Protocoles réseaux

BTS SIO - Bloc 1 - Support et mise à disposition des services informatiques

U4 - 1.2 Répondre aux incidents et aux demandes d’assistance et d’évolution

1. Principales familles de protocoles

À l'avènement des réseaux locaux, différents protocoles de couches moyennes et hautes furent utilisés, bien souvent liés à un éditeur de logiciels. Ils ont progressivement été remplacés par le standard de fait TCP/IP.

1.1. IPX/SPX

1.1.1. L'historique

Historiquement, cette famille de protocoles était utilisée avec les réseaux Novell Netware jusqu'à la version 3.12. TCP/IP était déjà disponible dans cette version, mais IPX/SPX était absolument nécessaire pour assurer le bon fonctionnement du système d'exploitation, éventuellement en plus de TCP/IP. Aujourd'hui, on ne l'utilise quasiment plus même s'il est resté longtemps préconfiguré sur les imprimantes réseau.

1.1.2. Les protocoles

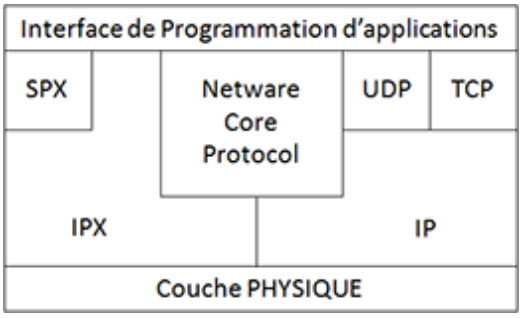
Internetwork Packet eXchange (IPX) agit au niveau des couches Réseau et Transport. Il assure, comme IP, un service sans connexion et sans garantie.

IPX est routable et identifie un hôte à l'aide d'une adresse logique qui ne nécessite pas, comme IP, un plan d'adressage statique. Une adresse IPX est la concaténation d'un numéro de réseau externe, sur 4 octets, et de l'adresse MAC du périphérique, sur 6 octets. L'attribution d'adresses IPX est automatique et, de surcroît, la résolution d'adresses logiques en adresses physiques est instantanée, puisque l'adresse physique fait partie intégrante de l'adresse IPX.

Les adresses IPX se présentent, par exemple, de la manière suivante 0000CAFE : 00-A0-00-26-37-10, où 0000CAFE est le numéro de réseau logique en hexadécimal sur 4 octets et 00-A0-00-26-37-10 constitue l'adresse MAC de la carte réseau.

Sous Netware, il ne faut pas confondre le numéro de réseau externe (lié aux périphériques) avec le numéro de réseau interne (lié aux applications). Ce dernier est lié à la structure interne de Novell qui associe les applications d'un serveur à un numéro de nœud et un numéro de réseau. Le serveur se comporte ainsi comme un routeur interne pour commuter le réseau physique (numéro de réseau externe) avec le réseau logique (les applications du serveur). Ainsi, un serveur Novell possède deux adresses réseaux, une adresse interne et une externe.

Comme pour IP, tous les nœuds reliés au même réseau physique doivent avoir le même numéro de réseau (externe) et chaque adresse IPX doit être unique au sein de l'inter réseau. De même, les numéros de réseaux internes utilisés doivent être uniques.



Une des particularités d'IPX est de pouvoir court-circuiter le modèle OSI, en s'adressant directement à la couche 5 du destinataire, et pas forcément SPX ! IP+TCP correspondent à IPX+SPX, tandis que IP+UDP serait équivalent à IPX seul.

Sequenced Packet eXchange (SPX) est implémenté au niveau de la couche Transport du modèle OSI et assure une livraison fiable des paquets (orientée connexion).

1.2. NetBIOS

1.2.1. L'historique

Network Basic Input/Output System (NetBIOS) a été introduit par IBM en 1985 et optimisé pour les petits réseaux. Sa mise en œuvre est simple, **mais il n'est pas routable**. Il introduit des **noms NetBIOS pour identifier les postes du réseau, sans gérer d'adresses logiques**. Il n'existe donc qu'une résolution de nom en adresses MAC. De plus, cette résolution est souvent gérée par le poste lui-même, qui envoie une diffusion sur le réseau.

