

Laboratoire Réseau

Année 2004-2005

Cours dispensé par Madame Buseyne,
Notes de cours, réalisée par madame Buseyne.

Notes introductives :

Ce document rassemble l'ensemble des documents fournis par madame Buseyne.

Sur le petit travail de concaténation des différents fichiers que j'ai pu réaliser, j'ai constaté de nombreuses anomalies dans le développement des chapitres et parties. Je crains que ce document ne soit pas complet. N'hésitez pas à me demander l'original en .doc pour y apporter vos corrections et modifications si vous le souhaitez.

Elfi

Sommaire

1. Installation d'une machine en réseau et dépannage	5
1.1.Qu'est-ce qu'un réseau ? A quoi sert –il ?.....	5
1.2.Domaine et groupe de travail.....	5
1.2.1. Groupe de travail.....	5
1.2.2. Domaine.....	5
1.3.Le modèle OSI.....	6
1.4.Installation hardware.....	6
1.4.1.Architecture en couches	6
1.4.2.Cartes réseaux.....	6
1.4.3.Câbles	7
1.5.Installation logicielle.....	7
1.5.1.Architecture en couches.....	7
1.5.2.Qu'est-ce qu'un service ?.....	7
1.5.3.Qu'est-ce qu'un protocole ?.....	8
1.5.4.Qu'est-ce qu'un client ?.....	8
1.5.5.Partage des fichiers et imprimante.....	8
1.5.6.L'architecture TCP/IP.....	8
1.5.7.Envoi des messages textes sur le réseau.....	9
1.6.Dépannage.....	9
1.6.1.Problèmes de réseau.....	9
1.6.2.Résolution des problèmes.....	9
1.6.3.Etapes à réaliser pour vérifier que la machine fonctionne correctement avec le protocole TCP/IP ?.....	10
1.6.4.Procédure de dépannage.....	10
1.6.5.Outils de dépannage.....	11
Moniteur de réseau :	11
2. Relier 2 ordinateurs en réseau.....	12
2.1. Le matériel à adopter.....	12
2.1.1. Les cartes réseau.....	12
2.1.2. Les câbles.....	12
2.1.2.1. Les paires torsadées non blindées (UTP : Unshielded Twisted Pairs).....	12
2.1.2.2. Les paires torsadées blindées	15
2.2. Fabrication du câblage RJ45 croisé.....	15
2.3. Contrôle du câble	15

2.3.1. Pourquoi un testeur de câble ?.....	15
2.3.2. Fonctionnement du testeur de câble CableMeter de Fluke	16
2.3.3. Connexions RJ45, règles de câblage et problèmes de liaisons.....	17
Dédoubler un câble RJ45.....	18
2.5.La partie logicielle.....	19
3. Protocoles.....	20
3.1 Introduction.....	20
3.2. Protocole TCP/IP.....	20
Définition, caractéristiques.....	21
3.1.2. Avantages et inconvénients.....	21
6.Avantages.....	21
7.Inconvénients.....	22
3.2. Protocole TCP.....	22
3.3. Protocole IP.....	23
Protocole ARP.....	25
Rôle.....	25
Résolution d'adresse avec arp.....	25
Mémoire cache de ARP.....	25
Structure des paquets ARP.....	25
Protocole ICMP.....	25
Rôle.....	25
Structure des paquets ICMP.....	25
Voir en plus le fichier suivant :	26
4. Adressage IP et masque de sous-réseau.....	26
4.1 Adresse IP	26
4.2. Masque de sous-réseau.....	27
4.3. IP version 6.....	30
5. Routage IP	31
5.1. Routage.....	31
Définitions.....	31
Fonctionnement d'une communication.....	31
Table de routage.....	31
Définition.....	31
5.1.3.2. Eléments constitutifs d'une table de routage.....	31
5.1.3.3. Quelques adresses particulières.....	32
5.1.4. Routage statique.....	32
5.1.5. Routage dynamique.....	32
6. Notions de cryptographie.....	33
6.1. Définition.....	33
6.2. Confidentialité	33
6.2.1. Clé symétrique (cryptage à clé secrète).....	33
6.2.2. Clés asymétriques (cryptage à clé publique).....	34
6.3. Intégrité des données.....	35
6.4. Authentification.....	36
6.5.1. Signature électronique.....	36
6.5.2. Certificat et autorité de certification.....	36

6.6. Algorithmes d'échanges de clés PKI et PKCS.....	36
6.7. Les logiciels PGP et GNUPG.....	37
6.8.2. Protéger sa clé privée.....	37
6.8.3. Obtenir une clé publique.....	37
Exemple.....	37
6.8.4. Enregistrer une clé publique dans son trousseau (keyring).....	37
Notes (à lire attentivement).....	38
6.8.5. PGP, ça marche comment, concrètement ?	38
Voir en complément le site suivant :.....	40
7. Réseau privé virtuel (VPN).....	40
7.1. Objectifs du VPN.....	40
7.2. Principes de base.....	40
7.2.1. Technologies VPN.....	40
7.2.2. PPTP.....	40
7.2.3. L2TP	40
7.2.4. IPSec.....	41
7.2.3.1. ESP(Encapsuling Security Payload).....	41
7.2.3.2. AH(Authentication Header)	42
7.2.3.3. Etablissement d'un tunnel IPSec	42
7.3. Comment fonctionne un VPN ?.....	42
7.4. Implémentation d'un VPN.....	43
Implémentation d'un VPN de façon logicielle.....	43
Implémentation d'un VPN avec matériel	43
Annexes :.....	44

1. Installation d'une machine en réseau et dépannage

1.1. Qu'est-ce qu'un réseau ? A quoi sert-il ?

Un réseau est un système permettant à plusieurs appareils (ordinateurs, périphériques, automates, ...) d'échanger des informations. Un réseau peut être filaire c'est-à-dire composé de câbles et éléments permettant d'envoyer les données sur ces câbles. Un réseau peut être un réseau sans fil c'est-à-dire il envoie les informations par l'intermédiaire des ondes, de l'infrarouge.

Les intérêts d'un réseau sont :

- le partage des données
- le partage des ressources (matériel informatique pouvant être accessible en réseau, par exemple une imprimante)
- le partage d'applications
- le travail coopératif
- l'intranet (site Internet accessible uniquement à l'intérieur du réseau local en lançant un navigateur) et l'extranet (configuration réseau permettant d'accéder à un intranet, et donc à tous ses services, depuis un point extérieur au réseau local).

1.2. Domaine et groupe de travail

1.2.1. Groupe de travail

Dans le cas de groupe de travail, on parle de réseau d'égal à égal (peer to peer). Chaque ordinateur contrôle ses propres informations et ses propres ressources. Il n'y a pas d'ordinateur central pour contrôler le réseau.

Caractéristiques :

- pour les réseaux de petites tailles
- les applications sont installées sur chaque ordinateur
- chaque utilisateur doit administrer sa propre machine
- tous les ordinateurs ont les mêmes droits

1.2.2. Domaine

Ensemble d'ordinateurs et d'utilisateurs d'un réseau microsoft qui se partagent une base de comptes et une stratégie de sécurité communes, stockées sur un contrôleur de domaine Windows NT Server ou Windows 2000 Server. Chaque domaine possède un nom spécifique.

