

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Sécurité Avancée

Pr. Abdelhak LAKHOUAJA

Département d'Informatique
Faculté des Sciences
Oujda

a.lakhouaja@ump.ma

<http://lakhouaja.oujda-nlp-team.net/>

Année universitaire : 2016/2017

Chapitre 1

Introduction aux Réseaux Informatiques

Définition d'un réseau

- Ensemble de systèmes informatiques (systèmes d'exploitation différents)
- Reliés entre eux directement ou indirectement (liaison de 2 ou plusieurs ordinateurs)
- Afin d'échanger des données (messageries, ...)
- Ou de partager des ressources (transfert de fichiers, exécution d'applications à distance)

Exemples d'applications réseaux

- **Web (www-world wide web) : il permet l'échange de pages HTML (HyperText Markup Language) en utilisant le protocole HTTP (HyperText Transfer Protocol)**
- **Email : permet l'échange de messages.**
- **Transfert et partage de fichiers : permet le transfert de fichiers entre 2 machines.**

L'ARCHITECTURE OSI

Vue globale

Application	Couches application
Présentation	
Session	
Transport	Couches flux de données
Réseau	
Liaison de données	
Physique	

Rôles des 7 couches

- 7 (application) : interface vers les programmes et/ou les utilisateurs
- 6 (présentation) : conversion de formats
- 5 (session) : synchronisation, établissement
- 4 (transport) : fiabilité/qualité de service (QoS) de bout en bout
- 3 (réseau) : échange les données via des nœuds intermédiaires
- 2 (liaison de données) : accès entre nœuds voisins
- 1 (physique) : modulation d'information élémentaire (souvent 1 bit) sur le médium
- 0 : médium de transmission

Interconnexion de réseaux (Adressage)

Adressage = identification sans ambiguïté d'une machine dans un grand réseau.

Une machine doit être accessible aussi bien par des humains que par d'autres machines, elle se présente sous la forme :

- **D'un nom (www.ump.ma)**
- **D'une adresse (196.100.20.30)**

L'adresse doit :

- **prendre en charge un grand nombre de machines**
- **faciliter la localisation**
- **être gérée au niveau mondial**

Interconnexion de réseaux (Routage)

Routage = processus permettant à un paquet d'être acheminé vers le destinataire lorsque celui-ci n'est pas sur le même réseau physique que l'émetteur .

Le routeur réalise le choix du chemin en appliquant un algorithme particulier à partir de tables de routage.

Interconnexion de réseaux (Adressage IP)

IP est un protocole à commutation de paquets :

- service sans connexion (paquets traités indépendamment les uns des autres)
- remise de paquets non garantie.

➔ Protocole non fiable

IP défini :

- une fonction d'adressage
- une structure pour le transfert des données (datagramme)
- une fonction de routage

Interconnexion de réseaux (Adressage IP)

- ◆ **Adressage binaire compact assurant un routage efficace**
- ◆ **Utilisation de noms pour identifier des machines**
- ◆ **Une adresse = 32 bits dite "internet address" ou "IP address" constituée d'une paire (n° réseau, n° machine).**
- ◆ **Cette paire est structurée de manière à définir cinq classes d'adresse**

Interconnexion de réseaux (Adressage IP)

- ✦ Une adresse se note sous la forme de quatre entiers décimaux séparés par un point, chaque entier représentant un octet de l'adresse IP :

Ex : 194.204.231.100

- ✦ Adresses particulières :

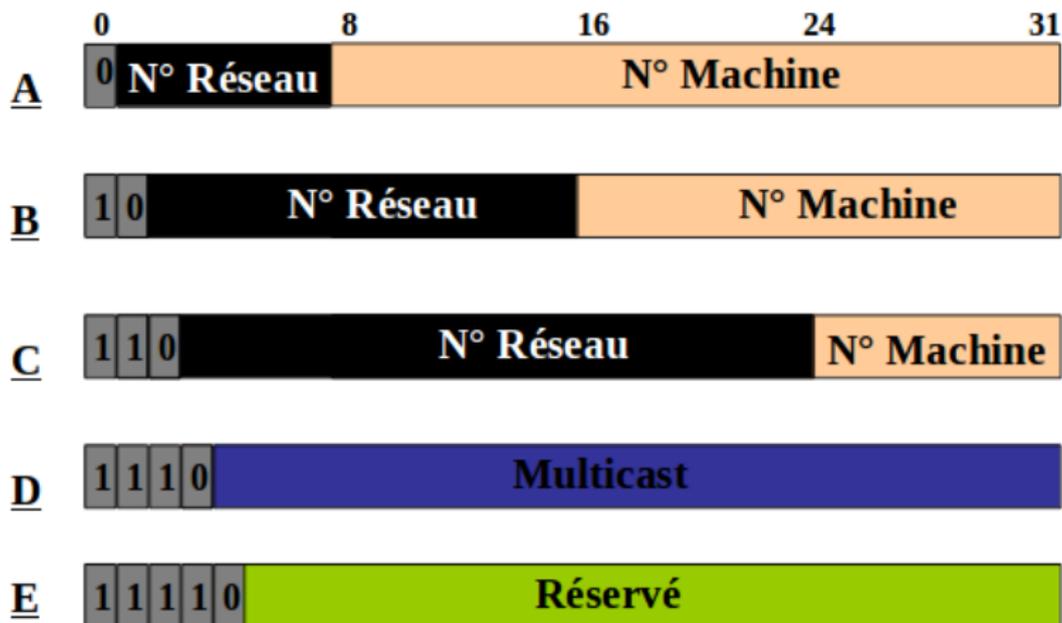
0.0.0.0 représente un hôte inconnu

255.255.255.255 représente tous les hôtes

127.0.0.1 machine locale (localhost)

→ Ces valeurs ne peuvent être utilisées comme adresses

Interconnexion de réseaux (Classes d'adresses IP)



Interconnexion de réseaux (Classes d'adresses IP)

Classe A :

Il est possible de créer $2^7 = 128$ réseaux
possédant chacun $2^{24} = 16\,777\,216$ hôtes

Classe B :

Il est possible de créer $2^{14} = 16\,384$ réseaux
possédant chacun $2^{16} = 65\,536$ hôtes

Classe C :

Il est possible de créer $2^{21} = 2\,097\,152$ réseaux
possédant chacun $2^8 = 256$ hôtes

