RÉSEAUX / DOCUMENT ÉLÈVE

# S1 — Un nom, une adresse : qui répond ?

1CIEL · 1C_NET_06 · 2 h · B12 · binôme puis vérification individuelle

Nom : _____ Groupe / binôme : _____

Poste : _____ Date : ___ / ___ / ____

## Ta mission

Au cabinet Les Filaos, personne ne retient les adresses IP : on tape agenda.filaos.lan pour ouvrir le logiciel des tournées. L'infirmière demande : « Comment mon poste sait-il où est l'agenda ? Et si ça ne marche plus, qui accuse-t-on ? »

Tu dois répondre avec des preuves : la question posée, le serveur qui répond, la réponse.

Tu apprends à — lire une requête et une réponse DNS, et en retrouver la trace côté serveur.

Tu dois montrer — le serveur interrogé, le statut et la réponse de la requête, puis la ligne du journal serveur qui prouve qu'il a reçu la question.

> **TON LABO**
>
> Le labo du 1C_NET_05 : SRV-FILAOS (serveur Linux, 192.168.50.1) et PC-ACCUEIL (poste Ubuntu) sur un réseau interne isolé. SRV-FILAOS distribue déjà les adresses (DHCP) ; il héberge maintenant aussi le serveur DNS BIND9 du cabinet.
>
> Avant chaque commande, regarde l'invite : `…@srv-filaos` = serveur, `…@pc-accueil` = poste client.

## 1. Commence ici : prévoir avant de tester (sur papier)

Voici l'annuaire du cabinet tel que le serveur doit le connaître. Complète la dernière colonne avant toute commande.

| Nom demandé | Adresse enregistrée | Que doit répondre le serveur ? |
|---|---|---|
| agenda.filaos.lan | 192.168.50.20 | |
| imprimante.filaos.lan | 192.168.50.30 | |
| www.filaos.lan | alias de agenda.filaos.lan | |
| compta.filaos.lan | (aucun enregistrement) | |

