de nom `www.apple.com` est-elle renvoyée vers des serveurs du domaine `aka*.net` ?

2.4.3 Sans la plateforme...

En cas de besoin, vous pouvez télécharger et analyser la trace `tme3-dn2.dmp` (similaire à celle capturée précédemment) des localisations habituelles (voir la partie 1.3.1).



3 Administration réseau

3.1 Exercices sur l'administration réseau (sans machine)

1. Pour un administrateur réseau, quel est l'intérêt d'utiliser des outils de gestion du réseau ? Citez plusieurs possibilités.
2. Représentez sur un schéma intégrant quelques éléments à administrer les mécanismes de bases de l'administration de réseau (éléments applicatifs, messages échangés...).
3. Définissez les termes suivants : Station d'administration, Equipement administré, Agent d'administration, Base d'information de gestion (MIB), Structure des informations de gestion (SMI) et Protocole de gestion du réseau.
4. Quels sont les PDU utilisés par SNMP ? Quels messages sont utilisés pour des requêtes/réponses ou des envois spontanés ? Quel est la différence entre ces deux types d'échanges ? Quels en sont les avantages et les inconvénients ?
5. A votre avis, pour quelles raisons utilise-t-on UDP plutôt que TCP pour le transport des PDU SNMP ?
6. Dans la suite, un administrateur souhaite gérer les routeurs du réseau de son entreprise grâce au protocole SNMP. Ce réseau fonctionne sous TCP/IP et interconnecte plusieurs réseaux locaux à l'aide de routeurs dont le service SNMP est activé.
   (a) Proposez un mécanisme pour découvrir les différentes machines présentes sur le réseau local de la station d'administration.
   (b) Expliquez comment vérifier qu'une machine est bien un routeur (la MIB-II standard définit un objet simple `ipForwarding`).
   (c) Comment obtenir le nom de ces routeurs (la MIB-II standard définit l'objet `system.sysName` de type chaîne de caractère...) ?

(d) Sachant que la MIB-II propose un objet tableau `ipAddrTable` qui référence toutes les interfaces d'une machine avec leurs paramètres IP (addresse IP, masque de réseau, adresse de diffusion...), précisez comment obtenir toutes les adresses IP (champ `ipAdEntAddr`) d'un routeur.

(e) Précisez comment modifier la valeur du masque de réseau (champ `ipAdEntNetMask`) associé à l'interface 3 d'un routeur (les entrées de l'objet table `ipAddrTable` sont indexées par le numéro de cette interface).

(f) Connaissant les informations précédentes disponibles dans la MIB-II, proposez un mécanisme général pour découvrir tous les routeurs du réseau de l'entreprise. Indiquez les limitations de votre approche.

3.2 Protocole SNMP

3.2.1 Capture de trafic SNMP

Cette dernière capture a pour but de percevoir la nature du trafic SNMP. Sur la plateforme d'expérimentation, toujours sur la topologie 1 (postes client et serveur sur le même LAN), réalisez la capture de trafic SNMP à l'aide du logiciel `wireshark` :

- A partir du poste ARI **N**, connectez-vous sur les 3 VM correspondantes de la plateforme à l'aide de 3 fenêtres textuelles.
- Vérifiez que le serveur SNMP (`snmpd`) tourne sur `10.0.7.`**N**3 (fenêtre 3)
- Démarrez la capture en lançant l'analyseur sur sur l'interface `eth1` de l'hôte `10.0.7.`**N**2 (fenêtre 2)
- Utilisez les commandes Net-SNMP (`snmpget`, `snmpgetnext`, `snmpwalk`...) sur `10.0.7.`**N**1 (fenêtre 1)
  - tapez `snmpget -v 1 -c public 10.`**N**`.1.`**N**`3 .1.3.6.1.2.1.1.1.0`
  - puis tapez `snmpgetnext -v 1 -c public 10.`**N**`.1.`**N**`3 .1.3.6.1.2.1.1.9.1.3.1`
  - puis tapez `snmpwalk -v 1 -c public 10.`**N**`.1.`**N**`3 .1.3.6.1.2.1.1.9.1.3`
  - puis tapez `snmpset -v 1 -c private 10.`**N**`.1.`**N**`3 .1.3.6.1.2.1.1.4.0 s toto@upmc.fr`
- Observez la capture se réaliser dans la fenêtre de `wireshark`
- Terminez la capture. **Filtrez le trafic afin de ne conserver que celui relatif à SNMP** (filtre = `snmp`). Enregistrez la trace filtrée pour pouvoir la ré-utiliser ultérieurement. Ne quittez pas l'application afin de pouvoir démarrer les analyses qui suivent.

3.2.2 Analyse de la première requête SNMP

1. Analysez la première trame en détaillant le mécanisme d'encodage de la couche application.
2. Quel est le but de cette requête ?
3. Qui a généré ce message ?

3.2.3 Analyse de la réponse SNMP

1. Suite à l'émission de la trame précédente, une seconde trame est émise. Analysez cette dernière.
2. Quel est le type d'équipement qui a été impliqué ?
3. A la vue de cet échange, que pensez-vous de la sécurité associée à SNMP ?

3.2.4 Analyse du deuxième échange SNMP

1. Après ce premier échange, analysez les deux trames échangées ensuite.
2. Quelle nouvelle opération est réalisée dans cet échange ? Quelles possibilités offre ce type de requête ?

3.2.5 Analyse des échanges SNMP suivants

1. Après ces deux premiers échanges, analysez les trames échangées ensuite.
2. Quelle mécanisme génère ces échanges ?

3.2.6 Analyse du dernier échange SNMP

1. Analysez ensuite la dernière trame émise par le client.
2. Quelle nouvelle opération est réalisée dans cet émission ? Quelles possibilités offre ce type de message ?

3.2.7 Sans la plateforme...

En cas de besoin, vous pouvez télécharger la trace `tme3-snm.dmp` (des localisations habituelles, voir la partie 1.3.1) pour répondre aux questions de la section 3.2.

4 Avant de quitter la salle

- Si vous avez enregistré des captures sur la VM "sonde", n'oubliez pas de les rapatrier sur votre compte utilisateur de l'ARI. Tapez : `scp root@10.0.7.N2:<ma_trace> <destination_locale>`.
- Avant de terminer vos connexions sur les équipements de la plateforme, supprimez vos fichiers et modifications effectuées afin de retrouver l'état initial.