Dans le cas d'un domaine, on parle de réseau client/serveur.

Un serveur central délivre les informations à d'autres ordinateurs appelés clients.

Le serveur (ordinateur plus puissant que les clients) met donc les informations et les ressources à la disposition des autres ordinateurs au sein du réseau.

Le client est un ordinateur qui peut utiliser les services d'un serveur et accéder aux informations qui y sont stockées.

Caractéristiques :

- identifier et surveiller utilisateurs
- authentification centralisée
- administration centralisée
- sécurité accrue

- installation des applications une seule fois sur le serveur

1.3. Le modèle OSI

Pour parvenir à une interopérabilité des solutions réseau incompatibles développaient au début des années 70, l'ISO (International Standards Organization) a proposé le modèle OSI (Open System Interconnection) en 1984. Ce modèle harmonise le processus général de communication en le découpant en 7 couches structurées.

Chaque couche s'appuie sur l'ensemble des services apportés par les couches inférieures (sans se préoccuper de la façon dont les couches inférieures effectuent son travail) et immédiatement supérieure à qui elle offre ses propres services.

Le modèle OSI comprend 7 couches. Chaque couche remplit des fonctions spécifiques.

1.4. Installation hardware

1.4.1. Architecture en couches

La partie physique du réseau représente les couches n°1 et n°2 du modèle OSI. Une fois l'adaptateur réseau correctement déclaré, le réseau (Ethernet, Novell, ...) devient totalement transparent aux couches 3 à 7, dont aussi aux administrateurs réseau, aux utilisateurs et il ne faut plus s'en occuper.

La couche n°1 (la plus basse) s'appelle la couche physique. Elle assure la transmission des bits sur le circuit de communication (média).

Elle définit les supports de transmission et les équipements de connexion à différents points de vue:

- mécanique: dimensions des connecteurs, nombre de pins de connexion...
- électrique: codage des bits en voltages ...
- fonctionnel: traduction des voltages reçus en bits
- procédurax: ordre des événements, règles de séquence ...

La couche n°2 s'appelle la couche de liaison de données. Elle transforme la ligne de transmission qu'on lui fournit en une ligne sans erreurs. Les interférences (parasites) peuvent modifier le signal envoyé.

Elle détecte les erreurs possibles, corrige les éventuelles erreurs trouvées

Elle fractionne les données en trames (frames).

Elle transmet les données en séquence.

Format d'une trame:

Adresse émetteur	Adresse récepteur	Données
------------------	-------------------	---------

Elle gère les trames d'acquittement (validation de la transmission).

IEEE (Institute of Electrical and Electronics Engineers) a décomposée cette couche en 2 sous-couches :

- la couche MAC (Medium Access Control) : s'occupe de l'accès au média, contrôle les moyens par lesquels plusieurs entités partagent le même canal de transmission (méthodes d'accès).
- la couche LLC (Logical Link Control) : assure la détection et la correction des erreurs ainsi que le contrôle de flux.

1.4.2. Cartes réseaux

(voir cours de périphériques)

Adresse physique :

Pilote de la carte (couche 2 du modèle OSI) : gère la communication entre la carte et le système

d'exploitation.

Vérification de l'installation correcte : la led doit être allumée à l'arrière quand on connecte la carte au réseau.

1.4.3. Câbles

(voir chapitre 2 : Interconnexion de 2 machines en réseau)

1.5. Installation logicielle

1.5.1. Architecture en couches

Le système d'exploitation de réseau ou gestionnaire de réseau et ses utilitaires permettent l'organisation logique du réseau et notamment le partage des ressources (fichiers, répertoires, applications, imprimantes), la définition des utilisateurs autorisés, des mots de passe, ...

Les couches moyennes et hautes (3 à 7) du modèle OSI représentant le réseau logique.

La couche n°3 s'appelle la couche réseau. Elle règle l'acheminement des données (groupées en paquets) d'un bout à l'autre du sous-réseau (*routage*).

Elle gère les problèmes pouvant survenir en cas de différence de protocole entre deux nœuds du *sous-réseau* (connexion de réseaux hétérogènes).

Elle se choisit un itinéraire en fonction de l'adresse de l'émetteur et de l'adresse du récepteur (adressage).

La couche n°4 s'appelle la couche transport. Elle est une couche charnière entre les couches inférieures, orientées transmission, et les couches supérieures, orientées application.

Elle offre aux couches supérieures un service de transmission de bout en bout suivant un niveau de qualité déterminé.

Elle permet le contrôle du flux, la gestion des erreurs et des problèmes relatifs à l'envoi et à la réception des paquets.

La couche n°5 s'appelle la couche session. Elle assure les modalités de contrôle entre 2 correspondants.

Elle fournit des services pour établir, maintenir et libérer une connexion

La couche n°6 s'appelle la couche présentation. Elle s'occupe du cryptage et de la compression des données

Elle gère la traduction des données, la conversion des protocoles.

La couche n°7 s'appelle la couche application. Elle gère l'interface avec l'utilisateur.

Elle contient les applications, les données à transmettre.

1.5.2. Qu'est-ce qu'un service ?

Programme, routine ou processus qui effectue une certaine tâche système permettant d'exécuter

d'autres programmes, en particulier au niveau du matériel.

Exemples : SAM (Security Accounts Manager, FRS(File Replication Service), telnet, routage et accès distant, ...[\(manage computer- services and applications – services\)](#)

Le service qui doit être rendu au niveau N de l'architecture est défini par le service N. Il est réalisé par un ensemble d'actions devant être effectuées au niveau N. Les services N sont fournis par une entité N à une entité N+1 aux points d'accès aux services N.

1.5.3. Qu'est-ce qu'un protocole ?

Un protocole est une langue qui permet la compréhension du contenu des paquets (segment de données) et donc aussi des données.

Un protocole de niveau N définit l'ensemble des règles nécessaires à la réalisation du service de niveau N. Ces règles définissent les mécanismes qui vont permettre de transporter les informations d'un niveau N à un niveau N correspondant au service N.

Les machines d'un réseau ne peuvent pas se comprendre s'ils utilisent des protocoles (format de paquets) différents. Une machine supportant plusieurs protocoles est accessible à toute machine équipée de l'un des protocoles.

1.5.4. Qu'est-ce qu'un client ?

Un client permet à un système d'exploitation d'accéder aux ressources de machines fonctionnant sous un autre système d'exploitation.

Exemple :

Client for Netware Networks : permet aux ordinateurs utilisant un Système d'exploitation Microsoft d'accéder aux ressources d'ordinateurs fonctionnant sous NetWare et les partager.

1.5.5. Partage des fichiers et imprimante

[Montrer comment partager une imprimante en réseau => A faire \(p 91...\)](#)

[Montrer comment partager un répertoire => A faire](#)

1.5.6. L'architecture TCP/IP

(voir chapitre 3 : Architecture TCP/IP)

Adresse IP : identifie l'emplacement d'un système sur le réseau tcp/ip (adresse logique sur 32 bits)

Passerelle (routeur) par défaut : connecte le sous-réseau à d'autres segments du réseau.

Masque de sous-réseau : identifie la partie d'une adresse Ip correspondant à l'identificateur réseau (sous-réseau) du segment physique.

