Internet et la sécurité

Quand nous parlons d'Internet, ce terme recouvre deux concepts :

- *une architecture de réseau informatique dont le cœur, nommé l'architecture TCP/IP, est apte à construire des réseaux hétérogènes offrant des services très évolués ; cette architecture est maintenant universellement employée à la fois dans le réseau Internet, mais également dans les réseaux d'entreprise (Intranet), les réseaux industriels, etc.*
- *une infrastructure de télécommunication qui s'appuie sur la technologie TCP/IP pour développer le média Internet ; cette infrastructure est essentiellement supportée par les opérateurs de télécommunications via le réseau téléphonique. Elle cherche à la fois ses modes de régulation techniques et économiques*

Rappel sur le fonctionnement d'Internet

Infrastructure Internet : Pour décrire ce qu'est l'architecture TCP/IP, considérons un exemple de communication sur le réseau Internet. Alice est devant son ordinateur, chez elle, à Belfort, et cherche à accéder au serveur web de Bob, et plus particulièrement une page qui lui permet, via un formulaire, de dialoguer avec Bob. Cette page se trouve à l'adresse URL ***www.bst.edu/Alice/formulaire.html*** . Dans cette URL, ***www.bst.edu*** désigne le serveur web de Bob. Ce serveur web est installé sur un ordinateur situé en Australie dans l'université BST (Bob School of Technology).

Alice lance son navigateur, compose l'URL, et attend.

Rappelons que les machines d'Internet sont connues par leurs adresses IP (Internet Protocol). La suite 193.78.60.3 est une adresse IP. Certaines machines, comme le serveur de Bob, ont un numéro IP permanent, d'autres, comme l'ordinateur d'Alice, n'en ont pas.

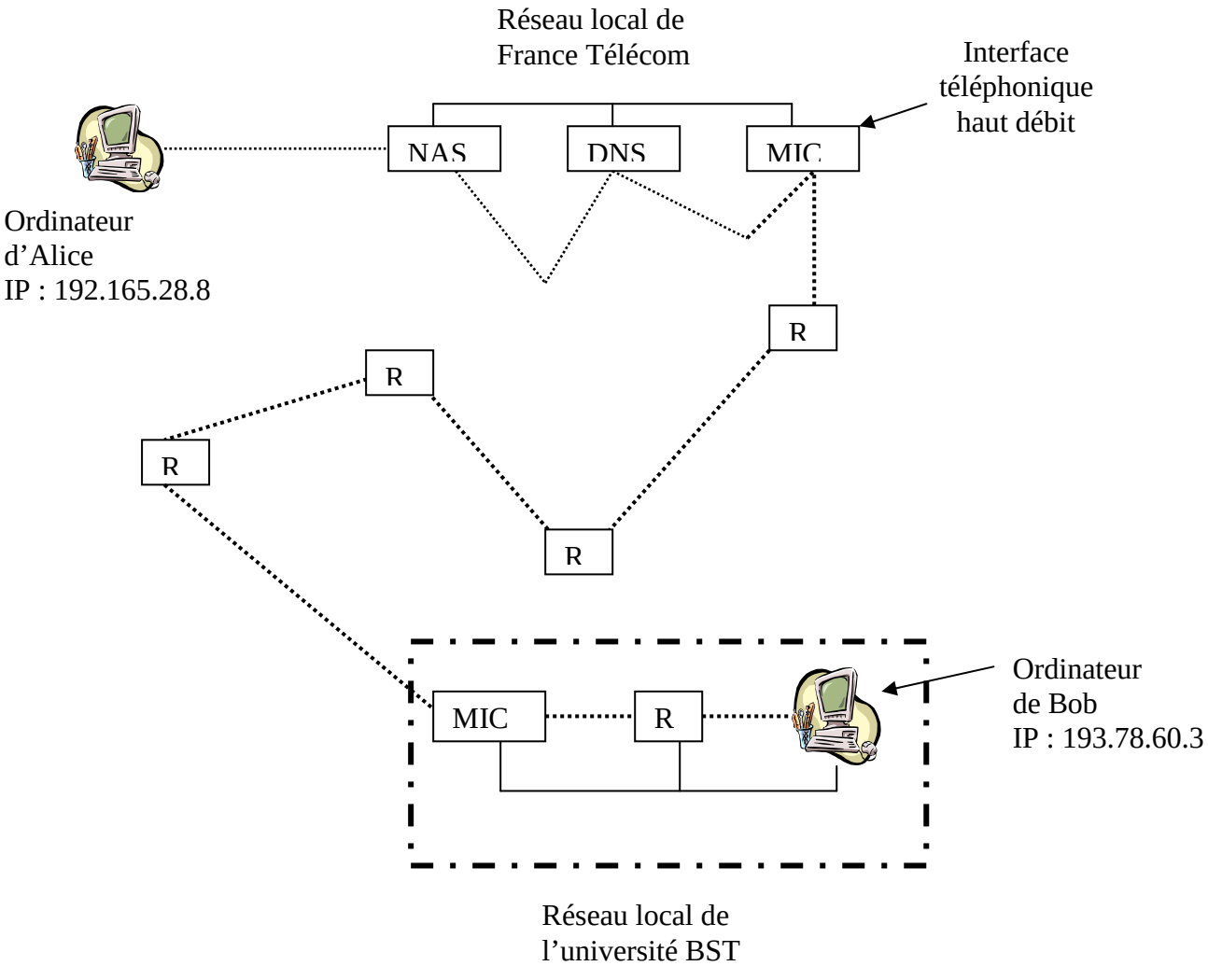
Le protocole de transport TCP (Transport Control Protocol) offre un service de remise fiable en mode connecté. Il met en relation deux applications qui dialoguent via des identificateurs de connexion ou ports. Dans notre exemple, l'adresse de l'application web de Bob est 193.78.60.3 :80, car le port 80 est celui alloué en standard à **http.** L'adresse IP et le port alloué au navigateur d'Alice sont déterminés dynamiquement lors de l'établissement de la connexion TCP.

