Module A - Réseautique

Préparé par Luc Baron
Le 2 septembre 2020

1 Introduction

1.1 Objectifs

Ce document a pour objectif de présenter un aperçu général du matériel, de l'architecture et des protocoles des réseaux informatiques. Il s'adresse aux futurs ingénieurs non spécialistes des réseaux. Il s'agit d'un survol des différents concepts que l'on manipule comme des blocs, sans aller en profondeur à l'intérieur de ceux-ci. Ce document est accompagné de démonstrations informatiques disponibles sous forme de capsules vidéo et d'une séance de travail pratique.

1.2 Définir quelques mots

Dans le contexte des réseaux informatiques, nous présentons les définitions suivantes :

Nom	Signification
protocole	Ensemble de règles qui déterminent la manière dont les données sont transmises dans un réseau
trame	Paquets de données véhiculés au travers d'un support physique (optique, électrique, onde)
bit	Unité de base d'information, soit 0 ou 1
octet	Ensemble de 8 bits permettant de représenter 2^8= 256 caractères différents
mémoire	Matrice de stockage d'octet de 8 bits
serveur	Ordinateur exécutant des logiciels de services pour des logiciels clients
Mbit/s	Vitesse de transmission d'un réseau en mégabits par seconde, soit 10^6 bits par seconde

2 Modèles de réseaux

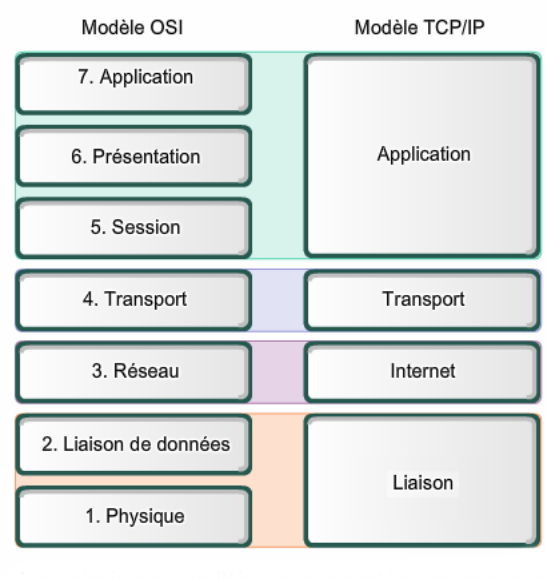
Internet est composés de matériels hétérogènes de différentes natures, vitesses, systèmes d'exploitation en provenance de différents fabricants, et pourtant, ils sont capables de communiquer entre eux. Les protocoles sont des standards de communication réseau développés afin de permettre cette interopérationalité du matérial et des logiciels. Les organismes publics supranationaux consultent les grandes entreprises du web (Microsoft, Apple, Cisco, Google et autre), afin d'établir ces standards. Les protocoles ne se situent pas tous au même niveau d'abstraction. Normaliser le codage des bits dans un câble électrique réseau est plus proche de la machine que la gestion des trajets des paquets de données. Ainsi, les protocoles ont été développés selon un modèle de réseau OSI à 7 couches, puis TCP/IP à 4 couches.

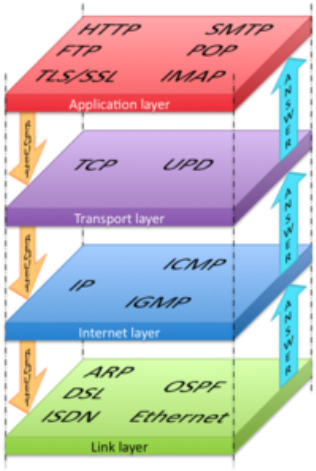
2.1 Modèle OSI

Le modèle OSI est composé de 7 couches entre le matériel physique du réseau (couche 1) jusqu'au services (couche 7) que les logiciels peuvent utiliser. Ainsi lorsqu'un navigateur Web désire obtenir un fichier d'un serveur Web distant, sa demande doit descendre de la couche 7 vers la couche 1, puis circuler sur le réseau, pour ensuite remonter dans le serveur de la couche 1 à la couche 7, puis au logiciel Web. La réponse doit suivre le chemin inverse. Nous allons décrite la fonction des 7 couches :

1. La **couche physique** s'occupe de la transmission physique des bits entre deux équipements réseau. Elle s'occupe de la transmission des bits, leur encodage, la synchronisation entre deux cartes réseau, etc. Elle définit les standards des câbles réseau, des fils de cuivre, du WIFI, de la fibre optique, ou de tout autre support électronique de transmission.
2. La **couche liaison** s'occupe de la transmission d'un flux de bits entre deux ordinateurs, par l'intermédiaire d'une liaison point à point ou d'un bus. Pour simplifier, elle s'occupe de la gestion du réseau local. Elle prend notamment en charge les protocoles MAC, ARP, et quelques autres.
3. La **couche réseau** s'occupe de tout ce qui a trait à internet : l'identification des différents réseaux à interconnecter, la spécification des transferts de données entre réseaux, leur synchronisation, etc. C'est notamment cette couche qui s'occupe du routage, à savoir la découverte d'un chemin de transmission entre récepteur et émetteur, chemin qui passe par une série de machines ou de routeurs qui transmettent l'information de proche en proche. Le protocole principal de cette couche est le protocole IP.
4. La **couche transport** permet de gérer la communication entre deux programmes, deux processus. Les deux protocoles de cette couche sont les protocoles TCP (mode interactive) et UDP (mode diffusion, tel radio, Netflix, ...).

5. La **couche session**, comme son nom l'indique, permet de gérer les connexions et déconnexions et la synchronisation entre deux processus.
6. La **couche présentation** se charge du codage des données à transmettre. Elle s'occupe notamment des conversions ou d'alignement, mais aussi du chiffrement ou de la compression des données transmises.
7. La **couche application** prend en charge les protocoles de services aux logiciels.





Modèle OSI Modèle TCP/IP Protocoles TCP/IP

L'évolution du matériel de communication réseau a permis d'obtenir des cartes réseau capables de prendre en charge les couches 1 et 2, alors que les couches 5 à 7 ont pu être regroupées en un ensemble de protocoles de haut niveau. Le réseau Internet est aujourd'hui mieux représenté par le modèle TCP/IP à 4 couches.

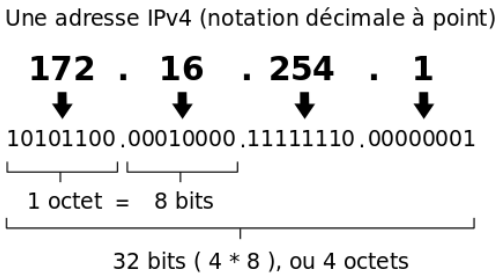
2.2 Modèle TCP/IP

Le modèle TCP/IP est composé de 4 couches :

1. La **couche liaison** prend en charge les couches 1 et 2 du modèle OSI;
2. La **couche internet** prend en charge la couche 3 réseau du modèle OSI;
3. La **couche transport** prend en charge la couche 4 transport du modèle OSI;
4. La **couche application** prend en charge les couches 5 à 7 du modèle OSI.

