CHAPITRE 6

LES PROTOCOLES RESEAUX

Leçon 1 : Introductions aux protocoles

Les protocoles sont des règles et des procédures de communication. On dénombre de nombreux protocoles. Tous les protocoles facilitent la communication, mais chacun à un rôle bien spécifique. Certains ne fonctionnent qu'au niveau de certaines couches du modèle OSI. La couche ou opère un protocole décrit la fonctionnalité de celui – ci. Par exemple, un protocole de la couche physique garantit le passage à travers la carte réseau et sur le câble.

Les protocoles peuvent coopérer au sein d'une pile de protocoles. De même que les fonctionnalités d'un réseau sont réparties sur toutes les couches OSI, de même les différents protocoles d'une pile se répartissent sur tous les niveaux de celle ci. Les niveaux d'une pile de protocoles correspondent à des couches du modèle OSI. Par exemple, la couche Application du protocole TCP/IP correspond à la couche Présentation du modèle OSI. Pris dans leur ensemble, les protocoles décrivent les fonctionnalités et les capacités de toute la pile.

Toute la procédure technique impliquée par la transmission de données sur le réseau doit être décomposée en un ensemble discret de phases. A chaque phase sont associées certaines actions qui ne peuvent pas se produise dans une autre phase. Chaque phase comporte ses propres règles et procédures, c'est à dire son protocole.

Ces phases doivent se succéder dans un ordre cohérent, qui est le même sur toutes les machines du réseau. Sur l'ordinateur émetteur, ces phases se font du haut vers le bas. Sur l'ordinateur récepteur, elles se font dans l'ordre inverse.

Au niveau de l'émetteur, les protocoles découpent les données en petits blocs, appelés paquets, susceptibles d'être traités par le protocole. Il ajoute des informations d'adressage aux paquets afin que l'ordinateur cible reconnaisse les données qui le concerne et prépare les données pour le transfert à travers la carte réseau et sur le câble.

Au niveau du récepteur, les protocoles s'occupent des mêmes charges, mais en ordre inverse. Ils récupèrent les paquets apportés par le câble. Ils transfèrent les paquets dans l'ordinateur, via la carte réseau. Ils suppriment des paquets toutes les informations de contrôle ajoutées par l'émetteur. Ils copient dans un tampon les données extraites des paquets, pour ensuite ré assembler ces données. Ils passent à l'application, sous une forme qui lui soit compréhensible, les données ré assemblés.

L'émetteur et le récepteur doivent réaliser chaque phase de façon identique, afin que les données soient reçues telles qu'elles ont été émises.

Par exemple, deux protocoles distincts découpent les données en paquets et y ajoutent diverses informations – numéros d'ordre, données d'horloge, informations de contrôle d'erreur – mais chacun

procède différemment. Un ordinateur utilisant l'un de ces deux protocoles ne pourra pas communiquer avec un ordinateur utilisant l'autre protocole.

Quand on parle de transmission entre deux réseaux locaux entre lesquels il existe plusieurs chemins, on dit que les données sont routées. Les protocoles compatibles avec les communications multichemins entre réseaux locaux sont appelés protocoles routables. Les protocoles routables permettent de relier plusieurs réseaux locaux et ainsi de créer des réseaux étendus.

Dans un réseau, plusieurs protocoles doivent collaborer les uns avec les autres. Cette collaboration garantit que les données seront correctement préparées, transférées à la bonne destination, reçues et traitées.

La coordination entre les divers protocoles s'avère incontournable, afin qu'il n'y ait ni conflits ni opération inachevées. De cette coordination naît une architecture en couches.

Une pile de protocoles est une combinaison de protocoles. Chaque couche de la pile spécifie un protocole différent, chargé de réaliser telle ou telle fonctionnalité du processus de communication. Chaque couche a son propre ensemble de règles. Les protocoles définissent les règles de chaque couche OSI. Les couches basses du modèle OSI spécifient la manière dont les fabricants peuvent connecter leurs matériels à ceux des autres fabricants ; par exemple, un même réseau peut utiliser des cartes d'origine différentes. Du moment que les matériels utilisent les mêmes protocoles, ils peuvent s'échanger des données.