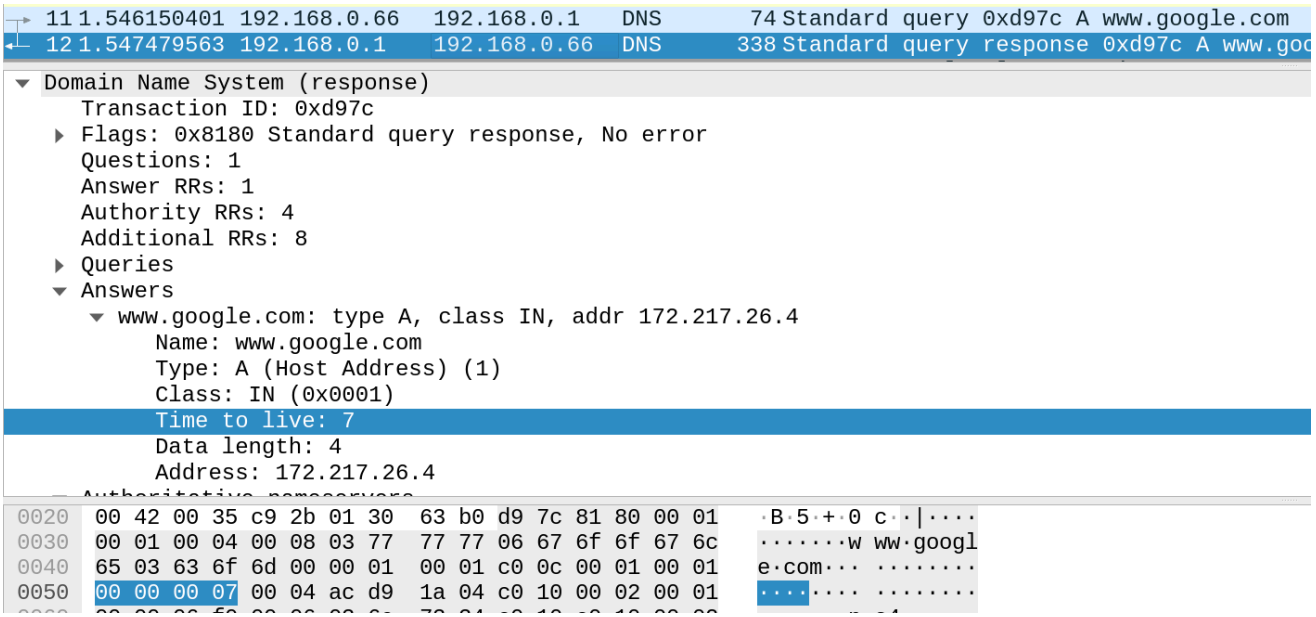
À SAVOIR — juste ce qu'il faut

Le DNS traduit un nom en adresse IP. Le poste pose une requête à un serveur DNS, qui renvoie une réponse.

Un enregistrement est une ligne de l'annuaire : A = nom → adresse IPv4 ; CNAME = alias → autre nom.

Dans ce labo, NXDOMAIN indique une réponse disant que le nom demandé n'existe pas. Vérifie le nom complet et son orthographe avant de conclure.

## Une requête et sa réponse DNS




Capture authentique historique de Wireshark, publiée par Syced le 17/07/2019. Les adresses et le nom appartiennent à cet exemple ; ce n'est pas une capture du labo B12.

À repérer : les deux lignes question/réponse, le serveur qui répond, puis le champ Answers avec le type A et l'adresse IPv4. Dans Flags, « No error » indique le statut de cette réponse.

Source : Wikimedia Commons · Syced · CC0 1.0 (ouvrir la page source).

## 2. Interroger depuis le poste (sur PC-ACCUEIL)

Poste client PC-ACCUEIL

resolvectl status | grep -i "dns server" # quel serveur DNS mon poste interroge ?
resolvectl query agenda.filaos.lan # le poste demande l'adresse de ce nom
Exemple de sortie sur un autre poste : relève le nom, l'adresse et la provenance réseau de la réponse.
agenda.filaos.lan: 192.168.50.20 -- link: enp0s8
-- Information acquired via protocol DNS in 16.9ms.
-- Data is authenticated: no; Data was acquired via local or encrypted transport: no
-- Data from: network
dig @192.168.50.1 agenda.filaos.lan # même question, posée directement au serveur

Dans la sortie de dig, trois zones comptent : la ligne status (NOERROR, NXDOMAIN…), la section ANSWER (la réponse) et la ligne SERVER (qui a répondu).

Sur PC-ACCUEIL, interroge les trois noms du tableau, puis renseigne chaque ligne :

dig @192.168.50.1 agenda.filaos.lan

dig @192.168.50.1 www.filaos.lan

dig @192.168.50.1 compta.filaos.lan

| Requête | Serveur qui répond (SERVER) | status | Réponse (ANSWER) |
|---|---|---|---|
| agenda.filaos.lan | | | |
| www.filaos.lan | | | |
| compta.filaos.lan | | | |

Compare avec ta prévision de l'étape 1 : une différence ? _____

## 3. Trouver la preuve côté serveur (sur SRV-FILAOS)

Serveur SRV-FILAOS

systemctl status named # état du service ; alias bind9 éventuel à vérifier sur cette VM

journalctl -u named -n 20 # lecture seule, si cet accès a été testé

dig @127.0.0.1 agenda.filaos.lan # le serveur s'interroge lui-même

1. Sur PC-ACCUEIL, relance dig @192.168.50.1 agenda.filaos.lan et note l'heure. Demande au professeur une trace récente du journal correspondant à ta requête. Si un accès en lecture a été testé pour ton compte, tu peux consulter le journal sur SRV-FILAOS ; en cas de refus, arrête-toi. Repère le nom, l'IP de ton poste et l'heure, puis recopie la ligne. Indique « trace fournie » si le professeur te l'a donnée._____

| |
|---|
| |
| |
| |

2. Dans cette ligne, quelle information prouve que la question vient bien de ton poste ?

_____

Question 1. Un camarade dit : « compta.filaos.lan répond NXDOMAIN, donc le serveur DNS est en panne. » Qu'en penses-tu ?