2.3 Adresses IPv4

Le protocole **IPv4** (Internet protocole version 4) de la couche 2 est encore aujourd'hui la version la plus largement déployée sur Internet, même si **IPv6** est prêt à être déployé. Selon ce protocole, chaque poste et équipement d'interconnexion sur Internet est identifié par une adresse IP logique unique de 4 octets de 8 bits (4 x 8 bits = 32 bits) comme dans l'exemple ci-dessous.



La conversion d'un nombre binaire en décimal se fait par :

$10101100_2 = 1 \times 2^7+0 \times 2^6+1 \times 2^5+0 \times 2^4+ 1 \times 2^3+1 \times 2^2+0 \times 2^1+0 \times 2^0= 172_{10}$

3 Protocoles de la couche application

L'usage du mot *serveur* est en général double. Il désigne un poste informatique physique performant offrant des services à plusieurs usagers. Il désigne aussi un logiciel de service spécifique utilisant différents protocoles de la couche 4 application, tels que HTTP, SSH, SFTP, ..., et qui s'exécute sur un serveur physique. Ainsi, un serveur physique peut exécuter le logiciel de service Web Appache qui

utilise le protocole HTTP, et aussi, exécuter un logiciel de service SFTP, afin de permettre le transfert de fichiers avec le serveur physique. Nous décrivons ci-dessous les principaux protocoles de la couche 4 *Application* du modèle de réseau TCP/IP.

3.1 VPN

Le protocole **VPN** (Virtual Private Network) permet de construire un canal de communication privé, c'est-à-dire encodé à travers internet entre un poste client et un réseau distant privé. Le serveur VPN sur le réseau distant attribue alors une adresse IP logique au poste client comme s'il était présent dans le réseau privé. Le serveur VPN du réseau privé de Polytechnique se nomme *ssl.vpn.polymtl.ca* et permet l'attribution d'adresse IPv4 du type 10.10.xx.xx avec les deux serveurs DNS 132.207.144.3 et 132.207.144.3

3.2 DHCP

Le protocole **DHCP** (Dynamic Host Configuration Protocol) permet à un ordinateur qui désire se connecter nouvellement à un réseau informatique d'obtenir dynamiquement une adresse IP unique et la configuration du réseau. Lorsque le mode DHCP est désactivé, c'est à l'usager de décrire manuellement la configuration du réseau dans les paramètres de la carte réseau. Il doit aussi inscrire une adresse IP, dite *statique*, qui n'est pas déjà utilisée par un autre poste, ni réservée dans la liste des adresses gérées par le serveur DHCP, sinon il y aura possiblement des collisions. Lorsque le mode DHCP est activé, le poste diffuse sur le segment (domaine de diffusion) de son nouveau réseau une demande de configuration selon le protocole DHCP. S'il existe un serveur DHCP à l'écoute, il lui répond en lui assignant une adresse IP non utilisée et la configuration du réseau qui inclut l'adresse du serveur DNS et de la passerelle de sortie. Habituellement, les adresses IP sont louées selon des baux de 24 heures renouvelables par le serveur DHCP.

3.3 Telnet/SSH

Les protocoles **Telnet** et **SSH** (Secure SHell) permettent tous deux l'envoi de commandes et l'affichage des réponses entre un poste client et un poste distant à travers un réseau. L'interface est habituellement une simple console, souvent appelé terminal, où l'on utilise le clavier du poste client pour entrer une commande qui est envoyée au poste distant. Ce dernier exécute la commande et retourne au poste client la réponse pour affichage. Les terminaux peuvent être du matériel physique spécialisé ou une simple fenêtre terminale sur votre ordinateur. La version Telnet est un protocole non sécurisé, alors que la version SSH est un protocole sécurisé. Plusieurs exemples d'utilisation du protocole Telnet sont présentés à la section 5.1 et SSH à la section 5.2.

3.4 FTP/SFTP

Les protocoles **FTP** (File Transfer Protocol) et **SFTP** (Secure File Transfer Protocol) permettent tous deux le transfert de fichier bidirectionnel entre un poste client et un poste distant à travers un réseau. L'interface peut être une simple console où l'on utilise le clavier du poste client pour entrer des commandes, telles que PUT qui permet d'envoyer un fichier vers le poste distant ou GET qui permet de recevoir un fichier du poste distant. Ce dernier exécute la commande et retourne au poste client la réponse pour affichage. Il faut utiliser la notion de répertoire de travail sur le poste client et le poste distant. L'interface peut aussi être un logiciel client graphique facilitant les transferts avec les déplacements de la souris. Sur Windows, le logiciel SSH Secure Shell Client est disponible gratuitement et est du domaine public. Sur MacOS, la fenêtre terminal permet de le faire gratuitement avec des commandes. Les logiciels clients graphiques sont nombreux, mais payants. La version FTP est un protocole non sécurisé, alors que la version SFTP est un protocole sécurisé.