- ***Couche application*** *Initie ou accepte une requête*
- ***Couche présentation*** *Ajoute des données de formatage, d'affichage et de chiffrement*
- ***Couche session*** *Ajoute des informations de flux pour déterminer le moment où le paquet sera émis*
- ***Couche transport*** *Ajoute des informations de traitement d'erreurs*
- ***Couche réseau*** *Ajoute des informations de contrôle, de séquencement et d'adressage*
- ***Couche liaison*** *Ajoute des informations de contrôle d'erreurs et prépare les données pour l'envoi sur le support physique*
- ***Couche physique*** *Envoie des paquets sous la forme de flots de bits*

L'industrie informatique a privilégié plusieurs piles comme modèles standards de protocoles. Les plus importants sont TCP/IP, IPX/SPX, Netbeui, DECnet de DIGITAL et SNA d'IBM.

A chaque niveau de ces piles, on trouve des protocoles qui effectuent des tâches spécifiées par ce niveau. Cependant, les tâches de communication effectuées par les réseaux sont regroupées dans trois types de protocoles. Chacun de ces types englobe une ou plusieurs couches OSI.

<table>
<tr><td>Couche application</td><td rowspan="3">Services réseau de niveau application, utilisateurs</td></tr>
<tr><td>Couche présentation</td></tr>
<tr><td>Couche session</td></tr>
<tr><td>Couche transport</td><td>Services de transport</td></tr>
<tr><td>Couche réseau</td><td rowspan="3">Services réseau</td></tr>
<tr><td>Couche liaison</td></tr>
<tr><td>Couche physique</td></tr>
</table>

Les protocoles de type application fonctionnent au niveau de la couche haute du modèle OSI. Ils assurent les interactions et les échanges de données entre les applications. Ex : SMTP, FTP, SNMP, SMB, NCP……

Les protocoles de type transport gèrent les sessions de communication entre les ordinateurs et garantissent le transfert fiable des données. Ex : TCP, SPX, Netbeui……

Les protocoles de type réseau assurent ce que l'on appelle un service de liaison. Ces protocoles gèrent les informations d'adressage et de routage, font du contrôle d'erreurs et traitent les requêtes de retransmission. Ils définissent également les règles de communication en usage dans un environnement réseau spécifique, par exemple sous ETHERNET ou TOKEN RING. Ex : IP, IPX, Netbeui…

On distingue les protocoles IEEE de la couche physique :

802.3 - ETHERNET – Le protocole CSMA/CD régule le trafic réseau, en n'autorisant la transmission que si le câble est libre qu'aucun ordinateur ne soit en train d'émettre.
802.4 - Bus à jeton – Bus utilisant un mécanisme de passage de jeton.
802.5 - TOKEN RING – Un jeton circulant sur l'anneau indique l'ordinateur autorisé à émettre.

L'installation d'un protocole ainsi que sa suppression du système est une démarche qui ressemble à l'installation de pilotes pour un périphérique.

Le modèle OSI définit les protocoles qu'il faut utiliser au niveau de chaque couche. Les OS réseaux tels que NT et Netware ont une approche lié à ce modèle.

	WINDOWS NT	*NETWARE*
Couche application	Redirecteur serveur	NCP – Netware Core Protocol -
Couche présentation	TDI	Canaux nommés netbios
Couche session	TCP/IP Nwlink NBT DLC	SPX
Couche transport	NDIS	IPX
Couche réseau	Wrapper NDIS – pilotes cartes réseau	Pilotes LAN
Couche liaison		ODI NDIS
Couche physique	Physique	Physique

Leçon 2 : TCP / IP

TCP/IP est devenu le protocole standard en matière d'interopérabilité entre ordinateurs hétérogènes. Cette interopérabilité constitue l'un des atouts majeurs de TCP/IP. Presque tous les réseaux sont compatibles avec TCP/IP. Il permet de faire du routage et sert souvent de protocole pour la communication inter réseau.