Ta réponse :

| |
|---|
| |
| |

Question 2. En 1C_NET_05, qui a indiqué à ton poste l'adresse du serveur DNS ? Quel service fait quoi ?

Ta réponse :

| |
|---|
| |

> AIDES GRADUÉES — après 10 minutes d'essai ; entoure celles que tu lis.
>
> Aide 1. Sortie trop longue ? `dig +short @192.168.50.1 agenda.filaos.lan` ne garde que la réponse (mais cache le status).
>
> Aide 2. Aucune requête visible ? Demande au professeur de vérifier le journal des requêtes et de te fournir une trace. Avec un accès lecture testé, tu peux filtrer : journalctl -u named | grep query. Les commandes privilégiées restent réalisées par le professeur.
>
> Aide 3. Pour relier poste et journal, cherche l'adresse IP de ton poste dans la ligne du journal.

## Avant le retour — relire mon travail

Coche la qualité de ta preuve. Sans essai examinable, laisse les cases vides. Le professeur note son constat séparément.

Repères de réussite

Relier une réponse à sa trace

Je montre : une ligne récente du journal correspond à ma requête par le nom, l'IP de mon poste et l'heure.

À construire : aucun rapprochement valable.

Partiel : rapprochement incomplet ou erroné.

Conforme : nom, IP et heure concordent.

Consolidé : j'explique aussi pourquoi ces repères identifient ma requête, sans confondre sa réception avec une réponse correcte.

### Validation professeur — fin de partie

| Critère observé / Ce que je montre | À construire | Partiel | Conforme | Consolidé |
|---|---|---|---|---|
| C04 — Les indicateurs de fonctionnement sont interprétés<br>Ce que je montre : Je relève le nom, le statut, la réponse et le serveur interrogé. Je rapproche la requête d'une ligne du journal par le nom, l'IP et l'heure ; cette ligne prouve la réception de la question, pas à elle seule la justesse de la réponse. | ☐ | ☐ | ☐ | ☐ |

## APPEL PROFESSEUR — OBSERVATION (individuel, 3 min)

Point à reprendre : _____.

Source : ☐ poste ☐ traces fournies.

Avant l'appel : ☐ tableaux 1 et 2 remplis ☐ ligne du journal recopiée.

Montre : tu relances une requête de ton choix ; tu montres le status, la réponse, le serveur, puis la ligne du journal correspondante.

Explique : ce que signifient NOERROR et NXDOMAIN, et comment tu relies ta requête au journal.

Élève interrogé : chacun, séparément ; le binôme ne souffle pas.

Pendant l'attente : relis ta première trace. Commence le réessai après le retour du professeur.

Le professeur consigne son constat séparément dans le suivi existant ; ton auto-évaluation ne vaut pas validation.

Après le retour du professeur, corrige ou complète sans effacer ton premier essai. Fais ensuite le nouvel item individuel ci-dessous.

Retour ciblé : _____

Date : _____ Visa du professeur : _____

> **À RETENIR**
>
> Une requête DNS se lit en trois points : qui a répondu (SERVER), quel statut (NOERROR, NXDOMAIN), quelle réponse (ANSWER).
>
> NXDOMAIN est une réponse DNS, pas une absence de réponse. Elle porte sur le nom demandé au serveur interrogé ; il faut contrôler ce nom. DHCP indique quel DNS utiliser ; DNS fournit des informations sur les noms.

### 4. Je réessaie seul

Sortie fictive relevée sur un autre poste :

Exemple fictif

;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 4102
**;; QUESTION SECTION:**
;imprimate.filaos.lan. IN A
**;; AUTHORITY SECTION:**
filaos.lan. 300 IN SOA ns1.filaos.lan. admin.filaos.lan. 2026092601 3600 900 604800 300
**;; SERVER: 192.168.50.1#53(192.168.50.1) (UDP)**

Une réponse DNS a-t-elle été reçue ? Propose une hypothèse, puis écris la requête qui permet de la tester.

Ta réponse :

| |
|---|
| |
| |