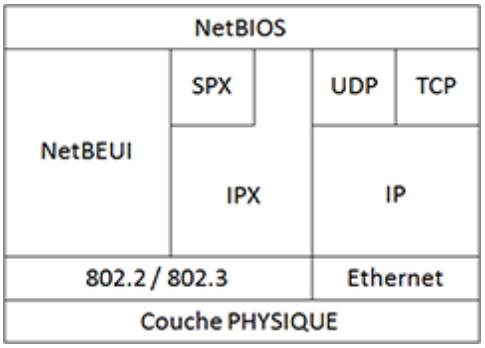
1.2.2. Les principes

La simplicité de ce protocole et le fait qu'il soit peu gourmand en ressources mémoire, font qu'aujourd'hui NetBIOS est encore très utilisé par les produits Microsoft, IBM et Novell.

Les Application Programming Interface (API) NetBIOS se sont largement développées sur PC, pour permettre une indépendance vis-à-vis du protocole sous-jacent utilisé.

NetBIOS est disponible en natif, encapsulé dans des trames LLC (802.2) ou encapsulé dans IPX ou TCP/IP.

Les produits Microsoft fonctionnent encore avec NetBIOS. Il est cependant possible d'utiliser n'importe quel protocole de couches 3, 4 parmi TCP/IP, IPX/SPX ou NetBEUI.



NetBIOS est, aujourd'hui encore, omniprésent dans les systèmes d'exploitation Windows, à travers NBT (NetBIOS over TCP/IP).

Il a fallu attendre Windows 2000 pour que les systèmes d'exploitation Microsoft n'exigent plus d'utiliser NetBIOS, notamment pour son très populaire service de fichiers Server Message Block (SMB).

Sur des versions UNIX/Linux implémentant SAMBa (SMB réécrit par Andrew Tridgel), NetBIOS est automatiquement installé sous la forme d'un démon nmbd.

1.3. TCP/IP

1.3.1. L'historique

Le réseau ARPANET, du nom de l'organisme militaire Advanced Research Projects Agency (ARPA), est né en 1969. Il a été créé par le Department of Defense (DoD) des USA pour connecter différents sites informatiques et a d'abord relié quatre instituts universitaires. Un certain nombre de centres militaires et de recherche, publics comme privés, participant à cette mise au point y furent progressivement reliés.

Au début des années 70, Bob Kahn, du Defense ARPA (DARPA), ex-ARPA, travaille avec Vinton Cerf, chercheur à Stanford Institute, sur de nouveaux protocoles permettant de relier des réseaux. Ainsi naît TCP/IP. En 1976, ARPANET migre sur TCP/IP. En 1978, un second réseau est connecté à ARPANET. Il utilise les lignes téléphoniques et prend le nom d'Internet.

Aujourd'hui, ARPANET est la partie de l'Internet utilisée par le DoD en Recherche et développement.

L'intégration des protocoles Internet dans UNIX Berkeley Software Distribution (BSD) et la diffusion quasi gratuite aux universités contribua à améliorer le succès de cette suite.

1.3.2. La suite de protocoles

La famille TCP/IP, comportant plusieurs dizaines de protocoles, définit un modèle en quatre couches réseau.

Il s'agit des protocoles de communication et d'application les plus populaires pour connecter des systèmes hétérogènes, indépendamment de la couche physique.

Transmission Control Protocol (TCP) est un protocole de transport qui assure un service fiable, orienté connexion pour un flot d'octets.

Par opposition avec TCP, User Datagram Protocol (UDP) est le protocole de transport non orienté connexion. Il est donc très rapide mais surtout peu fiable.

Internet Protocol (IP) fournit un système de livraison de paquets, sans connexion et non fiable. Il gère des adresses logiques, qui décomposent l'identifiant de chaque nœud en un numéro de réseau logique et un numéro de périphérique sur 4 octets (en IP version 4).