Interconnexion de réseaux (Classes d'adresses IP)

Classe A :

000.000.000.000 → 127.255.255.255

Classe B :

128.000.000.000 → 191.255.255.255

Classe C :

192.000.000.000 → 223.255.255.255

Classe D :

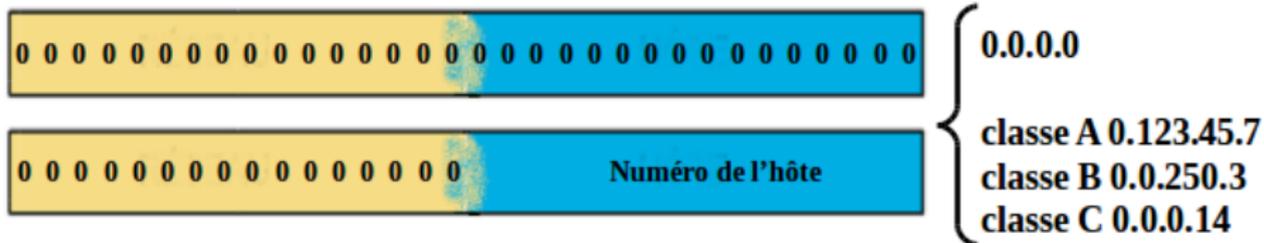
224.000.000.000 → 239.255.255.255

Classe E :

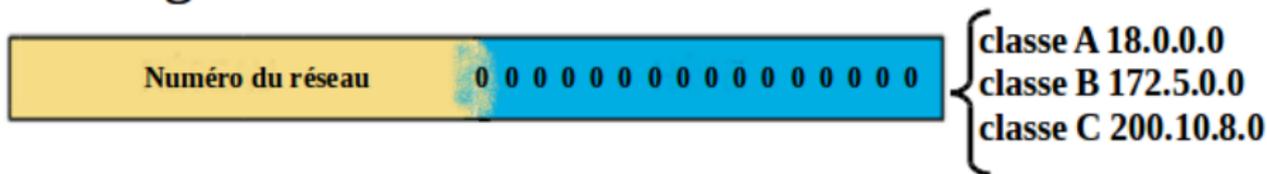
240.000.000.000 → 247.255.255.255

Adresses réservées

Désignation de la machine elle même

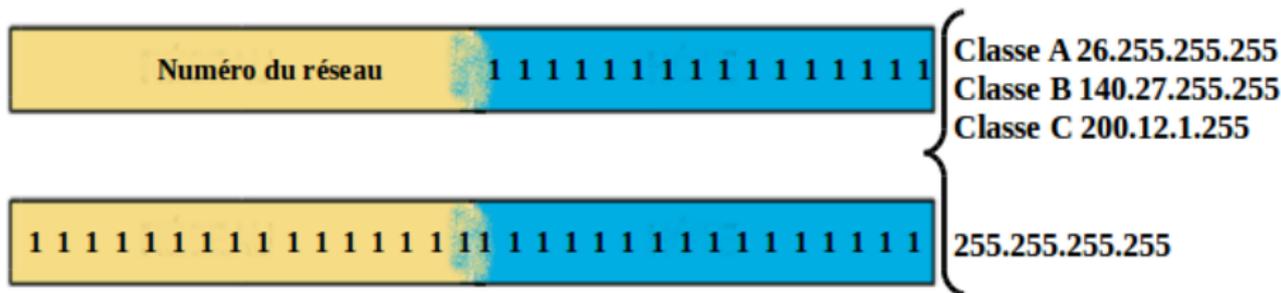


Désignation du réseau lui même



Adresses réservées (suite)

Broadcast



Boucle locale pour les tests : 127.0.0.1

Adresses privées (ou non routables)

- Adresse de classe A

10.0.0.0 ↔ 10.255.255.255

- Adresses de classe B

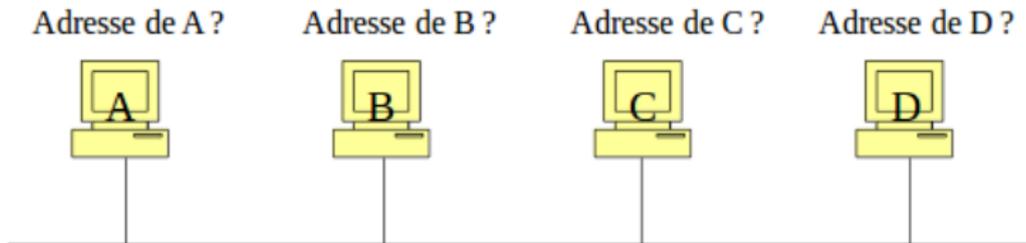
172.16.0.0 ↔ 172.31.255.255

- Adresses de classe C

192.168.0.0 ↔ 192.168.255.255

Adressage physique

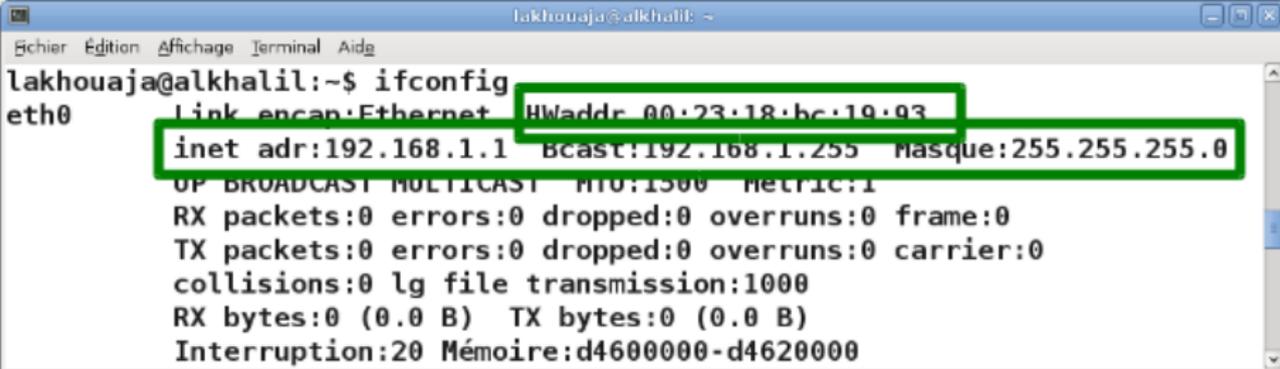
Dans le cas d'une liaison multipoint, il est nécessaire de disposer d'une adresse physique pour chaque machine.