Entre autres protocoles développés spécialement pour la suite TCP/IP, on trouve :

SMTP – Simple Mail Transfer Protocol –
FTP – File Transfert Protocol –
SNMP – Simple Network Management Protocol –

TCP/IP fut inventé par le ministère américain de la défense qui voulait un protocole routable, robuste et fonctionnellement performant, qui puisse servir à créer des réseaux étendus capables de fonctionner même en cas de guerre nucléaire.

C'est maintenant la communauté INTERNET qui gère l'évolution de TCP/IP : c'est une norme industrielle ouverte, elle n'appartient à aucune entreprise en particulier. Il apporte un ensemble d'utilitaire permettant de connecter des systèmes d'exploitation hétérogènes. Il utilise une architecture client – serveur évolutive et indépendante de la plate – forme ce qui fait qu'une application tournant sur un serveur UNIX peut être attaquée par un client Windows 9x via les sockets – identifie un service sur un certain nœud d'un réseau. Un socket se compose d'une adresse de nœud et d'un numéro de port associé au service.

TCP/IP ne présente pas que des avantages : c'est un protocole très volumineux et finalement pas aussi rapide que cela, en comparaison à IPX et Netbeui.

Les normes concernant TCP/IP sont définies dans ce que l'on appelle les RFC.

Les protocoles TCP/IP ne correspondent pas exactement au modèle OSI. Il y'a 4 couches, au lieu de sept. Connue sous le nom des protocoles INTERNET, la pile TCP/IP se compose des couches suivantes :

- ***F*** *Couche Application*
- ***F*** *Couche Transport*
- ***F*** *Couche Internet*
- ***F*** *Couche Interface réseaux*

La couche interface réseau correspond aux couches physiques et liaison du modèle OSI. Elle communique directement avec le réseau. Elle assure l'interface entre l'architecture du réseau – ETHERNET, TOKEN RING – et la couche Internet.

La couche Internet correspond à la couche réseau du modèle OSI. Elle utilise plusieurs protocoles pour le routage et la livraison de paquets. Les routeurs sont dépendants des protocoles. Ils fonctionnent au niveau de cette couche et servent à acheminer les paquets entre les réseaux. Voici les protocoles de cette couche :

IP - Internet Protocol - C'est un protocole à commutation de paquets qui gère l'adressage et se charge de sélectionner les routes. Lors de la transmission d'un paquet, ce protocole ajoute au paquet un en – tête qui facile le routage du paquet sur le réseau. IP est un protocole sans connexion : il émet des paquets sans demander au récepteur de faire des accusés de réception. IP, se charge, en outre, de l'assemblage et du désassemblage des paquets tels que l'imposent les couches physiques et liaison du modèle OSI. Chaque paquet se compose d'une adresse source, d'une adresse de destination, d'un identificateur de protocole, d'une somme de contrôle (valeur calculée) et d'un TTL (Time To Live). Le TTL indique à chaque routeur situé entre la source et la cible le temps que le paquet peut rester sur le réseau. Le TTL fonctionne comme un compte à rebours. Chaque fois que le paquet passe par un routeur, celui – ci décrémente le compteur d'une seconde ou d'un saut (hop). Par exemple : un paquet ayant un TTL de 128 peut rester sur le réseau pendant 128 secondes ou le temps de faire 128 sauts (chaque passage de routeur comptant pour un saut). Toutes les combinaisons de durée et de sauts sont permises. Le TTL sert à empêcher les paquets perdus ou altérés de circuler indéfiniment sur le réseau. Quand le compteur TTL arrive à 0, le paquet est détruit.