DNS (Domain Name System): (voir cours de réseau de 3ème)

Le rôle principal du service de nom de domaine consiste à présenter des noms pour les utilisateurs, puis à les convertir en adresses IP. La base de données DNS est une arborescence appelée espace de nom de domaine. Un nom est attribué à chaque domaine. Chaque domaine peut contenir des sous-domaines. Le nom de domaine identifie la position du domaine dans la base de données par rapport à un parent.

NSLOOKUP est un utilitaire de ligne de commande permettant de tester et dépanner une configuration DNS.

WINS (Windows Inetrnet Name Service) :

Le service WINS fournit une base de données dynamique qui gère les correspondances entre nom

d'ordinateur NETBIOS et adresse IP.

DHCP (Dynamic Host Configuration Protocol)

Le protocole serveur DHCP centralise et gère l'allocation de configuration du protocole TCP/IP en affectant automatiquement des adresses IP à des ordinateurs configurés pour utiliser DHCP.

Fonctionnement : A chaque démarrage, le client DHCP demande au serveur DHCP ces informations de configurations TCP/IP. Lorsqu'un serveur DHCP reçoit une demande, il sélectionne une adresse IP dans un groupe d'adresses défini dans sa base de données et la propose au client DHCP. Si le client l'accepte, l'adresse IP est louée au client pour une durée déterminée. S'il n'existe pas d'adresse IP disponible, le client ne peut pas initialiser le protocole TCP/IP.

1.5.7. Envoi des messages textes sur le réseau

L'utilitaire NET, utilisable en mode texte permet d'envoyer des messages en mode texte.

Pour obtenir de l'aide sur NET, il faut taper la commande : NET HELP.

Pour avoir de l'aide sur l'envoi de messages avec Net, il faut taper la commande NET HELP SEND. Il est possible d'envoyer un message à un groupe de travail ou à un utilisateur particulier.

1.6. Dépannage

1.6.1. Problèmes de réseau

La plupart des problèmes de réseau surviennent au niveau des câbles et de leurs connecteurs, des cartes ou encore des hubs. Dans la plupart des cas, les problèmes surviennent au niveau de la couche Physique du modèle OSI.

Un câble peut faire l'objet d'un court-circuit ou d'une rupture, ou il peut être raccordé à un connecteur défectueux.

Une carte défectueuse ou avec mauvais pilote.

1. Pour le câble réseau: câble défectueux, dépairé, trop long, ...(voir chapitre 2)
2. Pour la carte réseau : mauvais pilotes, ... (voir cours de périphérique)
3. Pour hubs
4. Dans le voisinage réseau, l'ordinateur ne se reconnaît pas lui-même.
5. Problèmes au niveau du routage (voir chapitre 4)
6. Problèmes au niveau des applications , des utilisateurs .

1.6.2. Résolution des problèmes

1. * Problèmes de câblage (voir MCSE page 426)
 - ↪ déconnecter le câble et tester avec un autre
 - ↪ veiller à ce que tous les connecteurs soient fermement et correctement connectés, que les longueurs soient respectées, que le nombre maximal de machines soient respecté.
 - ↪ Veiller à ce que le brochage des connecteurs soit correct et fermement serti
 - ↪ Rechercher les interférences électriques qui peuvent être provoquées

lorsque le câble du réseau et les cordons d'écran et d'alimentation sont liés.

2. S'assurer que le câble est correctement connecté à la carte, que le gestionnaire de carte est adéquat et qu'il a été bien installé et que la carte est liée au protocole de transport approprié. S'assurer que la carte et son gestionnaire soient compatibles avec le système d'exploitation. Faire des tests pour détecter tout conflit de ressources éventuel. Vérifier qu'aucun autre matériel ne tente d'utiliser les mêmes ressources.
Lancer le programme de diagnostic de la carte.
Remplacer la carte par une autre pour voir si elle est HS.

Si la carte est bien installée une led est allumée
(voir MCSE page 428)

3. Connexions hub et ordinateur et carte réseau (pilote OK) OK (voir mcse p429)
4. pilotes non ou mal installés, nom de machine incorrect, nom de machine en double sur le réseau, adresse ip en double sur le réseau, problème de protocole (non ou mal installé)
Vérifier que le partage fichier/imprimante est activé
Adresse IP déjà attribuées
Pas de partage de ressources activés

1.6.3. Etapes à réaliser pour vérifier que la machine fonctionne correctement avec le protocole TCP/IP ?

Les étapes suivantes permettent de vérifier la configuration d'un ordinateur et de tester les connexions de routeur.

1. Utiliser la commande IPCONFIG pour vérifier que la configuration TCP/IP a été initialisée.
2. Utiliser la commande PING sur l'adresse de bouclage (127.0.0.1) pour vérifier que TCP/IP est installé et chargé correctement.
3. Utiliser la commande PING sur l'adresse IP de la station de travail pour vérifier qu'elle a été ajoutée correctement et pour rechercher d'éventuelles adresses IP identiques.
4. Utiliser la commande PING sur l'adresse IP de la passerelle par défaut pour vérifier que cette passerelle fonctionne et que l'ordinateur peut communiquer avec le réseau local.
5. Utiliser la commande PING sur l'adresse IP d'un hôte distant pour vérifier que l'ordinateur peut communiquer via un routeur.

Conseil : Commencer à l'étape 5. En effet, si l'opération aboutit, les étapes 1 à 4 seront réussies par défaut.

1.6.4. Procédure de dépannage

En 5 étapes :

1. Définir la priorité du problème : définir le degré d'importance du problème par rapport aux autres
2. Recueillir des informations pour identifier les symptômes
3. Dresser une liste des causes possibles
4. Réaliser des tests pour isoler la cause
5. Etudier les résultats du test pour trouver une solution.

1.6.5. Outils de dépannage

Analyseur de protocole :

Equipement matériel et logiciel est employé pour surveiller le trafic réseau, ses performances et analyser les paquets (voir 3. Architecture TCP/IP). Il peut identifier les goulots d'étranglements, les problèmes de protocoles et les composants réseaux qui ne fonctionnent pas correctement. (faire démo analyseur)

Moniteur de réseau :

Outil logiciel permet de surveiller le trafic du réseau en affichant des informations de paquet et en conservant des statistiques sur l'exploitation du réseau. Il rassemble des informations sur les types de paquet, sur les erreurs et sur le trafic en provenance et à destination de chaque ordinateur. (à montrer – Outils d'administration/moniteur réseau)

Testeur de câblage :

(Voir 2. Mise en réseau de 2 machines)

2. Relier 2 ordinateurs en réseau

2.1. Le matériel à adopter

2.1.1. Les cartes réseau

(voir cours de périphériques)

2.1.2. Les câbles

Les caractéristiques des câbles sont :

- la vitesse de propagation :
- l'affaiblissement (proportionnel à la vitesse parcourue)
- la paradiaphonie (perturbations entre deux paires d'un même câble)
- le rapport signal/bruit (dépend du niveau du signal émis, des perturbations environnantes, de la longueur de la liaison)

Les caractéristiques mesurables pour les câbles sont :

- type de câble : UTP, FTP, STP, coax, fibres optiques
- standard de câblage : EIA/TIA 4-PR, 10BASE-T 2PR, TOKEN RING 2PR,
- catégorie de câble : pour UTP (cat5, cat4, cat3), pour STP (IBM Type 1, IBM Type 6)

IEEE fixe les normes sur les câbles.