Le navigateur d'Alice doit d'abord rechercher l'adresse IP de l'ordinateur qui supporte le serveur **http** *www.bst.edu***.** Il doit utiliser pour cela le service d'un annuaire distribué sur l'Internet, le DNS (Domain Name System). Le navigateur trouve dans la configuration TCP de l'ordinateur d'Alice, l'adresse IP (192.165.28.8) du serveur DNS du prestataire d'Alice (France Télécom) et tente d'ouvrir une connexion TCP vers ce serveur. Comme l'ordinateur d'Alice n'est pas encore connecté, TCP demande l'ouverture d'une connexion physique à distance via le protocole de niveau liaison PPP (Point to Point Protocol). Le protocole PPP, via le modem d'Alice, compose le numéro de France Télécom. L'appel est reçu sur une machine qui gère un groupe de modems NAS (Network Access Server), qui affecte automatiquement un modem à cet appel, ouvre la connexion PPP, transmet à l'ordinateur d'Alice une adresse IP provisoire valable pour la connexion.

TCP ouvre alors une connexion entre l'ordinateur d'Alice et le DNS. Le navigateur interroge le DNS qui lui répond que l'adresse IP de la machine bob.bst.edu support de ***www.bst.edu*** est 193.78.60.3.

Le navigateur demande alors à TCP d'ouvrir une connexion vers le protocole http de la machine de Bob, c'est-à-dire vers l'adresse 193.78.60.3 :80. La demande, ainsi que tous les messages suivants, va atteindre le réseau du prestataire via PPP, traverser ce réseau du prestataire puis une succession de routeurs R, qui vont trouver une route et propager les messages vers le réseau local de BST et le serveur web. Ces échanges utiliseront comme support le réseau essentiellement téléphonique. La recherche de la route est effectuée pour chaque message échangé par les routeurs. Ceux-ci utilisent des tables de routage qui, pour l'adresse IP de destination d'un message, donnent le prochain routeur à traverser.

Lorsque la connexion TCP entre l'ordinateur d'Alice et le serveur web est établie, le navigateur utilise le protocole applicatif http pour faire une requête à la page ***www.bst.edu/Alice/formulaire.html*****.** La réponse est retournée sur la même connexion TCP et affichée sur l'ordinateur d'Alice.



Architecture TCP/IP : Pour réaliser la suite d'opérations précédente, nous avons utilisé les protocoles de l'architecture TCP/IP. Les protocoles de cette architecture sont décrits par la figure suivante :

<table>
<tr><td>Dénomination
Des couches selon
l'architecture ISO</td><td colspan="5">Protocoles d'Internet</td></tr>
<tr><td>7 : Application