Adresse MAC (Media Access Control)

- L'adressage MAC est codé sur 48 bits. Elle permet d'identifier de manière unique un nœud dans le monde.
- La notation hexadécimale qui est utilisé (aa-aa-aa-aa-aa-aa)
- Exemple d'adresse MAC
00-0F-20-29-54-A0

Linux : ifconfig



```
lakhouaja@alkhalil:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:23:18:bc:19:93
          inet addr:192.168.1.1  Bcast:192.168.1.255  Masque:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interruption:20 Mémoire:d4600000-d4620000
```

windows : ipconfig/all

```
C:\Windows\system32\cmd.exe
C:\Users\fso>ipconfig/all

Configuration IP de windows

Nom de l'hôte . . . . . : fso-PC
Suffixe DNS principal . . . . . :
Type de noeud . . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non

Carte Ethernet Connexion au réseau local :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : Carte Intel(R) PRO/1000 MT pour stat
Adresse physique . . . . . : 08-00-27-D6-1F-E1
Configuration automatique activée. . . : Oui
Adresse IPv4 de liaison locale. . . . : fe80::6575:3701:7fbc:4527%11(préféré)
Adresse IPv4. . . . . : 10.0.2.15(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Date d'obtention. . . . . : vendredi, 10 octobre 2013 12:16:18
```

Trame ethernet

Adresse MAC destination (48 bits)	Adresse MAC source (48 bits)	Type de trame (16 bits)	Données (46 à 1500 octets)	CRC (24 bits)
--------------------------------------	---------------------------------	----------------------------	-------------------------------	------------------

Type de trame (protocole utilisé) :

- **0x0800 : IP (Internet Protocol)**
- **0x0806 : ARP (Address Resolution Protocol)**

CRC (Cyclic Redundancy Code) :

Permet de détecter les erreurs de transmission

Protocole ARP

- ◆ **Objectif** : La communication entre machines ne peut s'effectuer qu'à travers l'interface physique or les applications ne connaissant que des adresses IP, comment établir le lien adresse IP / adresse physique?
 - ◆ **Le protocole**: ARP (Adress Resolution Protocol) permet de fournir à une machine donnée l'adresse physique d'une autre machine située sur le même réseau à partir de l'adresse IP
 - ◆ **Technique** : Une machine émet un message contenant l'adresse IP dont elle veut l'adresse physique
- La machine concernée répond; les autres machines ne répondent pas

Protocole DHCP

- ♦ **Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole de configuration dynamique d'hôtes. Il se base sur un serveur qui permet d'attribuer des adresses IP aux machines qui en font la demande.**

- ♦ **Remarque: pour limiter le nombre d'adresses allouées, il est possible de fixer une période fixe d'allocation. Juste avant la fin de cette période, la machine doit renouveler sa demande.**

Protocole ICMP

- ◆ **Beaucoup d'erreurs sont rencontrées sur l'Internet :**
 - **machine destination déconnectée**
 - **durée de vie du datagramme expirée**
 - **congestion de passerelles intermédiaires.**
- ◆ **Si une passerelle détecte un problème sur un datagramme IP, elle le détruit et émet un message ICMP (Internet Control Message Protocol) pour informer l'émetteur initial.**
- ◆ **Les messages ICMP sont véhiculés à l'intérieur de datagrammes IP et sont routés comme n'importe quel datagramme IP sur l'internet.**

Protocole ICMP

- Une erreur engendrée par un message ICMP ne peut donner naissance à un autre message ICMP (pas d'effet cumulatif)
- Les informations contenues dans un message ICMP sont :
 - TYPE** 8 bits ; type de message
 - CODE** 8 bits ; informations complémentaires
 - CHECKSUM** 16 bits ; champ de contrôle
 - HEAD-DATA** en-tête du datagramme incriminé avec 64 premiers bits des données.

DNS (Domain Name System)

♦ Objectif : Un utilisateur mémorise plus facilement un nom de machine sous forme textuelle or les applications ne connaissant que des adresses IP, comment établir le lien nom de machine / adresse IP?

♦ Le DNS

Objectif : fournir à une machine donnée l'adresse IP de la machine a atteindre.

♦ Technique :

La machine émet au serveur DNS un message contenant le nom de la machine à atteindre

La machine concernée répond en renvoyant l'adresse IP, ou sollicite un autre serveur DNS.

Le principe

- **www.ump.ma** identifie la machine www sur le réseau **ump.ma**
- Le système est mis en œuvre par une base de données distribuée au niveau mondial
- Les noms sont gérés au niveau mondial
- basé sur le modèle client/serveur
- le logiciel client interroge un serveur de noms

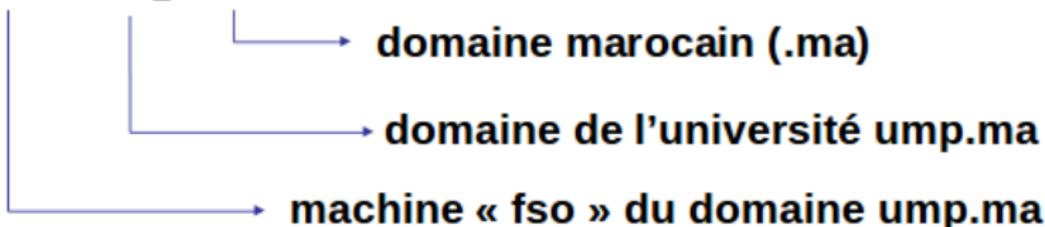
Lecture des noms de domaine

A l'inverse de l'adressage IP la partie la plus significative se situe à gauche de la syntaxe :

196.200.131.101
← vers le plus significatif

fso.ump.ma
→ vers le plus significatif

fso.ump.ma



Le protocole IP

**Internet Protocol
(Protocole Internet)**

Introduction

- Les différents réseaux hétérogènes d'Internet coopèrent grâce au protocole IP.
- IP permet l'identification de tout équipement (grâce à l'adressage IP).
- IP permet l'échange de datagrammes entre tout couple d'équipements.
- Objectif : faire le mieux possible pour transmettre les datagrammes de leur source vers leur destination.