Tout câble sera décrit par trois éléments :

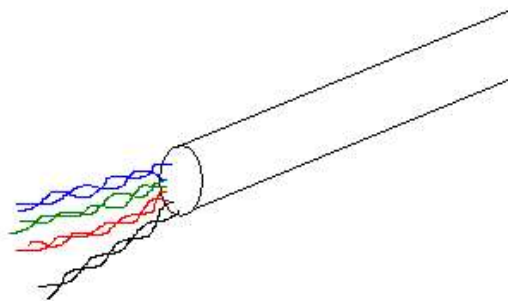
- o Vitesse de transmission (MB/s)
- o Utilisation de canal (Base ou broad)
- o Longueur maximale d'un segment de câble sans subir d'atténuation par 100 mètres

Ex : 10 BASE 2 : câble à 10MB/s fonctionnant en bande de BASE sur 200 mètres max (en théorie, 185 m en réalité).

Pour relier 2 ordinateurs en réseau, il faut utiliser un câble RJ45 croisé.

2.1.2.1. Les paires torsadées non blindées (UTP : Unshielded Twisted Pairs)

- Description :



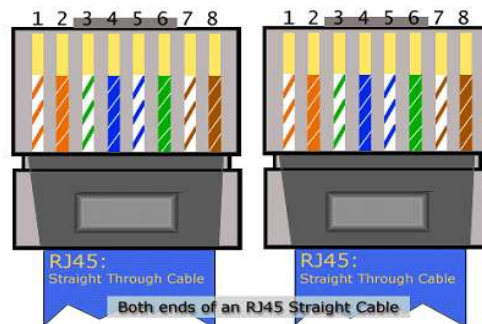
Les câbles ne sont pas protégés contre les radiations électromagnétiques extérieures.

Les paires sont torsadées deux à deux :

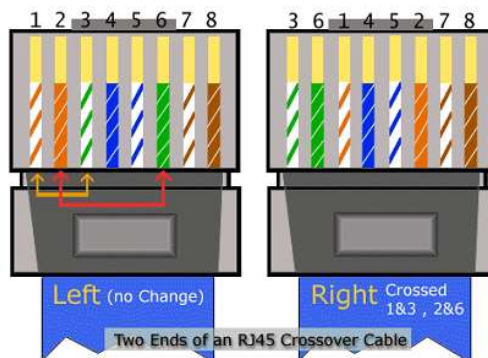
- pour limiter la paradiaphonie.
- pour limiter l'atténuation du câble
- pour limiter l'influence du câble aux perturbations électromagnétiques.

- Caractéristiques :
 - Les moins chers (1€/m).
 - Sensibles aux interférences électromagnétiques.
 - Impédances de 50 à 120 Ω .
 - Résistances de 9 à 12 Ω sur câble de 100 mètres.
 - Vitesse de transmission : 10Mb/s 100Mb/s 1Gb/s (suivant catégorie du câble)
 - Longueur maximale par segment : 100 mètres.
 - Usage de la bande : Base
 - Installation : facile à installer et à étendre.
- Plans de câblage : 2 normes :
 - T568-A
 - T568-B

⚡ Pour un câble droit : prendre 2 fois la norme T568-A ou 2 fois T568-B.



⚡ Pour un câble croisé : prendre T568-A à une extrémité et T568-B à l'autre.



- ★ Utile quand on met plusieurs concentrateurs en série (cascade).
- ★ Communication entre deux machines sans utiliser un concentrateur (il faut une carte réseau).

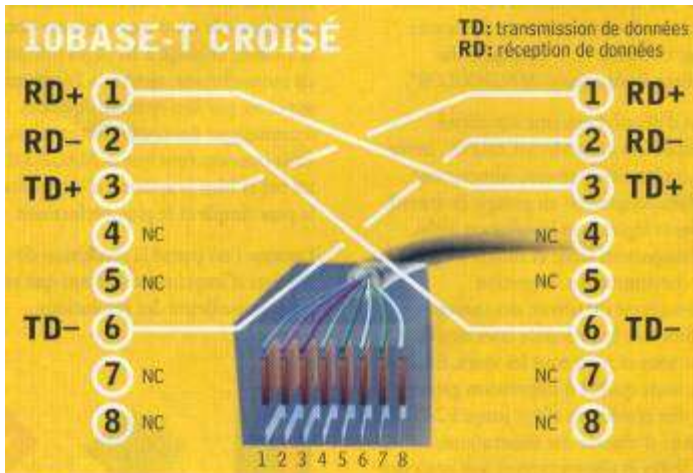
- Différentes catégories de paires torsadées non blindées :

<i>CATEGORIES</i>	<i>NORMES RESEAU</i>	<i>VITESSE DE TRANSMISSION</i>
3	10 BASE T (2 paires utilisées : 1+2, 3+6) ↙ Ethernet	10 Mb/s
4	UTP 16 (Token Ring)	16 Mb/s
5	100 BASE T (2 paires utilisées : 1+2, 3+6)	100 Mb/s
5 ^e	1000 BASE TX (4 paires utilisées)	1000 Mb/s
6	Plus de 1000	2Gb/s

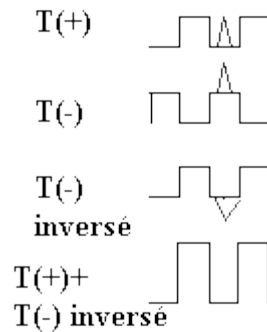
- Pourquoi respecter le câblage par paires. ?

Côté HUB

Côté carte réseau



Le signal au départ de la carte réseau est envoyé sur la forme T+ et sur la forme T- (signal inversé). Supposons un parasite qui apparaît sur le câble pendant la transmission du signal. Il est de même sens sur les 2 fils. Comme une paire est torsadée, les perturbations électriques liées à des courants induits seront généralement différentes d'une paire à l'autre. Pour rappel, le passage d'un courant électrique dans un fil produit un champ électromagnétique dans son entourage et de ce fait induit un courant dans les fils électriques proches.



Invertissons T(-). Le signal et le parasite sont inversés. En additionnant T(+) et T(-) inversé, le signal double mais le parasite est supprimé.

2.1.2.2. Les paires torsadées blindées

⚡ FTP = Foiled Twisted Pair (paires écrantées).

Entourer toutes les paires d'un même câble d'une tresse métallique ou d'un feuillard fin en aluminium

⚡ STP = Shielded Twisted Pair (paires blindées).

Entourer chaque paire d'une tresse métallique ou d'un feuillard fin en aluminium.

IBM ⚡ hermaphrodite.

RJ45 blindé

⚡ SFTP = Shielded an Foiled Twisted Pair.(paires écrantées et blindées).

2.2. Fabrication du câblage RJ45 croisé

Il faut donc :

- du câble réseau UTP
- 2 connecteurs RJ45
- une pince à sertir.

Sélectionner la longueur de câble réseau à la dimension souhaitée.

Dénuder l'extérieur du câble sur les 2 extrémités afin de n'avoir plus que les 4 paires colorées de chaque coté.

Désolidariser les paires et allonger les brins.