ARP - Adress Resolution Protocol – Le protocole détermine l'adresse physique du destinataire, c'est à dire l'adresse MAC de la carte réseau. Si ARP ne contient pas l'adresse dans son cache, il diffuse une requête « broadcast » pour la demander. Tous les hôtes du réseau reçoivent cette requête ; celui dont l'adresse physique correspond à la demande envoie cette adresse au demandeur. Le paquet est ensuite expédié là où il faut, et l'adresse physique nouvellement obtenue est placée dans le cache du routeur.

RARP – Reverse Adress Resolution Protocol – Un serveur RARP gère une base de données d'adresse physique, qui a la forme d'une table ARP. Alors que ARP donne des adresses physiques à partir d'adresse IP, RARP fait le contraire : il fournit une adresse logique (adresse IP) à partir d'une adresse physique. Quand le serveur RARP reçoit d'un nœud du réseau une demande concernant une adresse IP, il consulte sa table de routage et envoie au demandeur l'adresse IP associée à l'adresse physique qui lui a été fournie.

ICMP – Internet Control Message Protocol – ICMP envoie et reçoit des informations d'état concernant les transmissions en cours. Les routeurs utilise fréquemment ICMP pour contrôler le flux, ou la vitesse des données qui leur arrivent ou qu'ils envoient. Si le flux de données se révèle trop rapide pour un routeur, il demande aux autres de ralentir.

La couche transport correspond à la couche transport du modèle OSI. Elle est chargée de créer et de gérer des communications bout à bout (end to end) entre deux hôtes. Elle fournit les accusés de réception, fait du contrôle de flux et ordonnance les paquets. Elle gère également les retransmissions de paquets. La couche transport peut employer soit le protocole TCP soit UDP, selon les contraintes de la transmission.

TCP – Transmission Control Protocol – TCP assure des transmissions fiables entre les nœuds. C'est un protocole orienté connexion entre deux machines avent l'envoi de données. Pour établir une connexion fiable, TCP recourt à un mécanisme, connu sous le nom de « three way handshake » qui détermine le numéro de port et les numéros d'ordre initiaux.

Le Handshake se fait en trois temps :

-1- Le demandeur envoie un paquet spécifiant le numéro de port qu'il compte employer, ainsi que son numéro d'ordre initial.
-2- Le serveur accuse réception en envoyant son numéro d'ordre initial, qui est égal à celui du demandeur augmenté de 1.
-3- Le demandeur accuse réception de l'accusé de réception, en renvoyant le numéro d'ordre du serveur augmenté de 1.

Pour garantir la fiabilité de la connexion, chaque paquet doit contenir :

- **F** Les numéros de port TCP de la source et de la destination.
- **F** Un numéro d'ordre, si le message est découpé en paquets plus petits.
- **F** Une somme de contrôle qui garantit la non – altération des données.
- **F** Un numéro d'accusé indiquant à l'émetteur quelles sont les parties du message qui ont été reçues.
- **F** Des fenêtres coulissantes TCP.

Ports, sockets et fenêtre coulissante

Les numéros de ports de protocole indiquent l'emplacement d'une application (processus) sur chaque machine (dans la couche application). De même qu'une adresse IP identifie l'adresse d'un hôte sur le réseau, l'adresse des ports identifie l'application pour la couche transport ; cela permet de créer une connexion complète entre une application tournant sur un hôte et une application exécutée sur un autre hôte. Les applications et les services peuvent utiliser jusqu'à 65 536 ports. Les applications et services TCP/IP utilisent en principe les 1 023 premiers ports. Les applications clientes affectent dynamiquement les numéros de ports, en fonction des besoins. La combinaison d'un port et d'une adresse de nœud constitue un socket.

Les services et les applications utilisent des sockets pour créer des connexions entre les hôtes. Si l'application doit garantir la bonne livraison des données, le socket choisit le service orienté connexion (TCP). Dans le cas contraire, le socket choisit le service sans connexion (UDP).