Le protocole IPv6, ou IP Next Generation (NG), est désormais disponible dans les systèmes d'exploitation.

Une des clés du succès des protocoles Internet réside dans le fait que le modèle proposé est indépendant de couches Physique et Liaison de données (couches 1 et 2 du modèle OSI).

1.3.3. Le rapport au modèle OSI

Il est important de se souvenir que le modèle TCP/IP a été proposé dix ans avant le modèle OSI, ce dernier s'étant inspiré fortement de certains protocoles TCP/IP. Il est néanmoins intéressant de situer le modèle OSI qui définit un modèle en 7 couches, par rapport aux protocoles Internet qui fonctionnent sur quatre couches.

1.3.4. L'adoption en entreprise

Les qualités de la suite de protocoles TCP/IP, telles que la capacité de fonctionnement sur toutes tailles de réseau, son efficacité et son évolutivité, ont séduit les entreprises. Elles ont, dans un premier temps, interconnecté leurs réseaux par Internet, surtout pour des applications de messagerie et web.

Progressivement, elles ont également adopté ces protocoles, standards de fait, non liés à un constructeur ou un éditeur, au sein même des réseaux locaux. Des Intranet ont commencé à voir le jour. Utilisant les mêmes

protocoles et principes qu'Internet, dans lequel l'anonymat prime, une authentification en tant qu'employé de l'entreprise est nécessaire pour y accéder.

L'appellation Extranet qualifie la capacité d'accès, par un partenaire, au réseau local de type Intranet. Appliquant toujours les mêmes règles au niveau réseau, l'authentification reconnaît ici quelqu'un d'externe à l'entreprise, dont les privilèges seront moindres.

2. Protocole IP

2.1. Principes

IP assure une livraison des paquets sans connexion et sans garantie. Un de ses inconvénients majeurs est qu'il nécessite la mise en place d'un plan d'adressage explicite. Chaque nœud du réseau doit être identifié par une adresse IP. Celle-ci se décompose en deux parties : un numéro de réseau logique et une adresse d'hôte sur le réseau logique.

On pourrait se représenter le numéro de réseau IP comme un numéro de rue et le numéro d'hôte comme une adresse dans cette rue.

Un des aspects intéressants de IP est qu'il peut être configuré pour assurer un type de service. Parmi ceux-ci, on peut citer 'urgent' pour un paquet qui doit être transmis rapidement, 'débit important' lorsqu'une grande quantité d'informations va être transférée, 'haute fiabilité' dans la transmission qui rend compte d'un flux ne pouvant admettre une seule erreur.

2.2. Adressage IP

2.2.1. Concepts de base

Pour pouvoir recevoir des informations, chaque machine connectée sur un réseau doit pouvoir être identifiée de manière unique. On utilisera à cet effet un identifiant. Dans le cadre des réseaux TCP/IP, ces derniers porteront le nom d'adresses IP. Il s'agit en fait d'un simple numéro qui doit être unique sur l'entièreté du réseau.

Dans un souci de performance, un réseau TCP/IP sera subdivisé en sous-réseaux. Ainsi, une adresse IP possédera deux parties : une partie réseau située au début de l'adresse et une partie hôte située à la fin de l'adresse.

Exemple : NN...NNHH...HH

- N représente un bit d'adresse réseau
- H représente un bit d'adresse hôte

Les machines se trouvant sur un même sous-réseau communiqueront entre elles de manière directe. Les machines se trouvant sur des sous-réseaux différents devront passer par des routeurs. Si nous comparons cette situation à la poste classique, les sous-réseaux sont des rues. Si vous voulez envoyer une lettre à une personne habitant dans votre rue, vous la déposez directement dans sa boîte aux lettres. Sinon, vous la confiez à un facteur (le routeur) qui se chargera de la parvenir au destinataire.

2.2.2. Les adresses IP v4

Dans la version 4 du protocole IP, les adresses sont codées sur 32 bits. Elles sont représentées sous forme de 4 nombres décimaux allant de 0 à 255 séparés par des points.