Communication via IP

- La couche transport (protocole TCP) découpe le flux de données en datagrammes IP.
- Chaque datagramme est transmis au travers du réseau Internet. Il peut être re-découpé en fragments IP.
- À destination, tous les morceaux sont ré-assemblés par la couche réseau pour recomposer le datagramme.
- La couche transport reconstitue le flux de données initial pour la couche application.

Le service offert par IP

Le service offert par le protocole IP est dit non fiable :

- remise de paquets non garantie,**
- sans connexion (paquets traités indépendamment les uns des autres),**
- pour le mieux (best effort, les paquets ne sont pas éliminés sans raison).**

Datagramme IP

Constitué de deux parties : un entête et des données.

En-tête : partie fixe (20 octets) + partie optionnelle Variable

Données : charge utile du datagramme

Format du Datagramme IP

0	4	8	16			31
Version	Longueur entête	Type de service	Longueur totale du datagramme en octets			
Identificateur			D F	M F	Position du fragment	
Durée de vie	Protocole qui utilise IP		Total de contrôle d'entête			
Adresse IP émetteur						
Adresse IP destination						
Options (0 ou plusieurs mots)						
Données						

Champs d'en-tête

Position du fragment : localisation du déplacement du fragment dans le datagramme (13 bits)

Durée de vie (TTL) : compteur utilisé pour limiter la durée de vie des datagrammes (8 bits). Nombre maximal de routeurs que le datagramme peut traverser :

décémenté à chaque saut

détruit quand il passe à 0

Protocole : indique par un numéro à quel protocole confier le contenu du datagramme (8 bits)

6 = TCP, 17 = UDP, 1 = ICMP.

Protocole de niveau supérieur ayant créé le datagramme

Champs d'en-tête

Total de contrôle d'en-tête : vérifie la validité de l'en-tête, doit être recalculé à chaque saut (16 bits)

Adresse IP source : 32 bits

Adresse IP destination : 32 bits

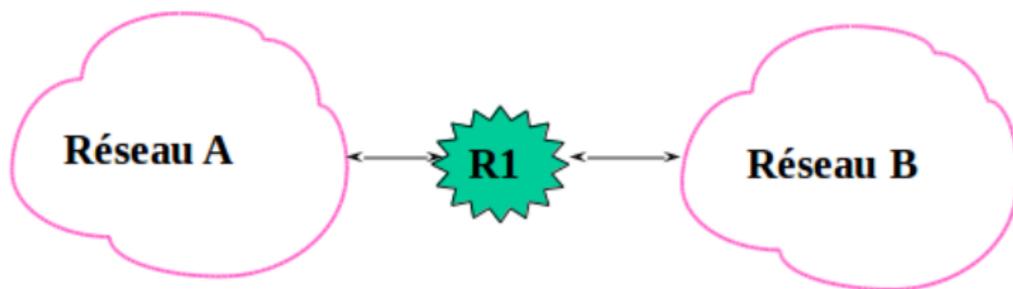
Le routage

- **Pour passer d'une machine source à une machine destination, il peut être nécessaire de passer par plusieurs points intermédiaires.**
- **Pour faire transiter des informations depuis un réseau vers un autre réseau on utilise des passerelles ou le plus souvent des routeurs.**
- **Les routeurs possèdent une connexion sur chacun des réseaux qu'ils interconnectent.**

Routeurs

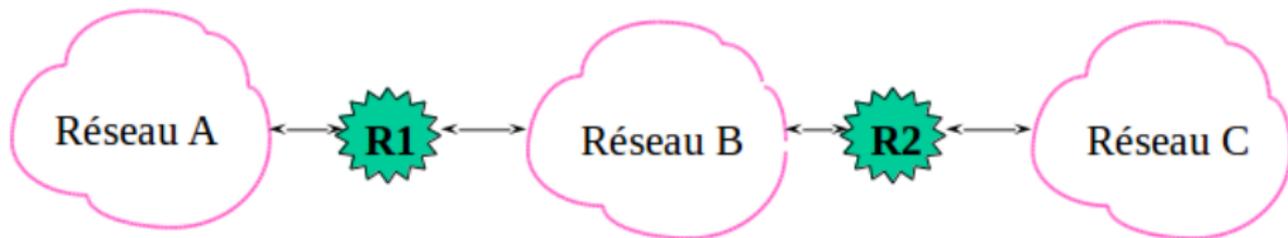
- **Les routeurs disposent de plusieurs adresses IP et plusieurs adresses physiques :**
 - **1 adresse physique par interface**
 - **1 adresse IP par réseau.**
- **Ils sont chargés de l'acheminement des paquets IP.**

Interconnexion simple



R1 transfère sur le réseau B, les paquets circulant sur le réseau A et destinés au réseau B

interconnexion multiple



- **R1 transfère sur le réseau B, les paquets circulant sur le réseau A et destinés aux réseaux B et C.**
- **R1 doit avoir connaissance de la topologie du réseau, à savoir que C est accessible depuis le réseau B.**
- **Le routage n'est pas effectué sur la base de la machine destinataire mais sur la base du réseau destinataire**