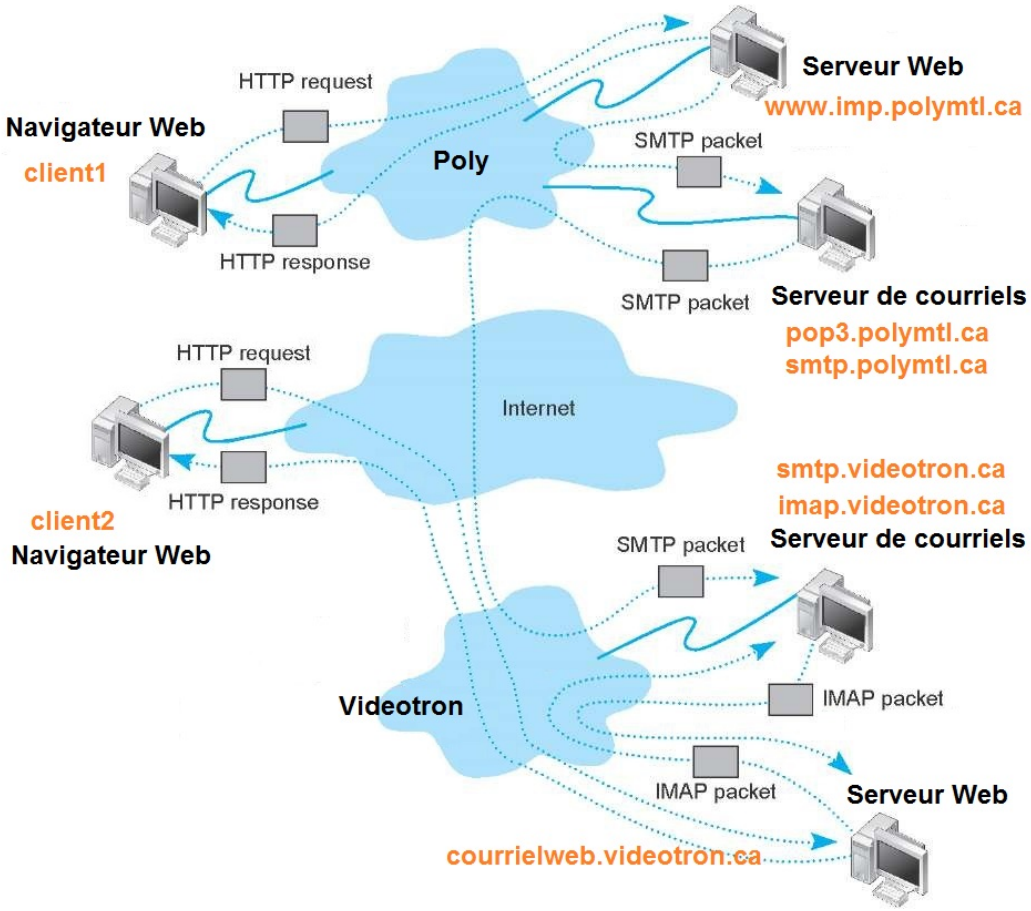
3.5 HTTP/HTTPS

Les protocoles **HTTP** (HyperText Transfer Protocol) et **HTTPS** (HyperText Transfer Protocol Secure) permettent tous deux l'échange de fichiers (principalement XHTML/HTML et images) entre le navigateur d'un poste client et un serveur Web d'un poste distant à travers un réseau. Selon ces protolocles, lorsque l'usager clic sur un hyperlien, le navigateur demande accès à cette ressource sur le serveur Web via son URL. Le serveur Web envoie alors le fichier demandé à travers le réseau au navigateur qui lui s'occupe de son affichage selon qu'il s'agit de code XHTML/HTML ou de scripts Java. Si la ressource demandée est un fichier PHP, le serveur Web demande au serveur PHP d'exécuter le code PHP avant d'envoyer le résultat au navigateur. Dans ce cas, jamais ce dernier ne reçoit le code source PHP. Par défaut, les navigateurs Web s'attendent à utiliser le protocole HTTP, c'est pourquoi il n'est pas nécessaire d'inscrire http:// dans le URL. Les navigateurs sont, cependant, capables d'utiliser d'autres protocoles, tels que ftp:// ou même smb://, si on les spécifie explicitement. La version HTTP est un protocole non sécurisé, alors que la version HTTPS est un protocole sécurisé.

3.6 POP/IMAP/SMTP

Les protocoles **POP** (Post Office Protocole), **IMAP** (Internet Message Acces Protocol) et **SMTP** (Simple Mail Transfer Protocol) sont tous des protocoles permettant de discuter directement avec un serveur de courriels.

- Le protocole POP permet de récupérer directement ses courriels d'un serveur de courriel. Dans ce mode, les courriels sont entièrement téléchargés dans le poste du client et retirés du serveur. Ce mode permet de libérer rapidement du serveur les courriels des usagers, mais les courriels ne sont alors plus disponibles de façon centralisée. Il existe en version POP2 et POP3.
- Le protocole IMAP permet, tout comme le protocole POP, de consulter ses courriels sur un serveur, mais offre beaucoup plus de possibilités. Il est possible de laisser ses courriels en dépôt sur le serveur, et ainsi permettre des accès simultanés. Il permet également de gérer plusieurs boîtes de courriels et d'en trier le contenu.
- Le protocole SMTP permettant d'acheminer directement un message courriel d'un serveur de courriel à un autre. Les pare-feu filtrent habituellement les trames SMTP sortantes dont l'origine n'est pas autoriée. Par exemple à Polytechnique, *smtp.polymtl.ca* et *cogito.meca.polymtl.ca* peuvent émettre des trames SMTP sortantes.



Envoi d'un courriel de client1@polymtl.ca à client2@videotron.ca

La figure précédente illustre la situation où client1@polymtl.ca désire envoyer un message à client2@videotron.ca.

Client1 utilise un navigateur avec le protocole HTTP pour se connecter au serveur Web *www.imp.pomtl.ca* de Polytechnique pour composer son message. Lorsqu'il appuie sur envoyé, le serveur Web utilise alors le protocole SMTP pour transmettre le message au serveur *smtp.polymtl.ca*, et ce dernier envoie la trame SMTP à travers Internet jusqu'au serveur *smtp.videotron.ca*.

Client2 est quelque part sur Internet. Il utilise un navigateur avec le protocole HTTP pour se connecter au serveur Web *courrielweb.videotron.ca*. Il demande de consulter sa boîte de messages. Le serveur Web utilise alors le protocole IMAP pour demander les messages au serveur *imap.videotron.ca*, ce dernier lui retour les messages avec le protocole IMAP. Le serveur *courrielweb.videotron.ca* construit alors l'affichage de la réponse en HTML qu'il envoi avec le protocole HTTP au navigateur de cilent2. Finalement, le navigateur Web du client2 affiche le fichier HTML qui contient le message reçu de client1.

Le parcours est très long parce que les deux utilisateurs ne communiquent pas directement avec leur serveur de courriels en utilisant les protocoles IMAP et SMTP, ils préfèrent utiliser HTTP avec un navigateur Web. Alternativement, le client1 aurait pu utiliser un logiciel de messagerie, tel qu'Outlook de Microsoft, Mail de MacOS ou Thunderbird (gratuiciel ou Free ware) pour envoyer son message. Une fois configuré, ces logiciels permettent de communiquer directement avec les serveurs *imap.polymtl.ca* et *smtp.polymtl.ca* de Polytechnique, ou de Videotron, ce qui peut alléger grandement la quantité de données échangées.

4 Matériels et architecture

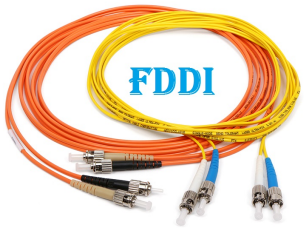
Selon le modèle de réseau TCP/IP à 4 couches, nous décrivons ci-dessous le matériel couramment utilisé pour implanter un réseau local (Local Area Network ou LAN) ou un réseau étendu (Wide Area Network ou WAN). Les numéros de couche indiqués sont ceux du modèle TCP/IP à 4 couches.

4.1 Technologies de liaison (couche 1)

Les quatre principales technologies de *liaison* de la couche 1 pour la transmission des données sur les réseaux informatiques sont :

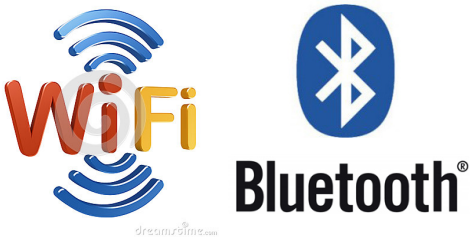
1. **FDDI (Fiber Distributed Data Interface)** : la technologie FDDI utilise des signaux de lumière pour transmettre des données à des vitesses extrêmement élevées (plusieurs Gbit/s) sur un réseau local ou à de grande distance. Elle repose sur des amplificateurs optiques, des lasers ou LED, et sur le multiplexage par répartition des ondes pour transmettre de grandes quantités de données à travers des câbles à fibres optiques;

2. **Ethernet** : la technologie Ethernet utilise des signaux électriques pour transmettre des données à très hautes vitesses sur des distances de moins de 100 m. Elle repose principalement sur des fils électriques à paires torsadées de type 10Base-T, 100Base-T et 1000Base-T pour transmettre des données sur un réseau local à des vitesses jusqu'à 1 Gbit/s;
3. **Wi-Fi** : la technologie Wi-Fi utilise des ondes radio pour transmettre des données à hautes vitesses dans un espace sans fil sur des distances de moins de 30 m. Elle repose sur la norme IEEE 802.11a/b/g/n/ac. La version IEEE 802.11b peut atteindre 11 Mbit/s jusqu'à 20 m, alors que la version IEEE 802.11g peut atteindre 54 Mbit/s jusqu'à 35 m;
4. **Bluetooth** : la technologie Bluetooth utilise des ondes courtes pour transmettre des données à bonnes vitesses sur de courtes distances. La majorité des téléphones, tablettes et ordinateurs sont de classe 2 avec une puissance de 2,5 mW et une distance maximale de 10 m.