Ordonner les brins selon le schéma ci-dessus.

Saisir la première fiche RJ45 entre vos doigts devant vous. Le petit levier en plastique doit être positionné derrière.

Insérer les brins dans l'ordre choisi pour chaque extrémité.

Sertir la fiche à l'aide de la pince.

2.3. Contrôle du câble

2.3.1. Pourquoi un testeur de câble ?

Après un certain temps d'utilisation des câbles, il n'est pas rare de rencontrer des problèmes dus aux

tractions répétées sur les câbles ou à leur écrasement.

Un testeur, sans être absolument indispensable, économisera un temps précieux.

Quand on veut intervenir sur des câbles à paires torsadées, il est indispensable de se procurer un véritable testeur de câblage, muni directement d'un ou plusieurs connecteurs RJ45.

En utilisant un scanner actif, on vérifie non seulement la présence ou non de continuités électriques, mais en plus la qualité des câblages en situation et donc leur conformité aux différents standards. Il envoie un signal calibré à l'extrémité d'un câble et mesure ses caractéristiques de retour (écho). Il est capable d'indiquer les défauts intermittents les bruits parasites, la longueur effective des câbles, la distance à laquelle se trouve le premier défaut, l'atténuation sur le signal, la paradiaphonie (influence d'une paire sur une autre paire, la capacité mutuelle, ...

2.3.2. Fonctionnement du testeur de câble CableMeter de Fluke

Le 620 CableMeter de Fluke est un appareil portable permettant :

- d'identifier les problèmes de câble
- de mesurer la longueur du câblage
- de vérifier le câblage

pour les LAN suivants:

- paire torsadée sans blindage (UTP)
- paire torsadée blindée (STP)
- paire torsadée protégée (FTP)
- câble coaxial.

Configuration des options :

- Pour faire défiler informations, appuyer sur ^ et sur ~
 - Pour configurer les options telles que
2. la langue, l'unité de longueur, l'unité de taille, la fréquence du filtre de bruit, il faut appuyer sur le bouton Setup (quand on tourne le commutateur rotatif vers TEST)
- le type de câble, le standard de câblage, la catégorie de câble, la taille du fil, l'étalonnage avec un câble, l'activation du bip, il faut appuyer sur le bouton Setup après être sur la position TEST

Test de type tout ou rien

1.

OK ID—

41.0m

Le câble est bon

2.

OK ID#1

41.0m

Le câble est bon et le module d'identification du câble a été détecté

3.

ECHEC ID—

6 OUVERT @1.0m

La broche 6 est ouverte à l'extrémité la plus proche

4.

ECHEC ID—

1&2 COURT <92.0m

Un court-circuit entre les fils 1 et 2 a été détecté à une distance inférieure à 92.0 mètres

5.

ECHEC ID—
LONGUEUR PAIRE

Les longueurs des paires sont différentes. Utiliser longueur pour vérifier la longueur de chaque paire

Test de type longueur

1.

12 93.0m
36 91.5.0m

Lors du test de 4 paires seules 2 paires apparaissent à l'écran => utiliser flèche bas pour suite

2.

45 94.0m
78 92.0m

Appuyer sur flèche haut pour revenir à l'écran précédent

Affichage des liaisons entre les broches (Wire Map)

1.

12 36 45 78 ID #1 :extrémité la + proche
12 36 45 78 :extrémité la +éloignée

L'extrémité la + proche est branchée correctement.

2.

12 36 45 78 ID –

Les 2 extrémités du câble sont branchées correctement. Le module d'identification de câble N°1 a été détecté

3.

12 36 ID#1
1o 36

Un numéro clignotant en alternance avec o signifie que la broche correspondant est ouverte. La broche 2 est ouverte dans la 2ème moitié du câble

4.

27 1 36 45 8 ID#?
cc

Un c clignotant signifie que le fil correspondant est court-circuité. Les fils 2 et 7 sont court-circuités dans la 2ème moitié du câble.

5.

12 63 45 78 ID#1
12 36 45 78

Le fil 3 est branché sur la broche 6; le fil 6 est branché sur la broche 3. La défaillance peut être située à n'importe quelle extrémité.

2.3.3. Connexions RJ45, règles de câblage et problèmes de liaisons

La première reste les conditions maximales d'exploitation. Il est tentant de mettre un fil plus

long que celui prévu par la norme entre un hub (ou un switch) et un PC (100 mètres pour un T base 10 ou 100).

Si les câbles sont achetés tout faits, la connexion est généralement bonne. Ceci est valable pour les petits réseaux internes mais est rarement le cas pour les réseaux industriels.

Chaque connexion est limitée par le nombre de HUBS en cascade. Pour une connexion 10 base T, le nombre maximum entre 2 stations est de 4. Par contre, elle est de 2 en 100 base T

En dernier, le câble RJ45 doit être correctement posé. Parmi les problèmes rencontrés, on trouve:

- câble réseau coupé ou égratigné ou plié.
- plus sournois: le câble passe à côté de câbles électriques qui perturbent le signal, à côté de tubes fluorescents ou néon (minimum 50 cm). Proximité de moteurs électriques de fortes puissances.

Pour un câble RJ45 de faible longueur, on pourrait mettre les câbles électriques et réseaux dans les mêmes goulottes. Ceci serait oublier les normes de sécurité électriques (Vincotte en Belgique) qui interdisent d'insérer des câbles électriques et téléphoniques (basse tension) dans les mêmes goulottes, même si c'est courant dans les faux-plafonds en industries.

o **Dédoubler un câble RJ45**

Le principe : la majeure partie du temps les installations réseaux sont prévues avec une prise murale dans un bureau reliée à la baie de brassage, puis connectée au Hub central. Le câblage ainsi installé est en 4 paires torsadées mais seulement 2 paires servent à véhiculer le signal Ethernet. L'idée c'est d'utiliser les 4 fils restant pour ajouter un nouveau poste sans avoir de câble à repasser dans les gaines ou goulottes.

Les fils utilisés sur la prise RJ45 sont d'ordinaire le 1, 2, 3 et 6. Les éclateurs de paires déroutent les bornes 4,5 et 7,8 de la prise RJ45 mâle vers le 1, 2, 3 et 6 de la deuxième prise RJ45 femelle de l'éclateur. La première RJ45 femelle n'est en fait que le report du 1, 2, 3 et 6 de la RJ45 mâle. Après avoir installé l'éclateur dans la prise murale, et branché les 2 cartes réseau à l'aide de cordon patch. Il faudra faire de même au niveau de la baie de brassage et donc connecter un autre éclateur sur l'embase femelle, puis raccorder les 2 prises femelles de l'éclateur vers 2 entrées du hub.

Le 252340 est composé d'une prise RJ45 mâle à l'arrière avec 2 prises femelles l'une au dessus de l'autre le tout dans un bloc de 5 cm de long (3,2cm lorsque la prise est enfoncée).

Le 252440 et 252450 est un modèle avec un câble RJ45 de 10 cm avec boîtier monté avec 2 vis et 2 prises RJ45 femelles juxtaposées (livré avec 2 vis pour une fixation murale). Même si le boîtier est démontable, le plan de câblage n'est pas modifiable car les liaisons sont gravées sur un circuit imprimé.