Exemple : 176.26.142.26

2.2.2.1. Les classes d'adresses IP

Toutes les adresses IP sont réparties sous différentes classes. À chaque classe correspond un nombre déterminé de bits pour le réseau et pour la machine. Ce sont principalement les classes A à C qui sont couramment utilisées. Les classes D et E sont réservées à des usages particuliers.

2.2.2.1.1. Classe A

Les adresses dont le premier bit est 0 sont de la classe A. En binaire, nous aurons les adresses du type suivant :

0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

Les 8 premiers bits correspondent à la partie réseau et les autres à la partie machine. Les valeurs du premier octet de la classe A iront donc de 0 à 127. Avec des adresses de classe A, nous aurons ainsi peu de réseaux mais de très grande taille. Nous retrouverons ces adresses principalement sur des backbones.

Exemple : 114.50.49.13

2.2.2.1.2. Classe B

Les adresses dont les deux premiers bits sont 10 sont de la classe B. En binaire, nous aurons les adresses du type suivant :

10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

Les 16 premiers bits correspondent à la partie réseau et les autres à la partie machine. Les valeurs du premier octet de la classe B iront donc de 128 à 191.

Exemple : 176.26.142.26

2.2.2.1.3. Classe C

Les adresses dont les trois premiers bits sont 110 sont de la classe C. En binaire, nous aurons les adresses du type suivant :

110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

Les 24 premiers bits correspondent à la partie réseau et les autres à la partie machine. Les valeurs du premier octet de la classe C iront donc de 192 à 223. Avec des adresses de classe C, nous aurons ainsi beaucoup de réseaux de petite taille. Nous retrouverons ces adresses chez les particuliers ou sur les LAN.

Exemple : 192.168.1.34

2.2.2.1.4. Classe D

Les adresses dont les quatre premiers bits sont 1110 sont de la classe D. En binaire, nous aurons les adresses du type suivant :

1110XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

Les valeurs du premier octet de la classe D iront donc de 224 à 239. Ces adresses sont réservées pour les communications multicast.

Exemple : 226.26.12.126

2.2.2.1.5. Classe E

Les adresses dont les quatre premiers bits sont 1111 sont de la classe E. En binaire, nous aurons les adresses du type suivant :

1111XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

Les valeurs du premier octet de la classe D iront donc de 240 à 255. Ces adresses sont réservées à des usages particuliers (indéterminé).

Exemple : 246.168.1.34

2.2.2.2. Références

L'adressage IP v4 est définie dans le document rfc791.

Excercice - Conversion

Convertir en binaire les chiffres suivants :

39 > 00100111

127 > 01111111

199 > 11000111

245 > 1111 0101

Convertir en binaire les adresses IP suivantes :

32.0.10.5 > 00100000.00000000.00001010.00000101

136.254.12.1 > 10001000.11111110.00001100.00000001

192.168.0.1 > 11000000.10101000.00000000.00000001

Convertir en chiffres les binaires suivants :

00110011 > 51

01001101 > 77

10010101 > 149

Convertir en adresses IP les binaires suivants :

01001001.10110001.00100011.11111100 > 73.177.35.252

11010100.00100100.11100111.00011010 > 212.36.231.26

00011100.10010010.00101001.00101111 > 28.146.41.47

Sous forme de jeu :

https://studio.code.org/projects/applab/iukLbcDnzqgoxuu810unLw

http://www.csitechno.net/pages/jeux-pedagoludiques/conversion-binaire-decimal-jeu-des-paires.html

2.2.3. Les adresses IPv6

Avec l'essor d'internet, nous nous sommes vite retrouvés à court d'adresses IPv4. Ainsi, il a fallu trouver des solutions. Dans la version 6 du protocole IP, les adresses sont maintenant codées sur 128 bits au lieu de 32. Nous avons considérablement augmenté le nombre d'adresses et chaque appareil peut maintenant recevoir la sienne.

2.2.3.1. Représentation des adresses

Le format des adresses est un peu différent dans la version 6 que dans la version 4. Ici, elles sont formées de 8 nombres hexadécimaux de 4 chiffres séparés par des deux-points.