Fibre optique

Câble RJ-45



Technologies sans-fil à portées différentes

Le protocole **ARP** (Address Resolution Protocol) fonctionne au niveau de la couche 1 *liaison*. Il permettant d'obtenir l'adresse physique MAC d'une interface réseau à partir de son adresse IP logique. Par exemple, obtenir l'adresse physique 00-22-4D-51-40-35 à partir de l'adresse IP logique 192.168.0.135 .

4.2 Matériels d'interconnexions

4.2.1 Concentrateur (couche 1)

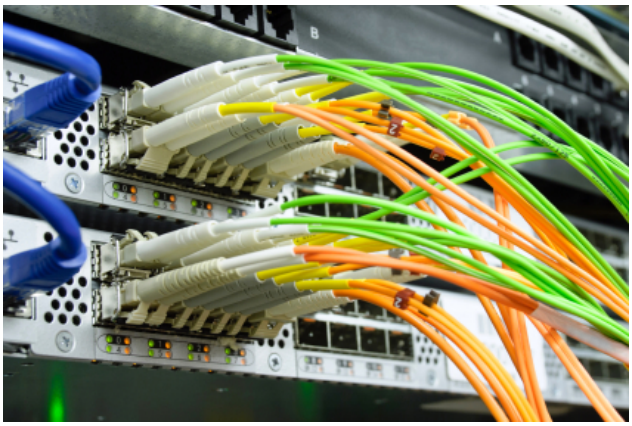
Le concentrateur (hub) fonctionne au niveau de la couche 1 *liaison* d'un réseau local. Il permet la connexion physique des câbles à fibre optique ou Ethernet. Chaque équipement attaché au concentrateur partage alors le même domaine de diffusion (appelé segment), ainsi que le même domaine de collision. Comme dans tout segment de réseau Ethernet, un seul poste peut transmettre à la fois. Dans le cas contraire, une collision se produit, les postes concernées doivent retransmettre leurs données après avoir attendu un temps calculé aléatoirement par chaque émetteur. C'est comme une route municipale à 1 voie dans chaque direction où les voitures (trames) doivent faire la file dans le trafic vers leur destination. La densité de trafic cause fréquemment des collisions.

4.2.2 Commutateur (couche 1)

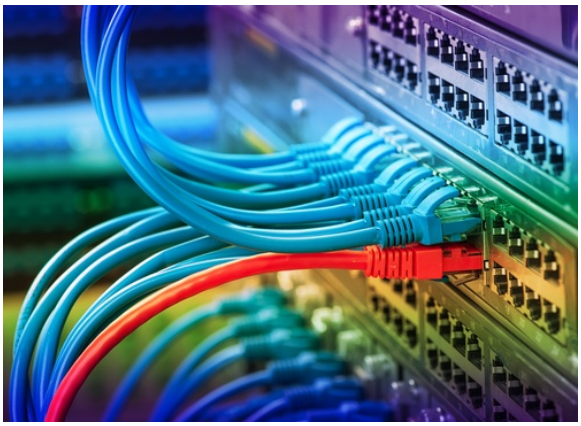
Le commutateur (switch) fonctionne au niveau de la couche 1 *liaison* d'un réseau local comme le concentrateur. Il permet aussi la connexion physique des câbles à fibre optique ou Ethernet. Il est souvent utilisé pour remplacer un concentrateur, car il permet de réduire les collisions de données. Contrairement à un concentrateur, il n'envoie pas, sur tous les ports, toutes les trames de données reçues. En utilisant le protocole ARP, il construit plutôt dynamiquement une table permettant d'associer l'adresse physique MAC de destination des trames et le port de destination. Ainsi, il peut acheminer directement les données vers le port de destination sans encombrer les autres ports. C'est comme une route régionale à quelques voies dans chaque direction où les voitures peuvent changer de voie vers leur destination. Les collisions sont moins fréquentes puisqu'elles ne se produisent que lors des changements de voie.

4.2.3 Routeur (couche 2)

Le routeur (router) fonctionne au niveau de la couche 2 *internet* d'un réseau local LAN ou étendu WAN. Il permet aussi la connexion physique des câbles à fibre optique ou Ethernet. Il assure le routage des trames de données selon le trafic actuel et la destination. Ainsi, il interroger les autres routeurs afin d'obtenir les adresses IP des chemins vers la destination. Il peut également utiliser le protocole DNS pour obtenir des adresses IP pour mettre à jour ses tables de routage. Le routeur est l'équivalent d'un ordinateur gérant plusieurs connexions réseau (les anciens routeurs étaient d'ailleurs des ordinateurs). Certains peuvent également avoir la fonction de pare-feu (firewall), de serveur DNS et/ou de serveur DHCP. C'est comme une autoroute à plusieurs voies dans chaque direction où les voitures peuvent changer de voie vers leur destination. Les collisions sont encore moins fréquentes puisque toutes les voitures utilisent un GPS intelligent capable d'ajuster le trajet à destination selon le trafic, et ainsi, réduire les temps de transport.



Routeur à fibre optique

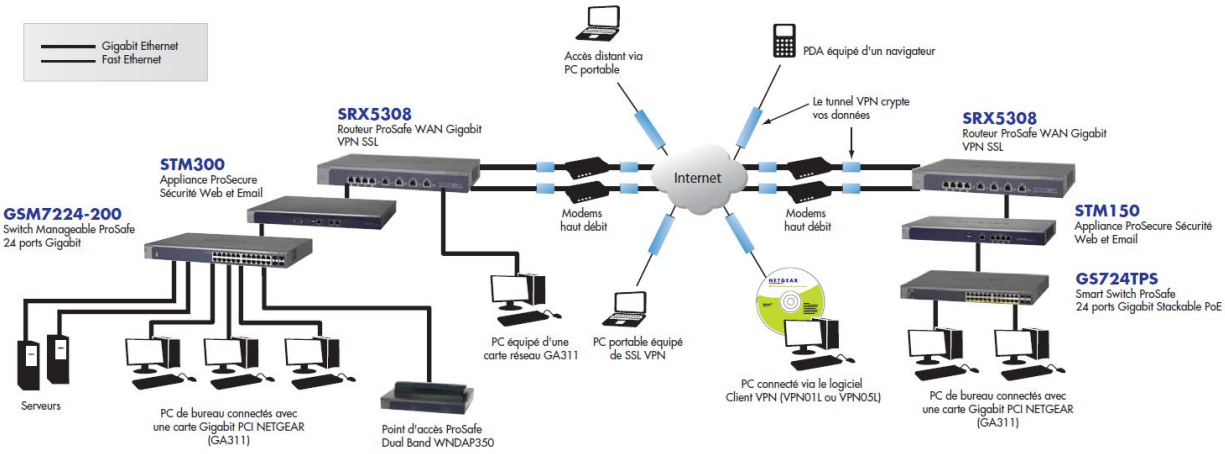


Commutateur Ethernet à câbles RJ-45

Le protocole **DNS** (Domain Name System) fonctionne au niveau de la couche 2 *internet*. Il permettant de traduire les noms de domaine et adresses IP symboliques en adresse IP logique. Par exemple, le serveur DNS de Polytechnique (ns1.polymtl.ca) permet d'obtenir l'adresse IP logique 132.207.6.35 à partir de l'adresse symbolique www.polymtl.ca.