Problème du routage

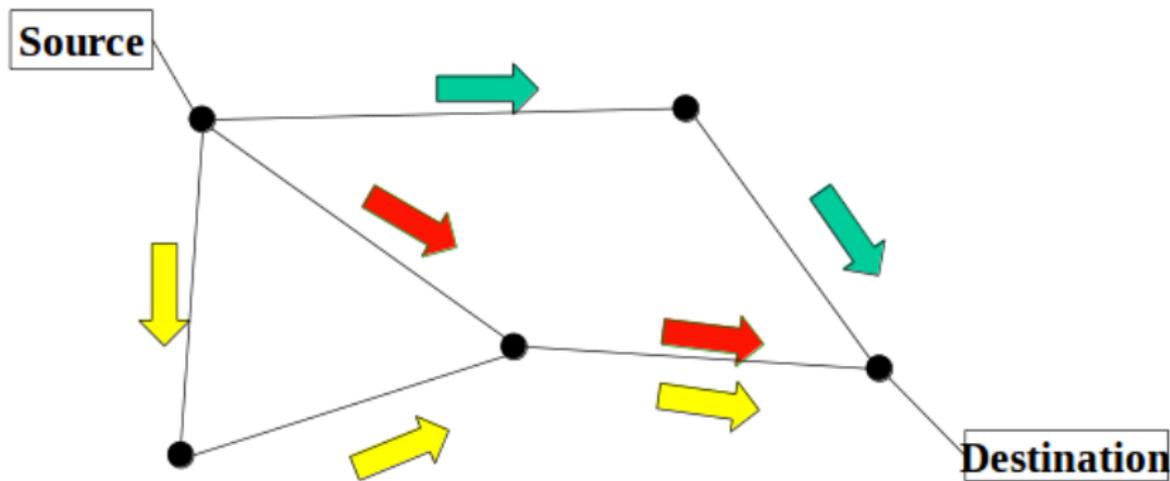


Table de routage

- Les routeurs décident de la route à faire suivre aux paquets IP par consultation d'une table de routage.
- La maintenance des tables de routages est une opération fondamentale. Elle peut être manuelle, statique ou dynamique.

Table de routage

Ne contiennent que les identifiants réseau des adresses IP.

La table contient, pour chaque numéro de réseau à atteindre, l'adresse IP du routeur le plus proche.

Chaque routeur possède une liste de couples (réseau, 0) [définit comment accéder à un réseau distant] ou (ce_réseau, ordinateur) [comment accéder à un ordinateur du réseau local].

Table de routage (exemple)

destination	masque	passerelle	interface
10.1.90.1	255.255.255.255	10.1.50.9	10.1.50.1
10.1.40.0	255.255.255.0	10.1.40.2	10.1.40.1
10.1.50.0	255.255.255.0	10.1.50.1	10.1.50.1
10.1.60.0	255.255.255.0	10.1.60.1	10.1.40.1
10.1.70.0	255.255.255.0	10.1.40.8	10.1.40.1
10.1.80.1	255.255.255.0	10.1.50.9	10.1.50.1
0.0.0.0	0.0.0.0	127.0.0.1	127.0.0.1

Le protocole UDP

User Datagram Protocol

Introduction

La couche transport d'Internet dispose de deux protocoles pour la communication entre applications :

UDP : protocole en mode sans connexion

TCP (Transmission Control Protocol) : protocole en mode orienté connexion

UDP

Service en mode non connecté

Livraison des messages sans garantie

Ordonnancement et arrivé des messages non garanti

UDP

Identification du service : les ports

les adresses IP désignent les machines entre lesquelles les communications sont établies. Lorsqu'un processus désire entrer en communication avec un autre processus, il doit adresser le processus s'exécutant cette machine.

L'adressage de ce processus est effectué selon un concept abstrait indépendant du système d'exploitation :

les processus sont créés et détruits dynamiquement sur les machines, il faut pouvoir remplacer un processus par un autre sans que l'application distante ne s'en aperçoive, il faut identifier les destinations selon les services offerts, sans connaître les processus qui les mettent en œuvre, un processus doit pouvoir assurer plusieurs services.

UDP : les ports

Ces destinations abstraites permettant d'adresser un service applicatif s'appellent des **ports** de protocole.

Port : entier identifiant l'application à laquelle la couche transport doit remettre les messages

L'émission d'un message se fait sur la base d'un port source et un port destinataire.

Les processus disposent d'une interface système leur permettant de spécifier un port ou d'y accéder.

Les accès aux ports sont généralement synchrones, les opérations sur les ports sont « tamponnés » (files d'attente).

Datagrammes UDP

Port source	Port destination
Longueur	Checksum
Données	

Port source : optionnel (identifie un port pour la réponse)

Port destination : numéro de port (démultiplexage)

Longueur : longueur totale du datagramme en octets (8 au minimum)

Checksum : optionnel (seule garantie sur la validité des données)

Classement des ports

1 - 1023 : services réservés s'exécutant avec des droits privilégiés (*root*)

1024 - 49151 : services enregistrés auprès de l'IANA et pouvant s'exécuter avec des droits ordinaires

49152 - 65535 : libres de toutes contraintes

Numéros de ports

Les derniers numéros de ports peuvent être obtenus sur le site de IANA :

<http://www.iana.org/assignments/port-numbers>

Sous Linux le fichier `/etc/services` contient les numéros de ports et les services associés.

Les ports standards

Certains ports sont réservés

<u>N° port</u>	<u>Mot-clé</u>	<u>Description</u>
7	ECHO	Echo
11	USERS	Active Users
13	DAYTIME	Daytime
37	TIME	Time
42	NAMESERVER	Host Name Server
53	DOMAIN	Domain Name Server
67	BOOTPS	Boot protocol server
68	BOOTPC	Boot protocol client
69	TFTP	Trivial File Transfer protocol
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management prot.

D'autres numéros de port (non réservés) peuvent être alloués dynamiquement aux applications

Le protocole TCP/IP

Transport Control Protocol

Introduction

S'appuie sur IP (réseau non fiable)

Communication en mode connecté

Ouverture d'un canal

Communication Full-Duplex

Fermeture du canal

TCP doit :

assurer la délivrance en séquence (Arrivée et ordre garanties)

contrôler la validité des données reçues

organiser les reprises sur erreur

réaliser le contrôle de flux

Connexion

une connexion de type circuit virtuel est établie

connexion = une paire d'extrémités de connexion

extrémité de connexion = couple (adresse IP, numéro port)

Exemple de connexion : ((124.32.12.1, 1034), (19.24.67.2, 21))

Une extrémité de connexion peut être partagée par plusieurs autres extrémités de connexions (multi-instanciation)

La mise en oeuvre de la connexion se fait en deux étapes :