Exemples de protocoles</td><td>- SMTP (Simple Mail Transfer Protocol)
-POP (Post Office Protocol)
- IMAP (Internet Message Access Protocol)</td><td>HTTP (Hypertext Transfer Protocol)</td><td>DNS (Domain Name System)</td><td>Telnet</td><td>FTP (File Transfer Protocol</td></tr>
<tr><td>6 : Présentation</td><td colspan="5">- MIME (Multipurpose Internet Mail Extension)
- HTML (HyperText Markup Language)
- XML (eXtended Markup Language)</td></tr>
<tr><td>4 : Transport</td><td colspan="5">- TCP (Transport Control Protocol)
- UDP (User Datagram Protocol)</td></tr>
<tr><td>3 : Réseau</td><td colspan="2">- IP (Internet Protocol) V4
- ICMP (Internet Control Message Protocol)
- RIP (Routing Information Protocol)
- OSPF(Open Shortest Path First)
- BGP (Border Gateway Protocol)</td><td colspan="3">IPv6
RIP, BGP, OSPF</td></tr>
<tr><td>2 : Liaison</td><td colspan="5">Encapsulation IP sur réseau local ou en PPP (Point to Point Protocol) sur liaison point à point et réseau téléphonique</td></tr>
<tr><td>1 : Physique</td><td colspan="5">Tout support de transmission en particulier les réseaux locaux, le réseau téléphonique</td></tr>
</table>

Le protocole de niveau Application, utilisé par le navigateur d'Alice, est HTTP. Il permet de gérer les applications web selon un protocole client/serveur. Le protocole de résolution d'adresse DNS est aussi un protocole applicatif. Il gère est maintient cohérente une base de données réparties sur tous les serveurs DNS du monde. Il y a au moins deux serveurs par domaine. Un domaine correspond à toutes les machines dont le nom se termine par exemple par ***.fr, utbm.fr*** ou ***bst.edu***. Le DNS fournit pour chaque machine son adresse IP et fournit également tous les serveurs de courriers d'un domaine. Les normes de niveau Présentation MIME, XML,… fournissent des formats d'encodage de documents transmis sur le web ou par le courrier. TCP est le protocole de transport en mode connecté. Il permet d'établir une ou plusieurs connexions entre deux applications supportées par deux ordinateurs ainsi que de transférer dans l'ordre des données sur cette connexion et en récupérant toutes les défaillances transitoires (perte d'un message par exemple). UDP est un protocole en mode non connecté qui permet le transfert de messages entre deux applications. En mode non connecté, chaque message est indépendant et transmis sans contrôle d'erreur.

Pour identifier un dialogue, TCP utilise des numéros de port et se base sur le concept de connexion, défini comme une paire d'extrémités de connexion : (*Adresse IP de la machine source, Port de la machine source*) et (*Adresse IP de la machine cible, Port de la machine cible*). Le tableau ci-après donne quelques exemples de ports réservés.

Service	Port TCP
FTP	20 (données), 21 (contrôle)
Telnet	23
SMTP (Mail)	25

DNS	53
HTTP	80
POP3	100

IP est le protocole de Réseau. Il véhicule des messages en mode non connecté entre deux ordinateurs (deux adresses IP). Son rôle principal est de donner la route (de routeur en routeur) que doit suivre un message pour atteindre sa destination. Il s'appuie, par exemple, sur les protocoles RIP, OSPF et BGP qui mettent à jours ces tables de routages en fonction des performances et de la fiabilité de chaque chemin possible. La version actuelle de IP est la version 4 (IPv4). Elle nécessite plusieurs autres protocoles dont ICMP qui permet de véhiculer les messages d'erreurs sur le routage et de modifier très vite les tables de routage en cas de pannes de liaisons et de routeurs. Dans la nouvelle version, IPv6, ces protocoles sont intégrés à IP. PPP sert à mettre en communication deux machines via une liaison physique.

Remarque : Dans l'architecture Internet, la couche 5 n'est pas utilisée. Par contre elle est utilisée par les protocoles de sécurité et pour implanter les appels de procédures à distance dans NFS (Network File System server : un système de fichiers par réseau qui permet d'exécuter un fichier situé sur le serveur, effectuer un traitement sur la machine distante et maintenir le fichier de données sur celle-ci).

Pour traiter comme exemple le transfert de courrier électronique entre Alice et Bob, outre l'ordinateur de Bob, deux machines supplémentaires sont nécessaires. Il s'agit des serveurs de courrier d'Alice et de Bob. Ils peuvent, par exemple, être respectivement situés sur le réseau local du prestataire d'Alice (France Télécom) et sur celui de l'université BST. Deux autres protocoles de niveau Application sont mis en oeuvre, SMTP et POP. SMTP permet à Alice de déposer des messages dans son serveur, puis, en utilisant le DNS, va trouver l'adresse du serveur de Bob. Le protocole SMTP va transférer le courrier du serveur d'Alice à celui de Bob. Enfin Bob va pouvoir prélever son courrier en utilisant POP ou IMAP. Notons q'il existe de nombreux protocoles applicatifs comme Telnet, qui permet de se connecter à distance sur un ordinateur en étant comme un terminal ou FTP qui permet de transférer des fichiers entre deux ordinateurs.