Un peu de théorie

L'histoire des communications numériques à distance est assez ancienne. Elle commence avec les signaux de fumée ou de tambour. Le début des *réseaux* numériques date concrètement de la fin du XVIII^{e} siècle avec le télégraphe de Chappe. Le télex, dans les années 1930, marque le début des communications *automatiques*. La formalisation des réseaux actuels s'est faite dans les années 1970 simultanément et en symbiose avec le développement d'Unix qui est à l'origine de GNU/Linux.

Que ce soit pour les systèmes d'exploitation dérivés d'Unix ou les réseaux, les ouvrages publiés depuis les années 1980 sont toujours d'actualité. Ainsi, Andrew S. Tanenbaum a rédigé en 1981 un livre sur les réseaux informatiques. Il a été réédité plusieurs fois[18]. Ce livre, et beaucoup d'autres, permettent de bien comprendre le fonctionnement des réseaux informatiques modernes.

Dans cette partie, nous nous proposons de présenter le minimum permettant de mettre au point un réseau opérationnel et d'en diagnostiquer les défaillances. Elle est divisée en trois chapitres :

Le chapitre I constitue une introduction sur la théorie des réseaux modernes. Le chapitre est centré sur le modèle TCP/IP. Les quatre couches sont présentées en approfondissant les parties utiles pour un réseau opérationnel. Le modèle ISO est juste mentionné. Il est certes important, mais pas très utile en pratique pour un petit réseau d'entreprise.

Le chapitre II présente quelques commandes GNU/Linux pour gérer le réseau IP. Nous ne présentons pas les commandes classiques des interpréteurs de commandes. D'autres ouvrages détaillent cela[9]. Les commandes sont regroupées pour chaque couche du modèle TCP/IP. Nous montrons comment activer une fonctionnalité et, encore plus important, comment voir l'effet produit par la commande. C'est crucial pour comprendre le fonctionnement et corriger les problèmes qui ne manqueront pas de survenir.

Le chapitre III présente la partie routage et firewall. Le noyau Linux dispose des fonctionnalités pour accomplir ces missions. Nous présentons

donc la partie routeur et surtout les quelques commandes permettant de commencer à configurer un firewall. Pour une petite entreprise, surtout qui utilise un réseau constitué de logiciels libres, le firewall pourra rester simple. Un logiciel de capture réseau permettra de valider que le comportement du firewall est bien celui attendu. Le test du type *boîte noire* avec une conclusion binaire « Ça marche » ou « Ça ne marche pas » conduit presque immanquablement à de graves déconvenues.

The words Don't Panic *are printed in large friendly letters on its cover.*
Douglas Adams

Chapitre 1

Le modèle TCP/IP

Il y a de nombreux cours sur les réseaux informatiques. Ceux-ci, très utiles, se concentrent sur chaque élément qu'ils détaillent. Nous ciblons les réseaux opérationnels. Ce sont les réseaux qui mélangent de nombreux protocoles et des logiciels spécifiques. Les problèmes mentionnés sont issus de la mise en place d'un réseau complet. Nous présentons dans cette partie les concepts utiles et essentiels pour maîtriser un réseau opérationnel. Nous expliquons les notions en les mettant en relation avec la réalité du terrain. Nous montrons aussi les différentes commandes permettant de valider chaque élément.

Il existe plusieurs types de réseaux. Les deux principaux, pour la plupart des entreprises sont les réseaux du modèle OSI et le modèle TCP/IP. Le modèle OSI est plutôt utilisé dans la téléphonie numérique chez les opérateurs. Il est aussi très utile comme fondement théorique des réseaux numériques modernes. Le modèle TCP/IP est le premier réseau utilisé par les administrateurs système et réseaux dans les petites entreprises.

Il existe de nombreux autres réseaux qui sont plus ou moins proches de ces deux modèles. Dans de nombreux cas, l'utilisation du mot *réseau* est un abus de langage. Il s'agit souvent d'une liaison numérique spécifique en point à point ou en point à multipoints. Les réseaux Wi-Fi, par exemple ne sont pas des réseaux, mais un lien utilisable pour un réseau IP.