TCP emploie une fenêtre coulissante pour transférer des données entre les hôtes. La fenêtre définit le volume de données susceptibles d'être passée via une connexion TCP, avant que le récepteur n'envoie un accusé de réception. Chaque ordinateur comporte une fenêtre d'émission et une fenêtre de réception qu'il utilise pour bufférisier les données en continu, sans devoir attendre un accusé de réception pour chaque paquet. Cela permet au récepteur de recevoir les paquets dans le désordre et de profiter des délais d'attente pour réorganiser les paquets. La fenêtre émettrice contrôle les données émises ; si elle ne reçoit pas d'accusé de réception au bout d'un certain temps, elle retransmet le paquet.

UDP – User Datagram Protocol – protocole sans connexion, UDP est chargé de la transmission bout à bout des données. Contrairement à TCP, UDP ne crée pas de connexion. Il essaie d'envoyer les données et de vérifier qu'elles sont parvenues à destination. UDP s'utilise surtout pour envoyer de petits volumes de données, qui n'exigent pas de livraison garantie. UDP fait appel à des ports, mais qui ne sont pas les mêmes que TCP ; les deux protocoles peuvent donc employer les mêmes numéros de ports sans qu'il y'ait interférences.

La couche application correspond aux couches session, présentation et application du modèle OSI et relie les applications au réseau. Deux API permettent d'accéder aux protocoles de transports TCP/IP : les sockets Windows et Netbios.

Les sockets Windows Winsock sont des API réseau qui facilitent les communications entre les applications TCP/IP et les piles de protocoles. Elle a été crée pour que les applications utilisant TCP/IP puissent écrire dans un modèle standard. Winsock dérive de l'API socket originel, inventée pour UNIX BSD. Winsock fournit une interface de programmation commune aux applications situées vers le sommet du modèle TCP/IP. Tout programme écrit avec Winsock peut communiquer avec n'importe quel protocole TCP/IP et vice versa.

<table>
<tr><th>Modèle OSI</th><th>Modèle TCP/IP</th></tr>
<tr><td>Application</td><td rowspan="3">Application</td></tr>
<tr><td>Présentation</td></tr>
<tr><td>Session</td></tr>
<tr><td>Transport</td><td>Transport</td></tr>
<tr><td>Réseau</td><td>Internet</td></tr>
<tr><td>Liaison</td><td rowspan="2">Interface réseau</td></tr>
<tr><td>Physique</td></tr>
</table>

Leçon 3 : Les protocoles NETWARE

NOVELL offre une suite de protocoles qui ont été inventée pour servir exclusivement sous NETWARE. Attention, depuis les versions 5, TCP/IP est aussi devenu le protocole standard utilisé par cet éditeur. Les 5 principaux protocoles netware sont : IPX,, SPX, RIP, NCP et SAP.

F *Comparaison entre le modèle OSI et le modèle NETWARE*

Application	NCP SAP RIP
Présentation	
Session	
Transport	
Réseau	IPX / SPX
Liaison	Protocoles d'accès au support (Ethernet, Token Ring, ARCnet….)
Physique	

Le protocole NETWARE ne recoupe pas exactement les spécifications du modèle OSI car IPX / SPX est antérieure à ce modèle. Les protocoles NETWARE suivent un modèle en enveloppe. Plus précisément, les protocoles de niveau supérieurs sont encapsulés par IPX/SPX, lui – même enveloppé par l'en tête et la queue du protocole d'accès au support.

Les protocoles d'accès au support définissent l'adressage qui permet de distinguer chaque nœud d'un réseau NETWARE. Il est chargé de placer l'en tête dans le paquet. Chaque en – tête inclut les adresses sources et de destination. Une fois le paquet envoyé sur le câble, chaque carte réseau vérifie l'adresse ; si son adresse est égale à l'adresse de destination inscrite sur le paquet, ou si le paquet est en diffusion générale – broadcast – la carte réseau copie le paquet et le passe à la pile de protocole.

Outre l'adressage, ce protocole fournit aussi du contrôle d'erreur.