4.3 Architecture d'un réseau étendu

Nous observons ci-dessous l'architecture d'un réseau étendu (Wide Area Network ou WAN). Le nuage central représente le réseau mondial Internet. À gauche et à droite, nous avons 2 réseaux locaux LAN chacun relié à Internet par 2 modems haut débit. Ces 2 LAN forment ensemble un WAN avec chacun de son côté un routeur WAN permettant de gérer des canaux VPN (Virtual Private Network). Chacun des routeurs est relié à un pare-feu (STM300/STM150) qui filtre les données courriels contre les virus et les sources malveillantes selon des règles prédéfinies. Ils filtrent également les communications Web entre un navigateur client et un serveur. Finalement, les serveurs, les postes de travail et les équipements réseaux partagés sont reliés directement à un commutateur qui lui-même est relié au pare-feu.



Réseau étendu WAN déployé sur deux sites éloignés à travers Internet

En raison de la présence des pares-feu et des routeurs avec VPN, les deux portions du WAN, bien que physiquement éloignées, peuvent communiquer entre elles comme si elles étaient situées dans un même lieu. Les usagers mobiles peuvent se connecter au WAN avec un téléphone intelligent, une tablette ou un ordinateur avec un VPN. Les liaisons indiquées en bleu sont des tunnels VPN.

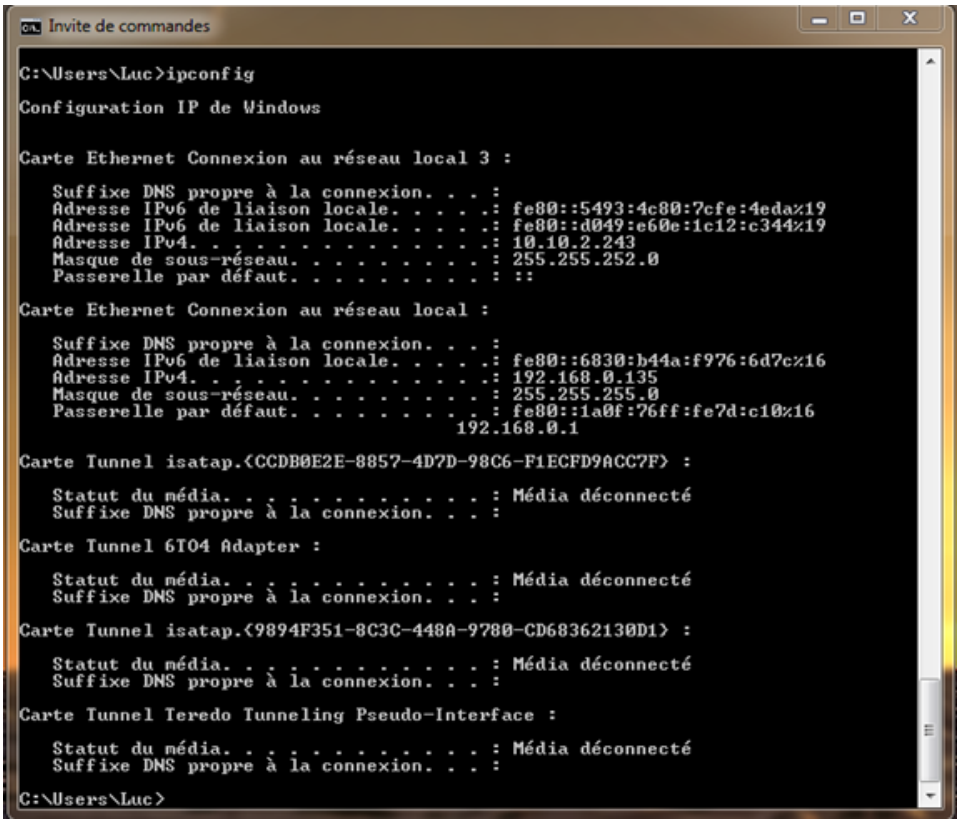
5 Aller à la découverte

5.1 Postes Windows

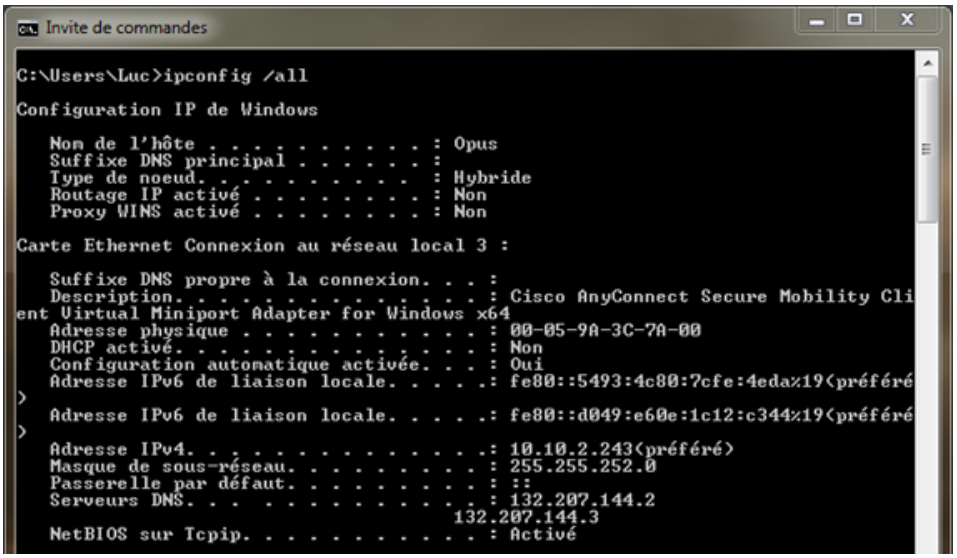
Sur un poste Windows, démarrer la console par le menu *Démarrer*, puis faites une recherche avec *CMD*, afin d'obtenir la console de commande.

5.1.1 Commande ipconfig /all

Utiliser la commande *ipconfig*, afin d'obtenir la configuration réseau de votre poste de travail, comme ci-dessous.



Les deux cartes Ethernet sont actives et possèdent des adresses IPv4, alors que les quatre cartes tunnel suivantes sont déconnectées. Utilisons maintenant, la même commande avec le paramètre */all*, afin d'obtenir plus d'information.