Un *réseau* est constitué de liens et de nœuds. Pour un réseau numérique, les liens sont des liaisons établies en point à point entre deux nœuds. Les nœuds sont des routeurs ou des commutateurs qui permettent, ou non, à l'information de continuer son chemin. Les liaisons peuvent aussi être du type point à multipoints, comme avec une diffusion par les ondes hertziennes.

1.1 Les modèles théoriques

Les modèles, que ce soit le modèle OSI ou TCP/IP utilisent une description en couches. Le modèle OSI en définit sept, TCP/IP quatre. Les modèles ont été définis dans les années 1970. Ils ont de nombreuses caractéristiques communes.

Le modèle OSI a été mis en place par les opérateurs de télécommunications. Il s'agissait de définir un modèle permettant de mettre en place le réseau de télécommunications en permettant l'ajout facile de nouveaux éléments et services. Un opérateur télécoms travaille à l'échelle d'un pays et raisonnait en décennies. Le matériel télécoms était acquis pour trente ans en moyenne. En 2016, j'ai visité un central téléphonique qui était en fonctionnement depuis le début des années 1980. Les abonnés n'avaient jamais senti le besoin de changer leur abonnement depuis cette époque, l'opérateur non plus !

Le modèle TCP/IP s'est développé de manière anarchique sans qu'un état ou une multinationale n'impose ses décisions. Dans les années 1960, chaque constructeur informatique disposait d'une méthode personnelle pour interconnecter ses ordinateurs. Le nom *Internet* (Inter réseau) indique qu'il s'agissait de relier entre eux des réseaux incompatibles. Cette interconnexion s'est faite à l'initiative des utilisateurs d'ordinateurs qui souhaitaient établir des communications entre eux. L'influence de la guerre froide et la peur de subir une attaque nucléaire à conduit à la mise en place d'un réseau pouvant se reconfigurer facilement en cas de défaillance d'une partie.

Ces deux modèles sont des *modèles en couches*. C'est-à-dire que chaque élément d'une couche interagit avec son correspondant de la même couche sur l'hôte distant en utilisant uniquement les services offerts par la couche immédiatement inférieure. Cela simplifie la conception. Les couches du modèles OSI sont les suivantes :

Application c'est la couche qui interagit avec l'utilisateur.

Présentation rend la représentation des données indépendantes de l'application et de celle du réseau.

Session assure les dialogues entre deux hôtes, cette couche établi et termine les connexions.

Transport assure les transferts de données entre deux hôtes en assurant une certaine qualité de service.

Réseau assure le transport des données entre deux hôtes quelle que soit leur position.

Liaison de données met en place la communication numérique entre deux nœuds reliés physiquement.

Physique définition de communication entre un périphérique et un support de transmission.

La définition du modèle TCP/IP est voisine. Le développement de ces deux modèles a été fait à la même époque. Les concepts sont regroupés différemment dans les deux modèles. Les RFC1122 et RFC1123 (Octobre 1989) définissent quatre couches que nous présentons dans la figure 1.1 :

Application regroupe les couches application et présentation du modèle OSI.

Transport fournit le service de communication de bout en bout. Les deux principaux protocoles de cette couches sont TCP, qui assure une communication fiable, et UDP, qui fournit un transport sans connexion.

Internet ou réseau : fournit aux couches transport la communication de bout en bout sans garantie (altération, perte, duplication, perturbation de l'ordre...).

Liaison de données permet d'assurer le transfert de données structurées entre deux nœuds reliés par un support physique (ou virtuel).