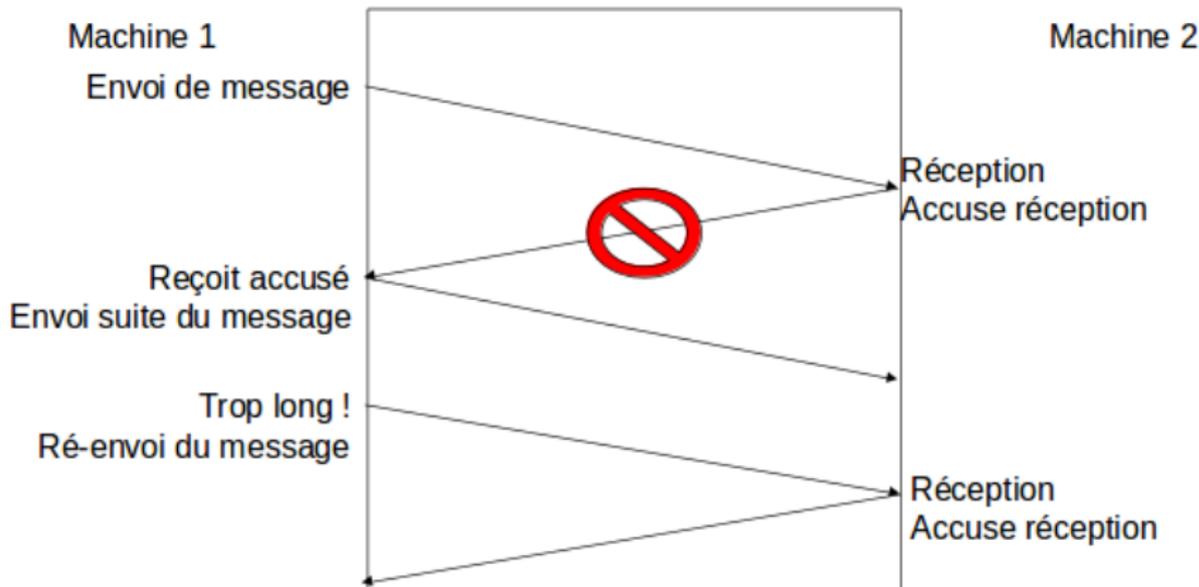
une application (extrémité) effectue une ouverture passive en indiquant qu'elle accepte une connexion entrante,

une autre application (extrémité) effectue une ouverture active pour demander l'établissement de la connexion.

Garantie de réception

Comment savoir si un paquet arrive ?

➔ Accusé de réception



Utilisation du réseau

La technique acquittement simple pénalise les performances puisqu'il faut :

Envoyer des données

Attendre

Envoyer un accusé de réception

Attendre

...

On peut faire mieux !

➔ Fenêtrage : une fenêtre de taille T permet l'émission d'au plus T messages "*non acquittés*" avant de ne plus pouvoir émettre

Notion de segment

Segment : unité de transfert du protocole TCP
pour établir les connexions
transférer les données et émettre des acquittements
fermer les connexions

Format du segment TCP

Port Source		Port Destination	
Numéro de séquence			
Numéro d'acquittement			
HLEN	Réservé	Bits de code	Taille de fenêtre
Somme de contrôle		Pointeur d'urgence	
Options			
Données			

Le contenu du segment

Port Source	Port Destination
-------------	------------------

Port (16bits) : entier identifiant l'application à laquelle la couche transport doit remettre les messages

Le contenu du segment

Numéro de séquence

Numéro d'accusé de réception

Numéro de séquence (32bits) : identifie la position des données par rapport au segment original

Numéro d'accusé de réception (32bits) : identifie la position du dernier octet reçu dans le flux entrant

Le contenu du segment

HLEN	Réservé	Bits de code	Taille de fenêtre
------	---------	--------------	-------------------

HLEN : longueur de l'en-tête

Bits de code : modificateur du comportement de TCP par caractérisation du segment

Taille de fenêtre : nombre d'octets que l'émetteur est prêt à accepter

Le contenu du segment

Bits de code

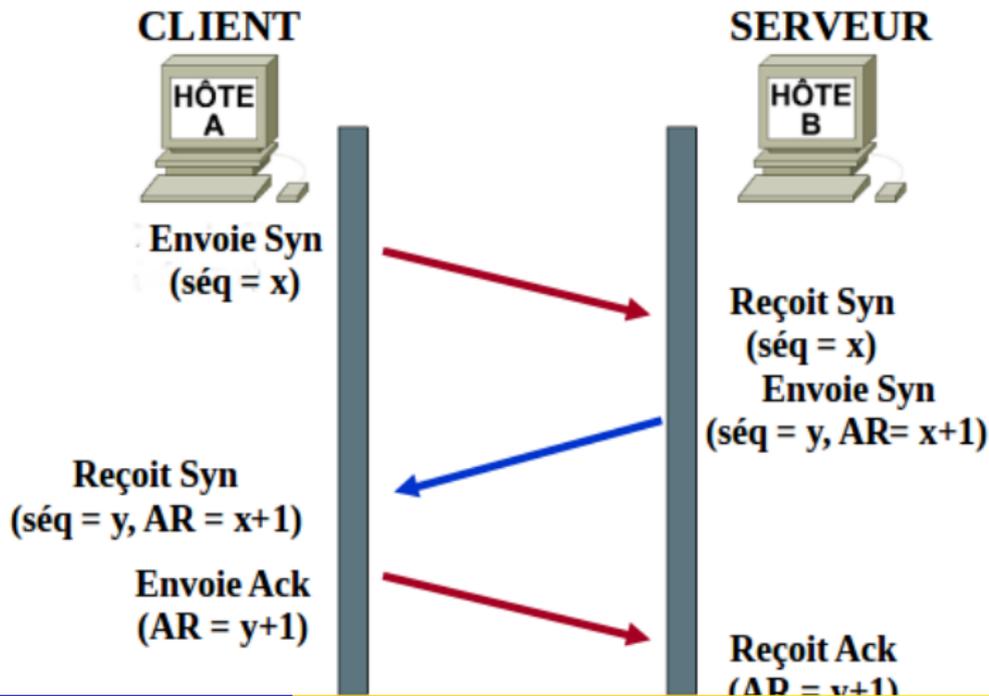
ACK : accusé de réception

RST : Re-initialisation de la connexion

SYN : début de connexion.

FIN : fin de connexion.

Connexion



Chapitre 2

Capture de données sur le réseau

La sécurité doit être prise en considération lors de l'installation et l'utilisation d'un ordinateur.

Les attaques touchent généralement les trois composantes suivantes :

- La couche d'application
- Le système d'exploitation
- La couche réseau

Cependant on distingue différentes attaques au sein d'un réseau dû à la faiblesse des composants :

- faiblesses d'authentification ;
- mauvaises configurations.
- faiblesses d'implémentation ou de bogues ;
- faiblesses liées aux protocoles.