Fonction

- Connecteurs conforme Catégorie 5.
- Couleurs des fils normalisées EIA-TIA 568B.
- Plan de câblage mentionné sur une étiquette collée sur le produit.

Caractéristiques

Connecteur RJ45 Mâle (côté hub ou switch)			Connecteur RJ45 femelle (1) (coté machine 1)			Connecteur RJ45 femelle (2) (côté machine 2)		
Pin	Fil	Couleur	Pin	Fil	Couleur	Pin	Fil	Couleur
1	P3	Blanc-Orange	1	P3	Blanc-Orange			
2	P3	Orange	2	P3	Orange			
3	P2	Blanc-Vert	3	P2	Blanc-Vert			
6	P2	Vert	6	P2	Vert			
4	P1	Bleu				2	P1	Bleu
5	P1	Blanc-Bleu				1	P1	Blanc-Bleu
7	P4	Blanc-Marron				3	P4	Blanc-Marron
8	P4	Marron				6	P4	Marron

2.5.La partie logicielle

Il faut installer :

3. Clients : Microsoft-> Client pour les réseaux Microsoft (pour connecter des machines sous Windows)
4. Protocoles : la plus simple NETBEUI, sinon modifier les adresses IP et les passerelles par défaut
5. Service : Partage des fichiers et imprimantes pour les réseaux Microsoft (permet d'accéder aux fichiers du PC distant et aux imprimantes.

Sur chaque ordinateur, on détermine les répertoires, disques et autres ressources à partager.

3. Protocoles

3.1 Introduction

Protocole : ensemble de règles ou normes élaborées pour permettre à des ordinateurs de s'interconnecter et à des périphériques d'échanger des informations avec le minimum d'erreurs.

Fonctions du protocole :

- ↙ choisir l'itinéraire pour véhiculer les informations.
- ↙ découper les informations en entités plus petites.
 - ↙ corriger les erreurs de transmission.
 - ↙ établir une relation entre adresse physique et adresse logique.
 - ↙ ...

5. Protocoles d'application : fonctionnent au niveau de la couche supérieure du modèle OSI et permettent une interaction entre les applications et les échanges de données.
6. Protocoles de transport : permettent les sessions de communication entre les ordinateurs et le transfert rapide et fiable des données entre les ordinateurs.
7. Protocoles de réseau : gèrent les informations d'adressage et de routage, de détection d'erreurs et de demandes de retransmission, définissent les règles de la communication au sein d'un environnement de réseau donné.

Les règles :

- 7.1. des machines d'un réseau ne peuvent se comprendre que s'ils utilisent des protocoles identiques
- 7.2. un serveur supportant différents protocoles est accessible à toute station cliente équipée de l'un des protocoles.

3.2. Protocole TCP/IP

TCP= Transmission Control Protocol (protocole de contrôle de la transmission) est un protocole de livraison des données fiable et orienté connexion.

Il sert à transférer des données entre des machines de bout en bout et se situe au niveau 4 du modèle OSI.

Il utilise les ports pour établir les connexions et surveille la transmission des informations.

Architecture TCP/IP : pile de protocole

5, 6 et 7	FTP	HTTP	Telnet	SMTP	DNS
4	TCP		UDP		
3	IP			ICMP	
1 et 2	Ethernet		Token Ring		

★ Définition, caractéristiques

L'architecture TCP/IP a été développée par la DARPA (Defence Advanced Research Project Agency – USA) et normalisée dans les années 70.

L'architecture TCP/IP est constituée d'un ensemble de protocoles permettant à plusieurs ordinateurs de partager des ressources communes, que les machines soient locales (réseaux locaux) ou distantes (interconnexion).

La pile des protocoles TCP/IP est utilisée pour faire communiquer des réseaux reliant des ordinateurs de différents types.

L'architecture TCP/IP est une architecture en couches. Elle comporte les couches suivantes :

figure 4.1 :Architecture TCP/IP

3.1.2. Avantages et inconvénients

6. Avantages

- 7.3. Architecture indépendante de tout constructeur, standard ouvert
- 7.4. Meilleur moyen actuel d'interconnecter des machines hétérogènes en LAN comme en WAN
- 7.5. Nécessaire à la communication sur Internet.

7. Inconvénients

- 7.6. Configuration non automatique : définir manuellement et sur chaque machine les paramètres techniques tels que adresse IP, masque de sous-réseau, ...(sauf si un serveur DHCP existe)
- 7.7. Capacité de stockage des adresses IP version 4 limitée à 32 bits (passage à la version 6 de IP – adresse IP codée sur 128 bits)

3.2. Protocole TCP

TCP= Transmission Control Protocol (protocole de contrôle de la transmission) est un protocole de livraison des données fiable et orienté connexion.

Il sert à transférer des données entre des machines de bout en bout et se situe au niveau 4 du modèle OSI.

Il utilise les ports pour établir les connexions et surveille la transmission des informations.

TCP travaille sur des ports. Certains sont figés. Ex : 21 ↯ FTP, 80 ↯ http

0 ↯ 1023 : ports prédéfinis.

1024 ↯ 65535 : ports utilisés pour clients et serveur pour communiquer sous TCP.

Fonctionnement :

Les données TCP sont transmises sous formes de segments (une session doit être établie avant que les hôtes puissent échanger des données). Cette session sert à synchroniser l'émission et la réception de segments, à informer l'hôte de la quantité de données qu'il peut recevoir à la fois et à établir une connexion virtuelle.

Il y a 3 phases dans l'établissement d'une liaison TCP : (à montrer sur simulateur)

- Le client demande une session en envoyant un segment avec l'indicateur de synchronisation (SYN activé)
- Le serveur accuse réception de la requête en renvoyant un segment avec :
 8. indicateur de synchronisation active (SYN=1)
 9. numéro de séquence indiquant l'octet de départ d'un segment qu'il peut envoyer
 10. un accusé de réception avec le numéro de séquence de l'octet du prochain segment attendu
- Le client renvoie un segment avec le numéro de séquence acquitté et le numéro d'accusé de réception.

Le contrôle de flux est effectué par un système de fenêtrage.

La fiabilité de l'acheminement des segments est assuré par l'acquiescement et la retransmission.

Pour la terminaison, les mêmes phases sont réalisées.

Format des paquets TCP (couche 4 du modèle OSI) :

Format des paquets TCP

PORT SOURCE (16)						
PORT DESTINATION (16)						
NUMERO DE SEQUENCE (32)						
NUMERO D'ACQUITTEMENT (32)						
LONGUEUR EN-TETE (4)	RESERVE (6)	URG (1)	ACK (1)	PSH (1)	RST (1)	SYN (1) FIN (1)
WINDOWS (16)						
CHECKSUM (16)						
URGENT POINTEUR (16)						
OPTIONS + BOURRAGE						
DONNEES						

6. Port source (16): 0C15 \llcorner 00001100 00010101 \llcorner $2^0+2^2+2^4+2^{10}+2^1 = 3093$
7. Port destination (16): 1236 \llcorner 00010010 00110110 \llcorner 4662
8. Numéro de séquence (32) \llcorner position du segment dans le flux de l'émetteur.
9. Numéro d'acquittement (32) \llcorner n° du prochain octet attendu par récepteur.
10. Longueur d'entête, **réserve**, différents flags :
 - **URG** Si 1 \llcorner tenir compte du champs de pointeur urgent,
 - **ACK** Si 1 \llcorner acquittement de l'info,
 - **PSH = PUSH**. Si 1 \llcorner envoi des infos sans attendre,
 - **RST = RESET**. Si 1 \llcorner redémarre la connexion,
 - **SYN** Si 1 \llcorner établissement de la connexion, synchronisation des connexions,
 - **FIN** Si 1 \llcorner libération de la connexion

5010 \llcorner 00000001 0000
11. Window (16) : nombre maximum d'octets transmissibles avant acquittement.
12. Checksum (16) : contrôle de l'intégrité des informations.
13. Urgent pointeur (16)
14. Options + bourrage
15. Données

3.3. Protocole IP

IP=Internet Protocol (protocole internet) offre un service réseau en mode non connecté et se situe au niveau 3 du modèle OSI.