Exemple : abcd:ef01:2345:6789:abcd:ef01:2345:6789

Il existe un certain nombre de règles pour la représentation des adresses IPv6. Ces règles sont définies dans le document rfc5952

Les symboles hexadécimaux a à f doivent être représentés par des minuscules.

Les premiers zéros de chaque nombre doivent être omis (mais pas les derniers).

Exemple : 0123:0078:9abc:def0:1234:5678:9abc:def0 doit s'écrire 123:78:9abc:def0:1234:5678:9abc:def0

Une suite de plusieurs nombres égales à zéros (et une seule) doit être omise. S'il est possible de supprimer plusieurs suites de zéros, la suite la plus longue sera supprimée. S'il n'y a qu'un seul nombre égale à zéro, il sera représenté par un seul zéro.

Exemple : a123:0:0:def0:1234:0:0:def0 doit s'écrire a123::def0:1234:0:0:def0 ou a123:0:0:def0:1234::def0

Exemple : a123:0:0:0:def0:1234:0:def0 doit s'écrire a123::def0:1234:0:def0

Exemple : abcd:ef01:0:6789:abcd:ef01:2345:6789

2.2.3.2. Les types d'adresse

Dans l'IPv6, la notion de classe de l'IPv4 est abandonnée. Les adresses sont réparties suivant leur usage. La partie réseau de l'adresse est constituée des 64 premiers bits et la partie hôte des 64 derniers.

Adresse unicast

Il s'agit d'une adresse "normale". Elle désigne une seule machine.

Adresse anycast

Une adresse anycast représente un ensemble de machines. Lorsqu'un message sera envoyé sur cette adresse, la machine la plus proche le recevra.

Adresse multicast

Comme pour les adresses anycast, une adresse multicast représente un ensemble de machines. Toutefois, lorsqu'un message sera envoyé sur cette adresse, toutes les machines du groupe le recevront. Les huit premiers bits de ces adresses sont à 1. Ce sont donc le adresses qui vont de ff00:: à ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

2.2.3.3. Références

L'adressage IPv6 est définie dans le document rfc4291

2.2.4. Les adresses particulières

Le protocole IP définit un certain nombre d'adresses particulières. En voici un aperçu.

2.2.4.1. L'adresse zéro

En IPv4, l'adresse zéro (0.0.0.0) signifie "tout le réseau". Il s'agit en fait d'une adresse réseau. En IPv6, l'adresse zéro (::) indique une adresse indéfinie, c'est à dire une absence d'adresse.

2.2.4.2. L'adresse de bouclage (loopback)

Une adresse de bouclage (loopback en anglais) est une adresse utilisée par une interface pour envoyer un message à elle-même. Elle peut, par exemple, être utilisée lors de tests.

En IPv4, il s'agit de l'adresse 127.0.0.1. En IPv6, il s'agit de l'adresse ::1.

2.2.4.3. Les adresses locales

Les adresses locales sont des adresses qui, normalement, ne sont pas retransmises par les routeurs. Elles ne devraient donc jamais se retrouver sur un réseau global comme internet.

2.2.4.4. IP v4

En IP v4, les adresses locales sont surtout utilisées derrière un routeur NAT. C'est en général ce genre d'adresse que vous avez chez vous à la maison. Il existe des adresses locales pour les classes A, B et C. Les voici.

Classe	Adresse réseau	Première adresse	Dernière adresse
A	10.0.0.0/8	10.0.0.0	10.255.255.255
B	172.16.0.0/12	172.16.0.0	172.31.255.255
C	192.168.0.0/16	192.168.0.0	192.168.255.255

2.2.4.5. IP v6

En IP v6, il est défini deux types d'adresses locales : les adresses locales de lien (link-local) et les adresses locales globalement uniques.

2.2.4.5.1. Les adresses locales de lien (link-local)

Ces adresses sont définies pour être utilisées sur des liens n'ayant pas de routeurs, pour des configurations automatiques d'adresses ou la recherche de voisins. Ces adresses commencent par les bits 1111111010 suivis de 54 zéros et de l'adresse hôte. Il s'agit donc des adresses fe80::/64.