La gestion des utilisateurs est fondamentale dans la sécurité d'un système informatique. De mauvaises privilèges ou un mauvais mot de passe peuvent compromettre la sécurité d'un ordinateur.

Lors de la création d'un nouveau utilisateur avec la commande **adduser** (par exemple **adduser smi**), le répertoire personnel de l'utilisateur **smi** est créé avec les droits `drwxr-xr-x`. Il faut enlever les droits de lecture pour les autres :

```
sudo chmod 750 /home/smi
```

Pour mettre cette valeur par défaut lors de la création d'un nouveau utilisateur avec la commande **adduser**, il faut modifier la valeur de la variable **DIR_MODE** dans le fichier **/etc/adduser.conf** de la façon suivante :

```
DIR_MODE=0750
```

Pour éviter les attaques qui utilisent un dictionnaire, le mot de passe doit être fort. Il doit :

- comporter des lettres minuscules et majuscules, des nombres et d'autres caractères ;
- comporter au moins 8 caractères ;

Il ne doit pas comporter :

- le nom ou le prénom de l'utilisateur ;
- la date de naissance de l'utilisateur ;
- un mot du dictionnaire.

Capture de données avec **tcpdump**

Sous Linux la commande **tcpdump** permet de capturer les paquets qui circulent sur le réseau. Elle peut être utilisée pour capturer les paquets qui circulent sur une interface. Le résultat du capture peut être dirigé dans un fichier qui sera analysé par un autre utilitaire tel que **wireshark**.

Cette commande nécessite des droits d'administration.

Wireshark ¹ est un outil d'analyse des réseaux qui permet de capturer et d'analyser les paquets qui circulent sur le réseau. Il peut être utilisé pour capturer les paquets qui circulent sur une interface ou pour visualiser le contenu d'un fichier qui des paquets capturés par un autre utilitaire tel que **tcpdump**. Il est multi-plateforme, il fonctionne sous Linux, Windows, MacOS, ...

1. Site officiel : <https://www.wireshark.org/>

interface de wireshark

exam_capture [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Enregistrer

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	6e:5f:98:37:0c:07	2e:18:cc:d4:8c:e7	ARP	42	Who has 192.168.1.2? Tell
2	0.000051	2e:18:cc:d4:8c:e7	6e:5f:98:37:0c:07	ARP	42	192.168.1.2 is at 2e:18:cc:
3	3.858131	192.168.1.2	192.168.1.1	TCP	74	54490 > http [SYN] Seq=0 Wi
4	3.858191	192.168.1.1	192.168.1.2	TCP	74	http > 54490 [SYN, ACK] Seq
5	3.858279	192.168.1.2	192.168.1.1	TCP	66	54490 > http [ACK] Seq=1 Acl
6	3.858509	192.168.1.2	192.168.1.1	HTTP	160	GET /xab HTTP/1.0 [Packet s

▶ Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

▶ Ethernet II, Src: 6e:5f:98:37:0c:07 (6e:5f:98:37:0c:07), Dst: 2e:18:cc:d4:8c:e7 (2e:18:cc:d4:8c:e7)

▶ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)

▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 54490 (54490), Seq: 1, Ack: 95, Len: 0

0000 2e 18 cc d4 8c e7 6e 5f 98 37 0c 07 08 00 45 00n_ .7....E.
0010 00 34 e6 64 40 00 40 06 d1 0b c0 a8 01 01 c0 a8 .4.d@.@.
0020 01 02 00 50 d4 da 98 6a d0 d0 98 60 f0 4f 80 10 ...P...j ...`.0..
0030 0b 50 b3 06 00 00 01 01 08 02 00 08 36 b4 00 08 P6

File: "/home/lakhouaja/SMI_S5/TP2/... Packets: 22 · Display... Profile: Default

Les colonnes se présentent comme suit :

No. : représente le numéro du paquet ;

Time : représente le temps de capture du paquet ;

Source : représente l'adresse IP ou MAC de la source ;

Destination : représente l'adresse IP ou MAC destination ;

Protocol : représente le type du protocole capturé ;

Length : représente la taille du paquet (en octets) ;

Info : représente une brève information concernant le paquet.

sous Linux, comme pour la commande **tcpdump**, **wireshark** ne peut pas être utilisé pour capturer des données en mode simple utilisateur. Pour capturer des données il faut passer en mode administrateur.

Description de l'interface

L'interface est découpé en trois zones :

- 1 Zone supérieure : contient l'ensemble des paquets capturés (figure suivante :)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	6e:5f:98:37:0c:07	2e:18:cc:d4:8c:e7	ARP	42	Who has 192.168.1.2? Tell
2	0.000051	2e:18:cc:d4:8c:e7	6e:5f:98:37:0c:07	ARP	42	192.168.1.2 is at 2e:18:cc:
3	3.858131	192.168.1.2	192.168.1.1	TCP	74	54490 > http [SYN] Seq=0 Wi
4	3.858191	192.168.1.1	192.168.1.2	TCP	74	http > 54490 [SYN, ACK] Seq
5	3.858279	192.168.1.2	192.168.1.1	TCP	66	54490 > http [ACK] Seq=1 Ac
6	3.858509	192.168.1.2	192.168.1.1	HTTP	160	GET /xab HTTP/1.0 [Packet s

- 2 Zone centrale : affiche les détails d'un paquet sélectionné sous forme de couches (figure suivante :)

```
▶ Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▶ Ethernet II, Src: 6e:5f:98:37:0c:07 (6e:5f:98:37:0c:07), Dst: 2e:18:cc:d4:8c:e7 (2e:18:cc:d4:8c:e7)
▶ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.2 (192.168.1.2)
▶ Transmission Control Protocol, Src Port: http (80), Dst Port: 54490 (54490), Seq: 1, Ack: 95, Len: 0
```

- 3 Zone inférieure : présente le paquet sous format octale et ASCII (figure suivante :)

```
0000 2e 18 cc d4 8c e7 6e 5f 98 37 0c 07 08 00 45 00  . . . . .n_ .7...E.
0010 00 34 e6 64 40 00 40 06 d1 0b c0 a8 01 01 c0 a8  .4.d@.@. ....
0020 01 02 00 50 d4 da 98 6a d0 d0 98 60 f0 4f 80 10  ...P...j ...'0..
0030 0b 50 b3 06 00 00 01 01 08 0a 08 08 36 b4 00 08  P          6
```

Il est possible de ne pas afficher tous les paquets on les filtrant. Par exemple, on peut afficher juste les paquets **http**, en tapant **http** dans la zone **Filter** :. Il est possible aussi d'utiliser des expressions.