La première carte réseau est de technologie Ethernet. Elle se nomme *Cisco AnyConnect Secure Mobility Client Virtual Miniport Adapter*. C'est une carte virtuelle qui n'existe pas physiquement dans ce poste de travail. Elle porte le nom du client VPN (Cisco AnyConnect) que Polytechnique demande d'utiliser pour se connecter à distance à son réseau informatique privé. Une fois la connexion VPN démarrée, Cisco AnyConnect installe cette carte réseau virtuelle. On constate que cette carte possède l'adresse physique *00-05-9A-3C-7A-00*, a obtenue l'adresse IPv4 logique *10.10.2.243* et que les serveurs DNS du réseau privé de Polytechnique sont *132.207.144.2* et *132.207.144.3*. Ce canal VPN permet l'accès à distance aux ressources informatiques de Polytechnique comme si vous y étiez physiquement présent. Observons maintenant la suite de la réponse.

```
Carte Ethernet Connexion au réseau local :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Intel(R) 82579V Gigabit Network Conn
ection
   Adresse physique . . . . . . . . . . . : 00-22-4D-51-40-35
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::6830:b44a:f976:6d7c%16(préféré
)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.0.135(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : 27 août 2020 00:08:50
   Bail expirant. . . . . . . . . . . . . : 6 septembre 2020 12:08:54
   Passerelle par défaut. . . . . . . . . : fe80::1a0f:76ff:fe7d:c10%16
                                            192.168.0.1
   Serveur DHCP . . . . . . . . . . . . . : 192.168.0.1
   IAID DHCPv6 . . . . . . . . . . . . . . : 184558157
   DUID de client DHCPv6. . . . . . . . . : 00-01-00-01-1E-D1-51-16-00-22-4D-51-40
-35
   Serveurs DNS. . . . . . . . . . . . . . : 192.168.0.1
   NetBIOS sur Tcpip. . . . . . . . . . . . : Activé
```

La deuxième carte réseau est aussi de technologie Ethernet. Elle se nomme *Intel(R) 82579U Gigabit Network Connection*. Cette carte possède l'adresse physique *00-22-4D-51-40-35* et a obtenue l'adresse IPv4 logique *192.168.0.135*. On note également que la passerelle, les serveurs DHCP et DNS possèdent la même adresse logique IPv4 *192.168.0.1*. En faîte, c'est le routeur du réseau local qui effectue le travail de passerelle, de serveur DHCP et de serveur DNS. Ce poste informatique a donc deux cartes réseaux: une première virtuelle pour le canal VPN vers Polytechnique, et une seconde réelle sur le réseau local.

5.1.2 Commande ping sous Windows

Utiliser la commande *ping*, afin d'obtenir l'aide sur l'utilisation de la commande *ping*, comme ci-dessous.

```
Invite de commandes

C:\Users\Luc>ping

Utilisation : ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
              [-r count] [-s count] [[-j host-list] | [-k host-list]]
              [-w timeout] [-R] [-S srcaddr] [-4] [-6] nom_cible

Options :
    -t             Envoie une requête Ping à l'hôte spécifié jusqu'à arrêt.
                   Pour afficher les statistiques et continuer, tapez Ctrl+Att.
                   Pour arrêter, tapez Ctrl+C.
    -a             Résout les adresses en noms d'hôtes.
    -n count       Nombre de demandes d'écho à envoyer.
    -l size        Taille du tampon d'envoi.
    -f             Active l'indicateur Ne pas fragmenter dans le paquet (IPv4
                   uniquement).
    -i TTL         Durée de vie.
    -v TOS         Type de service (IPv4 uniquement. Cet indicateur est fourni
                   à des fins de compatibilité descendante seulement. La
                   configuration de ce paramètre n'a aucun effet sur le type
                   de service dans l'en-tête IP).
    -r count       Itinéraire d'enregistrement du nombre de sauts (IPv4
                   uniquement).
    -s count       Datage du nombre de sauts (IPv4 uniquement).
    -j host-list   Itinéraire source libre parmi la liste d'hôtes (IPv4
                   uniquement).
    -k host-list   Itinéraire source strict parmi la liste d'hôtes (IPv4
                   uniquement).
    -w timeout     Délai d'attente pour chaque réponse, en millisecondes.
    -R             Utiliser l'en-tête de routage pour tester également
                   l'itinéraire inverse (IPv6 uniquement).
    -S srcaddr     Adresse source à utiliser.
    -4             Forcer l'utilisation d'IPv4.
    -6             Forcer l'utilisation d'IPv6.

C:\Users\Luc>
```

La commande *ping* doit se terminer par le *nom_cible* de l'équipement réseau que l'on désire obtenir l'adresse logique IPv4, ainsi que vérifier le temps de transport aller-retour d'un paquet de données. Les paramètres entre [...] sont optionnels. Le paramètre *-n* (valeur par défaut de 4) permet de choisir le nombre de répétitions des envois. Le paramètre *-l* (valeur par défaut de 32 octets) permet de choisir la grandeur des paquets de données. Utilisons maintenant la commande *ping* avec 6 répétitions et des paquets de 4096 octets.

```
Invite de commandes

C:\Users\Luc>ping -n 6 -l 4096 www.polymtl.ca

Envoi d'une requête 'ping' sur www.polymtl.ca [132.207.6.35] avec 4096 octets de
 données :
Réponse de 132.207.6.35 : octets=4096 temps=19 ms TTL=64
Réponse de 132.207.6.35 : octets=4096 temps=28 ms TTL=64
Réponse de 132.207.6.35 : octets=4096 temps=15 ms TTL=64
Réponse de 132.207.6.35 : octets=4096 temps=16 ms TTL=64
Réponse de 132.207.6.35 : octets=4096 temps=22 ms TTL=64
Réponse de 132.207.6.35 : octets=4096 temps=27 ms TTL=64

Statistiques Ping pour 132.207.6.35:
    Paquets : envoyés = 6, reçus = 6, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 15ms, Maximum = 28ms, Moyenne = 21ms

C:\Users\Luc>
```