10 bits	54 bits	64 bits
1111111010	00000000...00000000	adresse hôte

2.2.4.5.2. Les adresses locales globalement unique

Ces adresses ont une portée plus grande que les adresses locales de lien. Elles peuvent par exemple être utilisées au sein d'une entreprise. Ces adresses commencent par les bits 11111101 suivis d'un identifiant global de 40 bits généré aléatoirement, de 16 bits d'adresse réseau et de 64 bits d'adresse hôte. Il s'agit donc des adresses fd00::/8.

8 bits	40 bits	16 bits	64 bits
11111101	identifiant global	adresse réseau	adresse hôte

2.2.5. Les sous-réseaux

Comme nous l'avons vu, l'adresse IP possède une partie réseau et une partie hôte. Pour ce qui est de l'IP v4, les adresses ont une partie réseau de 8, 16 ou 24 bits suivant la classe d'adresse. Pour ce qui est de l'IP v6, les adresses ont une partie réseau de 64 bits.

Ces masques par défaut ne permettent pas toujours de coller aux besoins particuliers de tout le monde. C'est pourquoi, il est possible de subdiviser les réseaux par défaut au moyen d'un masque de sous-réseau.

Un masque de sous-réseau est un nombre de la même taille que l'adresse. Les premiers bits sont à 1 et désignent la partie réseau. Les derniers bits sont à 0 et désignent la partie hôte.

Exemples : 111111...111111000000...000000

2.2.5.1. Notation

En IPv4, les masques de réseau peuvent se représenter comme une adresse réseau.

Exemples : 11111111111111111111111111100000 peut s'écrire 255.255.255.224 en IP v4

Une autre notation utilisée en IP v4 et seule valable en IPv6 est de faire suivre l'adresse IP d'une barre oblique / et ensuite du nombre de bit du masque de réseau.

Exemples : 11111111111111111111111111100000... peut s'écrire /27

2.2.5.2. Subdivision de réseaux

Lorsque nous avons à subdiviser des réseaux, il y a deux approches possibles. Soit nous essayons de déterminer le nombre de sous-réseaux que nous voulons obtenir, soit nous essayons de déterminer le nombre de machines par sous-réseaux.

2.2.5.2.1. Subdivision sur base du nombre de sous-réseaux

Dans ce cas-ci, nous allons agrandir le masque réseau (bits à 1) d'autant de bit qu'il est nécessaire pour obtenir le nombre de subdivisions voulu. Voici un petit tableau explicatif.

Nombre de subdivisions	Nombre de bits
2	1
3 à 4	2
5 à 8	3
9 à 16	4
17 à 32	5
etc	

Par exemple, si nous voulons subdiviser un réseau en 350, nous devons agrandir le masque de 9 bits (8 bits nous donnent 256 subdivisions et 9 bits 512).

Ainsi, en IPv4, si nous avons une adresse de classe B qui a un masque par défaut de 16 bits, nous aurons un masque de sous-réseau de 16+9 bits, soit 25 bits.

En IPv6, si nous avons un masque standard de 64 bits, nous aurons un masque de sous-réseau de 64+9 bits, soit 73 bits.

2.2.5.2.2. Subdivision sur base du nombre d'hôtes

Dans ce cas-ci, nous allons garder pour la partie machine (bits à 0) autant de bit qu'il est nécessaire pour obtenir le nombre de machines moins deux (l'adresse réseau et l'adresse de diffusion). Voici un petit tableau explicatif.

Nombre de machines	Nombre de bits
2	2
3 à 6	3
7 à 14	4
15 à 30	5
31 à 62	6
etc	

Par exemple, si nous voulons subdiviser un réseau pour qu'il contienne 40 machines par sous-réseau, nous devons garder 6 bits pour la partie hôte.

Ainsi, en IPv4, nous aurons un masque de réseau de 32-6 bits, soit 26 bits.

En IPv6, nous aurons un masque de réseau de 128-6 bits, soit 122 bits.