Exemples de filtres

Filtre/expression	Signification
tcp	afficher seulement les paquets TCP
ip.src==192.168.1.2	afficher seulement les paquets qui sortent de 192.168.1.2
ip.dst==192.168.1.1 && http	afficher les paquets HTTP qui partent vers 192.168.1.2
ip && !udp	afficher les paquets IP mais n'afficher pas les paquets UDP

Il faut identifier les services qui doivent être accessibles de l'extérieur, comme un serveur Web, ou un serveur DNS. Les machines qui abritent ces services devront être visibles de l'Internet.

Les autres ordinateurs :

- serveurs internes
- ordinateurs personnels

ne doivent pas être visibles de l'extérieur.

Par contre, il faut qu'ils accèdent à l'Internet.

→ C'est-à-dire, une connexion TCP depuis un de ces ordinateurs est autorisée, par contre, mais une connexion de l'extérieur vers le même ordinateur sera interdite.

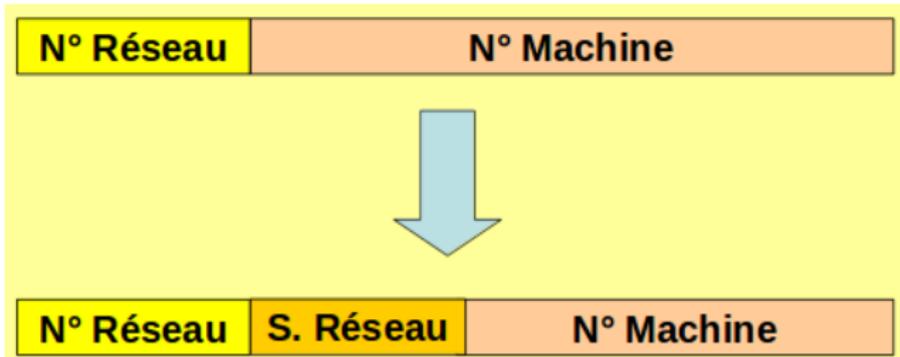
Pour sécuriser un réseau, il faut :

- segmenter le réseau en sous-réseaux ;
- utiliser des filtres ;
- utiliser un pare-feu.

segmenter le réseau en sous-réseaux

Dans le but de séparer les machines sensibles des autres machines, on peut découper un réseau en plusieurs sous-réseaux, alors que l'ensemble continue à se comporter comme un seul réseau vis-à-vis de l'extérieur.

Dans l'adresse IP, le champ d'identification de l'ordinateur est subdivisé en 2 parties : N° sous réseau et N° machine.



segmenter le réseau en sous-réseaux

Pour réaliser un découpage du réseau, on dispose des masques de sous réseaux (subnet mask).

Sans découpage, les bits correspondant au N^o réseau sont tous mis à 1, les autres à 0.

Masques par défaut

Classe A :

11111111.00000000.00000000.00000000 → 255.0.0.0

Classe B :

11111111.11111111.00000000.00000000 → 255.255.0.0

Classe C :

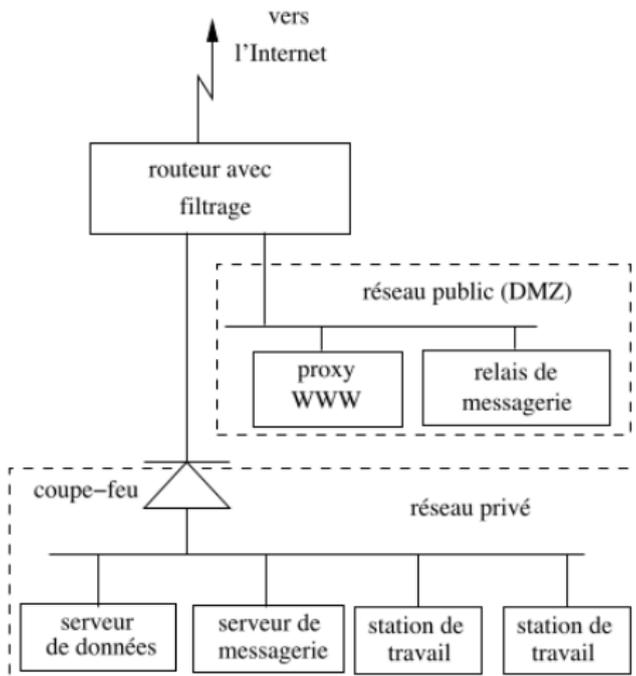
11111111.11111111.11111111.00000000 → 255.255.255.0

Les règles d'accès et de trafic appliquées aux réseaux consistent à établir quels sont les type de paquets (en termes de protocole et de numéro de port) autorisés en entrée ou en sortie depuis ou vers tel réseau ou telle adresse particulière.

→ un serveur web pourra recevoir et émettre du trafic HTTP (port 80) mais n'aura aucune raison de recevoir un autre trafic sur le port 22 (protocole SSH). Appliquer ce genre de règles, c'est faire du filtrage par port.

- Le sous-réseau public (souvent appelé « zone démilitarisée » ou DMZ) devra faire l'objet de mesures de sécurité particulièrement strictes. Il est exposé à toutes les attaques en provenance de l'Internet.
- Le principe de base est : tout ce qui n'est pas autorisé est interdit.
- Il est prudent que les serveurs en zone publique contiennent aussi peu de données que possible. Idéalement, ils ne doivent pas contenir de données pour éviter qu'ils soient la cible d'attaques

Filtrage



Tiré du Livre : Sécurité Informatique - Principes Et Méthodes 2ème Edition (Eyrolles).

Les Firewall (Pare Feu)

Un **pare-feu** est un ensemble matériel ou logiciel qui trie les paquets qui circulent par son intermédiaire en provenance ou vers le réseau local, et ne laisse passer que ceux qui vérifient certaines conditions.

C'est un système de protection dédié à la sécurité d'un réseau.

Les noyaux Linux contiennent le système **Netfilter** pour manipuler le trafic réseau. Pour accepter, manipuler ou rejeter un paquet, on utilise **iptables**.