Il se charge du routage et de l'adressage des paquets entre les hôtes. Il n'est pas fiable car il ne garantit pas la livraison des paquets. Il ne nécessite pas d'accusé de réception des données.

Fonctionnement :

Si le protocole identifie l'adresse de destination comme locale, il transmet directement le paquet au destinataire.

Si le protocole identifie l'adresse de destination comme distance, il recherche dans la table de routage locale la route vers l'hôte distant. S'il en trouve une, alors envoie le paquet en utilisant cette route, sinon envoie le paquet à la passerelle par défaut de l'hôte source.

Le protocole IP sur le routeur (recevant un paquet) :

11. IP décrémente TTL (Time To Live) (d'au moins un ou plus si le paquet est bloqué). Quand TTL = 0, le paquet est supprimé.
12. IP peut fragmenter le paquet lorsque ce dernier est trop volumineux pour le réseau sous-jacent.
Si un paquet est fragmenté, IP crée pour chaque nouveau paquet un en-tête en incluant :
 - 12.1. un indicateur précisant que d'autres fragments suivent (MF=1)
 - 12.2. un ID du fragment identifiant tous les fragments appartenant à la même entité
 - 12.3. un décalage de fragment (fragment offset) indiquant à l'hôte récepteur comment ré assembler le paquet.
13. IP calcule un nouveau total de contrôle
14. IP obtient l'adresse matérielle de destination du routeur suivant (grâce au protocole ARP)
15. IP achemine le paquet.

Sur hôte suivant, le paquet remonte dans la pile jusqu'à la couche TCP ou UDP. La procédure est répétée jusqu'à ce que le paquet atteigne sa destination finale (où IP ré assemble les différents paquets pour reconstituer le paquet d'origine).

Structure paquet IP (couche 3 du modèle OSI) :

Structure des paquets IP

→ 5 * 32 = 20 Octets

Version IP (4)	Taille en-tête IP (4)	Type de service (8)
LONGUEUR TOTALE (16)		
IDENTIFICATION (16)		
FLAG	OFFSET FRAGMENT	
TTL (8)	PROTOCOL (8)	
CHECKSUM		
Adresse source (32 bits)		
Adresse destination (32 bits)		
Options + padding (32bits)		
Données		

- Version IP (4)
 - Longueur entête IP (4)
 - Type de service (8)
 - D : délai d'acheminement : 1 ≙ délai transmission court
0 ≙ délai transmission normal
 - T : débit de transmission : 1 ≙ élevé
0 ≙ normal
- } 3bits milieu

- R : fiabilité : 1 ↯ grande fiabilité
0 ↯ fiabilité normale
- Longueur totale (16) : longueur entête + longueur données 1000 --> 0100 0000 0000 :
1 ↯ pas fragmenter
0 ↯ peut fragmenter
- Identificateur (16) :
- Flags + Offset fragment
- Protocol (8) : référence le protocole de la couche supérieure + TTL (8) : (Time To Live)
= nombre de nœuds que le paquet peut traverser. Si TTL = 0 : paquet détruit
- Checksum : contrôle l'intégrité de paquet
- Adresse source (32)
- Adresse destination (32)
- Options + padding (32)
- Données

○ Protocole ARP

- ★ *Rôle*
- ★ *Résolution d'adresse avec arp*
- ★ *Mémoire cache de ARP*
- ★ *Structure des paquets ARP*

○ Protocole ICMP

- ★ *Rôle*
- ★ *Structure des paquets ICMP*

Voir en plus le fichier suivant :

[adressage et masque \(complément\).doc](#)

4. Adressage IP et masque de sous-réseau

4.1 Adresse IP

Chaque matériel, connecté à un réseau, est identifié par une adresse IP qui est unique.

Elle présente un format normalisé et comprend 2 parties :

- identificateur du réseau : identifie le réseau sur lequel les machines sont connectées (toutes les machines d'un même réseau ont la même adresse de réseau)
- identificateur de l'hôte : identifie la machine dans le réseau (unique pour chaque identificateur de réseau).

La version 4 est limitée à 32 bits.

Il existe 2 formats de représentation des adresses IP :

- le format binaire
- la notation décimale à point : 4 champs de 8 bits séparés par des points (nombre de 0 à 255).

Les classes d'adresses ne sont plus utilisées.

Chaque classe définit la partie de l'adresse IP qui identifie le réseau et celle qui identifie l'hôte. Elle identifie le nombre de réseaux et d'hôtes par réseau autorisés.

Les classes d'adresses :

Classe	Préfixe	Intervalle
A	0	1. -- 126.
B	10	128.0. -- 191.255.
C	110	192.0.0. -- 223.255.255.
D	1110	224.0.0. -- 239.255.255.
LoopBack		127.

Classe	Nb réseaux	Nb hôtes
A	126	16.777.214
B	16.384	65.534
C	2.097.152	254
D	--	--
LoopBack	1	1

Il faut respecter certaines directives pour affecter correctement les identificateurs de réseau et hôte.

- l'identificateur de réseau doit être différent de 127 (adresse de boucle de retour, par exemple 127.0.0.1)
- tous les bits de réseau ou d'hôte à 1 ne sont pas permis
- tous les bits de réseau ou d'hôte à 0 ne sont pas permis
- tous les bits de réseau à 0 indique une adresse de réseau
- tous les bits de réseau à 1 indique une adresse de broadcast(c'est-à-dire une adresse servant à diffuser un message sans destinataire précis sur le réseau concerné)
- identificateurs de l'hôte doivent être uniques pour un identificateur de réseau
- chaque réseau et connexion WAN doit avoir un identificateur de réseau unique

Adresses IP réservées :

L'INTERNIC a réservé une poignée d'adresses dans chaque classe pour permettre d'affecter une adresse IP aux ordinateurs d'un réseau local relié à Internet sans risquer de créer de conflits d'adresses IP sur le réseau. Il s'agit des adresses suivantes:

- 10.0.0.1 à 10.255.255.254
- 172.16.0.1 à 172.31.255.254
- 192.168.0.1 à 192.168.255.254

Classe A (32): ↯0 figé à la première place.
 ↯ID réseau : $2^7 - 0 \leq 127$ mais on ne peut pas utiliser 0 (tout des 0) et 127 (tout des 1) ↯ $1 \leq 126$.
 ↯ID hôte : $2^{24} - 2 = 16\,777\,214$ IP possibles.