IPX est un protocole de couche réseau, sans connexion et non garanti. IL est l'équivalent d'IP. IPX n'exige pas d'accusé de réception pour chaque paquet envoyé. SPX apporte un protocole de couche transport orienté connexion et fiable.

RIP – Routing Information Protocol – facilite l'échanges des informations de routage sur un réseau NETWARE. Il permet de déterminer la route la plus rapide à travers le passage de routeurs. De plus, il permet aussi aux routeurs de s'adresser à d'autres routeurs pour connaître les routes les plus efficaces.

SAP – Service Advertising Protocol – SAP permet aux nœuds fournissant des services (serveurs de fichiers, d'impression, serveurs de passerelles, d'application…) de signaler au réseau leurs services et adresses. Par défaut un serveur SAP annonce sa présence via des « broadcasts » toutes les 50 secondes.

NCP définit les détails du contrôle des connexions et des requêtes de service, toutes choses qui permettent l'interaction entre les clients et les serveurs. C'est le protocole qui fournit les services de transport et de session. IL intègre aussi les fonctionnalités de sécurité NETWARE.

Leçon 4 : Les autres protocoles

F Netbios

La plupart des services et des applications exécutées sous Windows utilisent l'interface netbios. Netbios, inventée pour les réseaux locaux, est une interface standard que les applications peuvent employer pour accéder aux protocoles de la couche transport, tant pour des communications orientées connexion ou sans connexion. Il existe des interfaces Netbios pour netbeui, Nwlink et TCP/IP. Netbios exige un nom Netbios pour identifier sans ambiguïté un ordinateur.

F Netbeui

C'est l'acronyme de netbios Extended User Interface. A l'origine netbeui et Netbios étaient étroitement liés, et ils étaient considérés comme formant un seul protocole. Cependant, plusieurs fournisseurs séparèrent Netbios, le protocole de couche Session, afin qu'ils puissent servir avec d'autres protocoles de transports routables. Netbios est une interface IBM pour réseaux locaux, qui opère au niveau de la couche Session et fait office d'interface entre les applications et le réseau. Netbios fournit les outils qui permettent à une application d'établir une session réseau avec une autre application. Elle doit sa popularité au fait qu'elle est utilisée par de très nombreuses applications.

Netbeui est un protocole de la couche transport, petit, rapide et efficace, fourni avec tous les produits réseaux MICROSOFT. Ce protocole existe depuis le milieu des années 80 et il était déjà fourni avec le premier produit réseau de MICROSOFT, à savoir MS-NET.

Les atouts de Netbeui sont : sa pile de taille réduite, sa vitesse de transfert sur le câble et sa compatibilité avec tous les réseaux MICROSOFT.

Il présente l'inconvénient majeur d'être un protocole de transport non routable. Il se trouve limité, en outre, aux seuls réseaux MICROSOFT. Par contre, il est très adapté aux réseaux dits poste à poste.

F Commutation de paquets X25

X25 est un ensemble de protocoles pour réseaux étendus, qui est incorporée à un réseau à commutation de paquets composé de services de commutation. Les services de commutation ont été crées à l'origine en vue de connecter des terminaux distants à des gros systèmes.

F XNS

Xerox Network System, développé par XEROX pour ses réseaux locaux ETHERNET, fut très utilisé dans les années 80, mais il a été progressivement remplacé par TCP/IP.

F *APPC*

Protocole de transport développé par IBM en tant que partie de l'architecture SNA – Systems Network Architecture – Il a été conçu pour permettre à des applications fonctionnant sur des ordinateurs différents de communiquer et d'échanger des données directement.

F *APPLETALK*

C'est la pile de protocoles propriétaire d'APPLE, conçue pour permettre aux ordinateurs de cette marque de partager des fichiers et imprimantes dans un environnement réseau.

F *DECnet*

Pile de protocole propriétaire de DIGITAL. DECnet définit des réseaux de communication qui s'appuient sur ETHERNET, TOKEN RING ou FDDI ainsi que sur des réseaux étendus utilisant des fournisseurs publics. C'est un protocole routable.