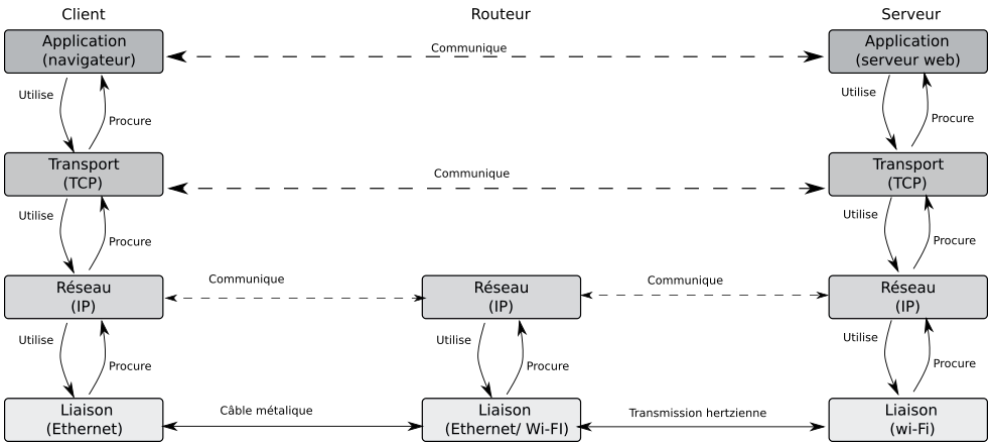

FIGURE 1.1 – Le modèle en couches : TCP/IP.

Nous allons détailler les couches du modèle TCP/IP en présentant les protocoles les plus communs. Ceci nous permettra de mettre au point, corriger et vérifier le comportement du réseau local.

1.2 La couche liaison de données

La couche liaison de données définit comment la transmission s'effectue physiquement et l'activation de la communication numérique. La transmission utilise un signal analogique. Un signal réel est transmis depuis une source vers

un ou plusieurs récepteurs. En utilisant uniquement certaines valeurs du signal analogique, il est possible de considérer qu'il s'agit d'un signal numérique. La réception de la valeur numérique consiste à mesurer le signal reçu et de décider qu'il s'agit de la valeur la plus probable. En augmentant le nombre de signaux pouvant être transmis, il est possible d'augmenter le débit binaire. Le nombre d'erreurs de transmission est alors aussi plus élevé. Une erreur peut imposer une retransmission et donc baisser le débit effectif. Un compromis doit être trouvé pour utiliser le support de transmission le plus efficace possible.

Dans le contexte d'un réseau pour une petite entreprise, le signal peut être :

électrique : Ethernet dans les câbles métalliques ;

hertzien : le Wi-Fi ou le Bluetooth ;

lumineux : dans les fibres optiques, l'infrarouge ou le Li-Fi.

Chaque support physique vient avec ses problèmes. Les câbles (métalliques ou fibres optiques) supportent difficilement les torsions, pincements et autres altérations physiques. Avec de la chance, le signal est interrompu et la conclusion est simple : il faut changer le câble. Dans d'autres cas, la défaillance du support se traduit par un taux d'erreur plus élevé que la norme. Le taux d'erreur peut aussi augmenter alors dramatiquement lorsque que la connexion est chargée. Un simple test de transmission lors de la mise en place peut se transformer en panne quand l'utilisation devient cruciale ! C'est pour cela qu'il faut valider les câbles avec les instruments adaptés.

L'accès aux câbles et aux connecteurs permet à un malfaisant d'enregistrer les signaux (réseau, clavier, écran...). Il faut donc s'assurer qu'aucun appareil n'est inséré entre deux équipements, par exemple *derrière l'ordinateur*.

Les communications utilisant un câble métallique rayonnent. Il est possible de récupérer à distance ce signal. Une fibre optique soigneusement pliée laissera le signal sortir sans couper la communication.

Pour les communications hertziennes, le support de transmission peut être perturbé. La perturbation la plus facile à mettre en évidence, c'est l'interférence avec un ou plusieurs autres signaux. Un analyseur de spectre permet de visualiser les sources parasites. Parfois ces sources ne sont pas permanentes et sont donc difficiles à détecter.

La deuxième cause de problèmes, c'est l'atténuation du signal. Le signal va perdre de l'énergie avec la distance et en traversant les obstacles. Acheter du matériel destiné au grand public est synonyme de faible coût. Malheureusement, il n'est pas aisé d'obtenir du fabricant les paramètres importants,

comme les seuils de réception. C'est l'expérience qui permettra de décider qu'en dessous d'un certain seuil, ce matériel spécifique connaîtra des problèmes de réception.

Enfin, les transmissions sont réfléchies par les obstacles. L'émetteur peut alors recevoir un écho qui va le perturber ou le récepteur va recevoir plusieurs fois le même signal.

La couche physique est une grosse source de défaillances. Si les câbles sont défectueux, alors la caractérisation de ceux-ci avec un appareil adapté permet de résoudre les problèmes. Il faut aussi protéger les câbles contre les manipulations accidentelles, en particulier par le personnel de nettoyage. De plus, c'est une cible de choix pour les malfaisants.