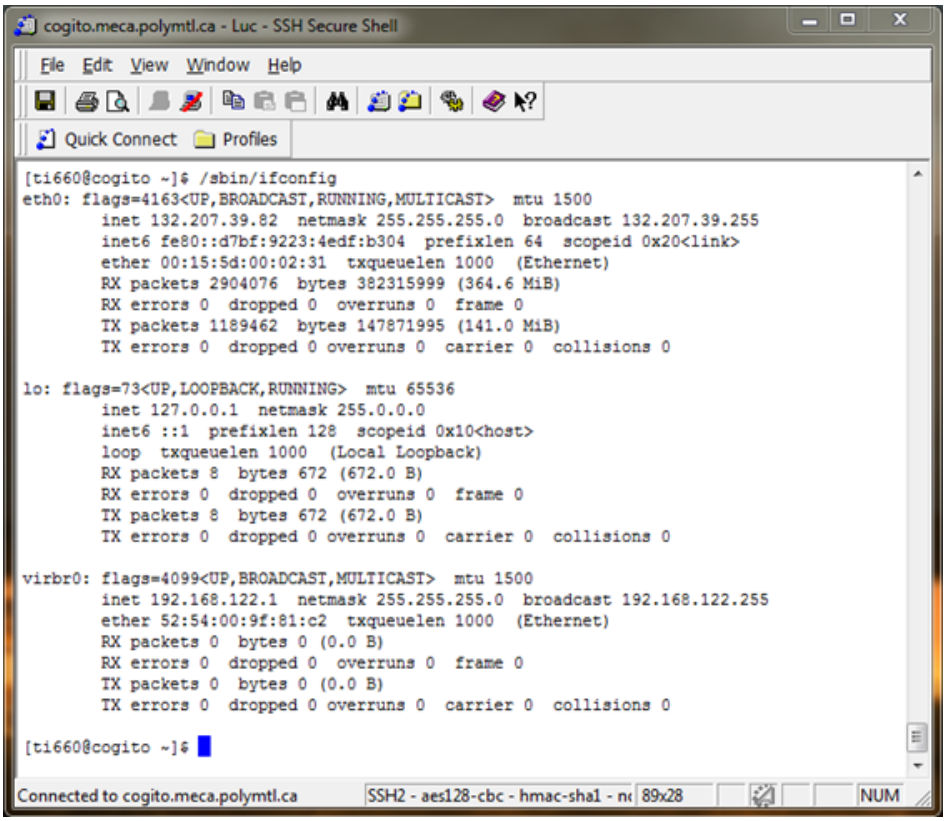
La commande *ping* interroge le serveur DNS et obtient l'adresse logique IPv4 *132.207.6.35* correspondant à *www.polymtl.ca*. Le temps moyen de transit aller-retour des paquets avec ce serveur est de 21 ms, donc le temps moyen de transport aller seulement est de 21 ms / 2 = 10,5 ms = 0,0105 seconde. Puisque les octets sont formés de 8 bits, alors l'envoi se fait à la vitesse de (4 096 octets x 8 bits/octet) / 0,0105 s = 3 120 762 bits/s = 3,1 Mbit/s. Les temps de transit sont très variables, puisqu'ils dépendent du trafic à l'instant de la mesure et de la distance à parcourir sur internet.

5.2 Postes Unix/Linux/MacOS

Les commandes décrites dans cette section peuvent être exécutées sur des postes Unix, Linux ou MacOS. Nous utilisons le poste Linux *cogito.meca.polymtl.ca* pour illustrer le résultat.

5.1.1 Commande /sbin/ifconfig

Utiliser la commande */sbin/ifconfig*, afin d'obtenir la configuration réseau du poste Linux, comme ci-dessous.

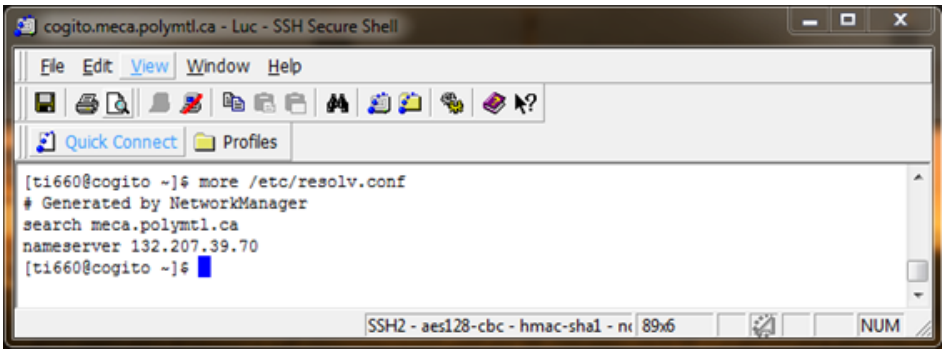


Il y a trois cartes réseau dans ce poste Linux:

- La première carte *eth0* est de technologie Ethernet. Elle est active (RUNNING) et possèdent une adresse logique IPv4 *132.207.39.82*. Puisqu'il s'agit d'un serveur accessible à plusieurs utilisateurs, son adresse IPv4 doit certainement être statique, c'est-à-dire fixée par configuration manuelle plutôt que par DHCP. Il n'est évidemment pas pratique que l'adresse IPv4 d'un serveur change continuellement.
- La deuxième carte *lo* est la boucle de retour vers le poste lui-même qui est disponible sur tous les postes Unix, Linux et MacOS. Elle est active (RUNNING) et possèdent l'adresse réservée IPv4 *127.0.0.1*. Elle est utile lors que les logiciels client et serveur sont tous les deux installés sur le poste et qu'ils doivent communiquer par le réseau.
- La troisième carte *virbr0* est de technologie Ethernet. Elle n'est pas active (pas de RUNNING) et possède l'adresse locale IPv4 *192.168.122.1*. Elle est probablement virtuelle (virbr = virtual board??) et utilisée par les *sysadmin* pour l'entretien du serveur.

5.2.2 Fichier /etc/resolv.conf

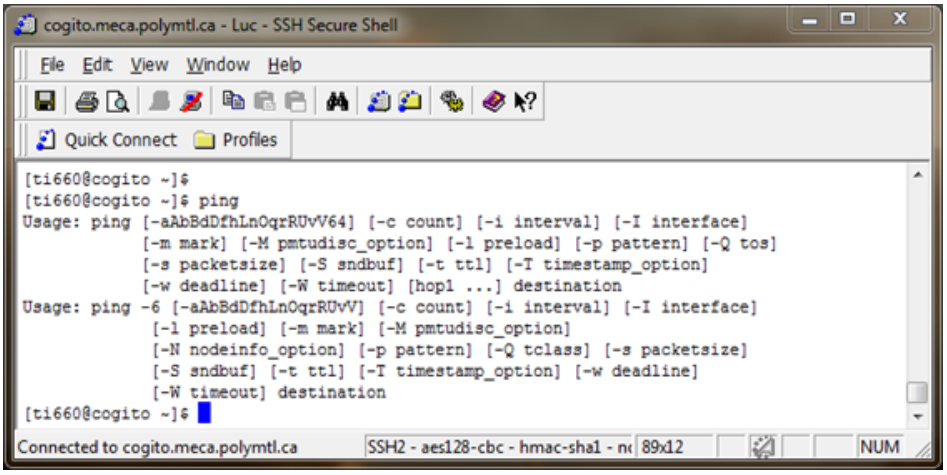
Le fichier */etc/resolv.conf* contient l'adresse IPv4 du serveur DNS utilisé par ce poste Unix. Utiliser la commande *more* afin d'afficher le contenu de ce fichier texte, comme ci-dessous.



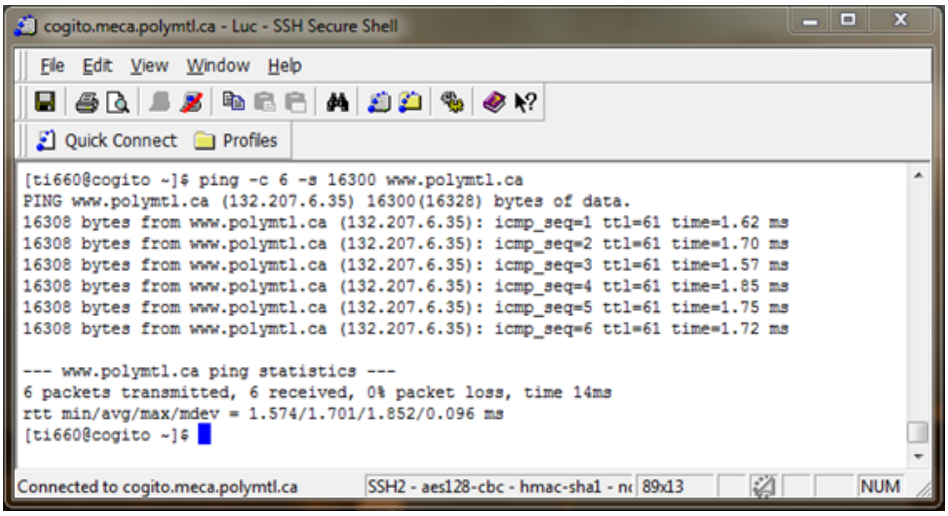
Ce poste recherche le nom des autres postes du sous-réseau *meca.polymtl.ca* avec le serveur DNS *132.207.39.70*. Noter que ce fichier est généré automatiquement par le gestionnaire de configuration réseau comme l'indique le commentaire à la ligne 1. Modifier ce fichier ne permet donc plus de modifier la configuration DNS de ce poste.