Le personnel de nettoyage et de gardiennage disposent de toutes les clefs de l'entreprise et est présent quand l'entreprise est déserte. La compétence technique nécessaire pour insérer un keylogger est faible. Confier ces services à une entreprise sous-traitante est un risque non négligeable.

Pour compléter la couche liaison, il faut ajouter un protocole de transmission numérique sur le support de transmission physique. Un réseau d'entreprise utilise quelques protocoles de liaison de données classiques :

Ethernet : c'est le protocole le plus utilisé sur câbles métalliques ;

Wi-Fi : c'est le protocole de liaison sans fil entre les ordinateurs ;

Modem : la liaison longue distance utilise des équipements appelés parfois abusivement modems.

Nous allons, maintenant, présenter ces trois supports physiques.

1.2.1 Le protocole local : Ethernet

Ethernet est un protocole qui commence à avoir une longue histoire chargée de rebondissement. En 2020, les équipements d'un certain âge ont un débit de 100Mb/s, voire moins. Les équipements actuels ont un débit d'1Gb/s. Des versions plus rapides existent mais sont encore peu répandues dans les petites entreprises.

Dans la plupart des cas, il faut des équipements actifs (ordinateurs, commutateurs) reliés entre eux par un câble. Pour relier deux hôtes dans deux pièces distinctes, le câble sera en fait constitué de trois parties : un câble, à l'intérieur des murs relié à deux prises murales et deux câbles reliant chaque hôte à la prise murale. Selon le standard utilisé, il faut des câbles de catégorie suffisante pour cet usage et certifier la chaîne de bout en bout.

Les interfaces Ethernet doivent posséder une adresse Ethernet ou adresse MAC. Cette adresse est composée de deux triplets d'octets, chacun représenté

par un couple de chiffres hexadécimaux. Ces couples hexadécimaux peuvent être séparés par des deux-points (`42:af:14:30:03:02`), des virgules ou pas séparés. Cette adresse peut être inscrite par un code barre sur l'emballage ou l'équipement lui-même, ce qui facilite la saisie par l'opérateur. Le premier triplet identifie le fabricant, le second identifie le composant chez ce fabricant.

Le premier triplet peut aussi définir d'autres usages, comme une adresse définie localement par l'administrateur. C'est utile, en particulier pour les machines virtuelles qui doivent avoir une adresse valide. Choisir 42 comme premier octet permet de définir une adresse locale.

Le point crucial en exploitation, c'est qu'il ne doit pas y avoir deux interfaces ayant la même adresse sur le même réseau. Ces adresses peuvent être réutilisées sur d'autres réseaux, même si c'est maladroit. Il est facile de changer l'adresse d'une interface. La sécurité ne doit donc pas reposer sur la connaissance de l'adresse.

Il est important de bien remarquer que cette adresse identifie une interface réseau, pas un ordinateur. Un ordinateur peut disposer de plusieurs interfaces, chacune avec son adresse Ethernet distincte de préférence.

1.2.2 La liaison sans fil, dont le Wi-Fi

Les transmissions sans fil utilisent principalement les transmissions hertziennes. La lumière est aussi utilisée et il est possible, mais peu courant, d'utiliser le son.

Bien que la lumière, les ondes radios, les micro-ondes et d'autres soient toutes des ondes électromagnétiques, l'ingénierie utilisée dépend fortement de la fréquence. Il est possible de les classer en trois catégories :

1. ondes radio et micro-ondes ;
2. lumière ;
3. radiation ionisantes.

Dans la première catégorie, nous retrouvons des noms qui peuvent évoquer des souvenirs (grandes ondes, petites ondes, VHF, UHF…). L'utilisation des plages de fréquences est réglementée par l'Agence Nationale des FRéquences (ANFR). Certaines bandes sont réservées à un organisme (comme l'armée) ou un usage (télévision, téléphonie…).

Certaines fréquences sont dites libres. C'est-à-dire qu'elles ne sont pas soumises à une déclaration d'utilisation ou une demande de licence. Les bandes ISM (industriel, scientifique et médical) sont des bandes de fréquences qui peuvent être utilisées dans un espace réduit pour des applications industrielles, scientifiques, médicales, domestiques ou similaires. En Europe, les bandes de