5.2.3 Commande ping sous Unix

Utiliser la commande *ping*, afin d'obtenir l'aide sur l'utilisation de la commande *ping*, comme ci-dessous.



Sous Unix, il existe deux versions de la commande *ping*, c'est-à-dire une version pour IPv4 et une pour IPv6 en sélectionnant le paramètre *-6*. La commande *ping* doit se terminer par la *destination* de l'équipement réseau que l'on désire obtenir l'adresse logique IP, ainsi que vérifier le temps de transport aller-retour d'un paquet de données. Les paramètres entre [...] sont optionnels. Attention, sous Unix les paramètres ne sont pas identiques à ceux sous Windows. Le paramètre *-s* (valeur par défaut de 64 octets) permet de choisir la grandeur des paquets de données. Le paramètre *-c* (par défaut de valeur infini) permet de choisir le nombre de répétitions des envois. Si vous ne fixez pas ce paramètre, la répétition sera infinie ou jusqu'à ce que vous fassiez un ^C (ctrl-C). Utilisons maintenant la commande *ping* avec 6 répétitions et des paquets de 16 300 octets. Noter que la commande ajoute 8 octets à la grandeur demandée.



La commande *ping* interroge le serveur DNS et obtient l'adresse logique IPv4 *132.207.6.35* correspondant à *www.polymtl.ca*. Le temps moyen de transit aller-retour des paquets avec ce serveur est de 1,701 ms, donc le temps moyen de transport aller seulement est de 1,701 ms / 2 = 0,8505 ms = 0,0008505 seconde. Puisque les octets sont formés de 8 bits, alors l'envoi se fait à la vitesse de (16 308 octets x 8 bits/octet) / 0,0008505 s = 153 396 825 bits/s = 153,4 Mbit/s. Dans cet exemple, les temps de transit sont beaucoup moins

variables et très courts, parce que cogito est situé dans la salle des serveurs, à proximité du serveur *www.polymtl.ca*. Noter que sous Unix, les temps de transit sont mesurés au 0,01 ms plutôt que 1 ms sous Windows.

6 Lexiques

Ce lexique présente un résumé des acronymes réseau les plus importants.

ASCII
(American Standard Code for Information Interchange) est une norme permettant d'écrire tous les caractères alphanumériques en chiffres de 0 à 255. Par exemple, la lettre A majuscule a le code ASCII 65. Les programmes sources sont des fichiers textes purs qui ne contiennent que des codes ASCII.

ARP
(Address Resolution Protocol) est un protocole permettant d'obtenir l'adresse physique d'une carte réseau à partir de son adresse IP logique. Par exemple, obtenir l'adresse physique 00-22-4D-51-40-35 à partir de l'adresse IP logique 192.168.0.135

DHCP
(Dynamic Host Configuration Protocol) est un protocole permettant à un ordinateur qui se connecte sur un réseau d'obtenir dynamiquement sa configuration réseau.

DNS
(Domain Name System) est un service informatique distribué utilisé pour traduire les noms de domaine et adresses IP symboliques en adresse IP logique. Par exemple, le serveur DNS de Polytechnique (ns1.polymtl.ca) permet d'obtenir l'adresse IP logique 132.207.6.35 à partir de l'adresse symbolique www.polymtl.ca

FTP/SFTP
(File Transfer Protocol/Secure File Transfer Protocol) sont deux protocoles de transfert de fichier bidirectionnel entre un client et un serveur FTP/SFTP. La version FTP est non sécurisé, alors que la version SFTP est sécurisée.

HTTP/HTTPS
(HyperText Transfer Protocol) est un protocole d'échange de fichiers (HTML, images et autres) entre un ordinateur client et un serveur Web. Le client est habituellement un navigateur Web, alors que le serveur Web souvent un logiciel tel qu'Appache installé sur un ordinateur de grande capacité.

IMAP
(Internet Message Access Protocol) permets, tout comme le protocole POP, de consulter ses courriels sur un serveur, mais offre beaucoup plus de possibilités. Il est possible de laisser ses courriels en dépôt dans le serveur, et ainsi permettre des accès simultanés. Il permet également de gérer plusieurs boîtes de courriels et d'en trier le contenu.

IP
(Internet Protocol) est probablement le protocole le plus important d'internet. Tout comme une adresse postale, une adresse IP permet d'identifier la destination (ou source) d'un paquet de données à transmettre (ou reçu) avec TCP. Dans la version IPv4, il utilise 4 octets de 8 bits (4 nombres entre 0 et 255) pour identifier un poste, un serveur ou un équipement réseau. Par exemple, l'adresse IP logique 132.207.6.11 pour le serveur DNS ns1.polymtl.ca de Polytechnique.

POP
(Post Office Protocol) permets de récupérer directement ses courriels d'un serveur de courriel. Dans ce mode, les courriels sont entièrement téléchargés dans le poste du client et retirés du serveur. Ce mode permet de libérer rapidement du serveur les courriels des usagers, mais les courriels ne sont alors plus disponibles de façon centralisée. Il existe en version POP2 et POP3.

Telnet/SSH
Les protocoles Telnet et SSH (Secure SHell) permettent l'interfaçage d'un terminal (affichage et clavier de commande) avec un serveur à travers un réseau. Les terminaux peuvent être du matériel physique ou une simple fenêtre terminale (console). La version Telnet est non sécurisé, alors que la version SSH est sécurisée.

TCP
(Transmission Control Protocol) est une suite de protocole permettant d'assurer la communication des données entre les postes informatiques sur internet. Il permet le fractionner des données, les acheminer, les récupérer à destination et en assurer leur assemblage sans erreur. Il se base sur la notion d'adressage du protocole IP.

SMTP
(Simple Mail Transfer Protocol) est le protocole permettant d'acheminer un courrier directement d'un serveur de courriel à un autre.

URL
(Uniform Resource Locator) est un format de nommage universel pour désigner les ressources sur Internet. Il peut contenir le protocole, le nom d'usager et le mot de passe, l'adresse IP symbolique ou logique du poste, le numéro de port et finalement, le chemin dans les répertoires jusqu'au nom du fichier.

VPN
(Virtual Private Network) est un canal de communication privé (encodé) construit temporairement à travers internet entre un poste client et un réseau distant privé. Le serveur VPN distant attribue alors une adresse IP logique au poste client comme s'il était présent dans le réseau privé.