Classe B (32): ↯1 et 0 figés aux premières places.
 ↯ID réseau : $2^{16-2} = 2^{14} = 16.384$ réseaux possibles.
 ↯ID hôte = $2^{16} - 2 = 65534$ hôtes.

Classe C(23) : ↯1, 1 et 0 figés aux premières places.
 ↯ID réseau : $2^{24-3} = 2^{21} = 2\,097\,152$ réseaux possibles.
 ↯ID hôte : $2^8 - 2 = 254$ hôtes possibles.

Classe D : adresse de diffusion de groupe (multicast).

Classe E : adresses réservées aux expérimentations.

4.2. Masque de sous-réseau

Un **sous-réseau** est un segment physique dans un environnement TPC/IP utilisant des adresses IP dérivées d'un ID de réseau unique.

But s :

- diminuer la taille des domaines de diffusion
- mieux utiliser les bits de la partie hôte
- permettre de mélanger des technologies différentes
- réduire l'encombrement réseau.

Protocole IP : ↙ adresse source : IP A : 132.160.10.1
 ↙ adresse destination : IP B : 132.160.12.1
 adresse destination : IP C : 132.240.10.1

Masque pour :

- Classe A : IIIIIII.00000000.00000000.00000000 ↙ 255.0.0.0
- Classe B : IIIIIII.IIIIIII.00000000.00000000 ↙ 255.255.0.0
- Classe C : IIIIIII.IIIIIII.IIIIIII.00000000 ↙ 255.255.255.0

Masque par défaut : 255.255.0.0

A↙B : A : 10000100.10011100.00001010.00000001 AND
 MSR: 11111111.11111111.00000000.00000000
 ↙ 10000100.10011100.00000000.00000000 ↙ 132.160.0.0

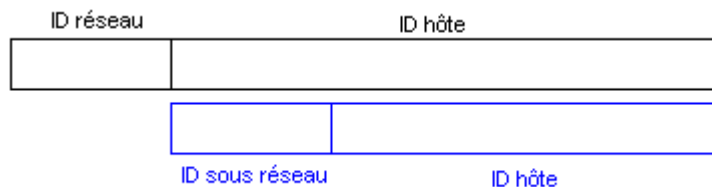
B: 10000100.10011100.00001100.00000001
 MSR : 11111111.11111111.00000000.00000000
 ↙ 10000100.10011100.00000000.00000000

A↙C : A: 10000100.10011100.00001010.00000001 AND
 MSR: 11111111.11111111.00000000.00000000
 ↙ 10000100.10011100.00000000.00000000 ↙ 132.160.0.0
 C: 10000100.11110000.00001010.00000001
 MSR: 11111111.11111111.00000000.00000000
 ↙ 10000100.11110000.00000000.00000000 ↙ 132.240.0.0

Sous-réseaux :

Subnetter : découpe un réseau en sous-réseaux.

Pour cela : emprunter des bits à la partie hôte.

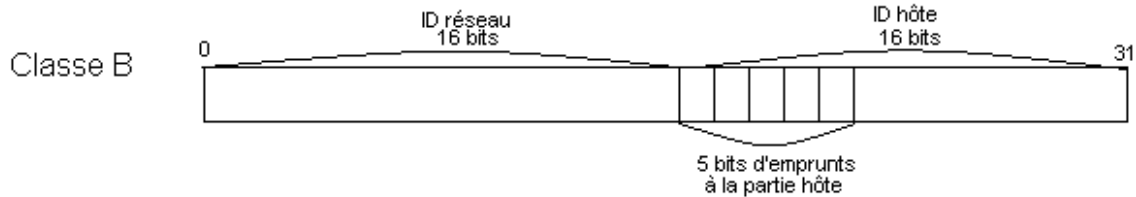


Nombre de bits empruntés	Nombres de sous-réseaux possibles
1	2
2	4
3	8

4	16
5	32
6	64
7	128
8 (impossible pour classe C)	256

Exemple : un réseau de classe B : 130.120.0.0

On souhaite diviser le réseau en 20 SR de 100 hôtes chacun.



Classe B : 16 bits partie réseau
16 bits partie hôte

Déterminer le nombre de bits utilisés pour représenter 20 :

$$20 = 2^4 \cdot 1 + 2^3 \cdot 0 + 2^2 \cdot 1 + 2^1 \cdot 0 + 2^0 \cdot 0 = 10100 \llcorner 5 \text{ bits.}$$

On emprunte donc 5 bits à la partie hôte :

130. 120. **00000000.** **00000000**
S-R **11 bits hôtes**

Masque de sous-réseau :

11111111.11111111.11111000.00000000
255.255.248.0

Nombres d'hôtes possible : 11 bits

$$2^{11} - 2 = 2046 \text{ hôtes.}$$

Liste des différents sous-réseaux :

N° S-R	Binaire	Décimale	Utilisable
1	10000010.01111000.00000 000 .00000000	130.120.0.0	Non
2	10000010.01111000.00001 000 .00000000	130.120.8.0	Oui
3	10000010.01111000.00010 000 .00000000	130.120.16.0	Oui
4		130.120.24.0	
...

Déterminer les plages d'adresses IP.

N° S-R	Binaire	Décimale
1	10000010.01111000.00000 000 .00000001 à 10000010.01111000.00000 111 .11111110	130.120.0.1 à 130.120.7.254

2	10000010.01111000.00001000.00000001 à 10000010.01111000.00001111.00000001	130.120.8.1 à 130.120.15.254
3

4.3. IP version 6

Actuellement la taille de l'Internet double tous le 12 mois. Il y a donc 2 problèmes à résoudre :

- l'épuisement des adresses IP
- l'explosion de la taille des tables de routage.

Pour résoudre ces problèmes, création d'une nouvelle version de Internet Protocol : version 6 (Ipv6).

Ce nouveau protocole étend la fonction d'adressage et de routage, il tend à résoudre les problèmes qui vont devenir critiques (applications temps réel, sécurité, ...).

Les caractéristiques de Ipv6 sont :

- Adresse plus longue : 128 bits
- Plus d'agrégation dans le routage (renforcement de CIDR)
- types d'adresse : unicast (adresses allouées de manière contiguë et qui ont les mêmes bits de poids forts), multicast (identifiant pour un groupe de noeuds)
- En-tête simplifié : nombre de champ réduit

Extension de l'en-tête pour les options (longueur options plus limitée à 40)

5. Routage IP

5.1. Routage

★ Définitions

Le routage est une technique basée sur des adresses de niveau réseau (niveau 3 du modèle OSI) permettant d'aiguiller une trame quelconque émise par un nœud d'un sous-réseau vers un nœud de destination pouvant être situé sur un autre sous-réseau.

Les éléments matériels permettant d'effectuer cette tâche s'appellent des routeurs. Un routeur est un équipement relié au moins à 2 réseaux.

★ Fonctionnement d'une communication

On peut adresser directement tout poste connecté physiquement à son réseau et partageant la même adresse réseau au niveau IP.

Un poste qui émet un paquet à destination d'un autre réseau IP, utilise une passerelle (routeur) qui se trouve sur son réseau.

Couche 2 : ARP –MAC

Couche 3 : IP- Adresse IP

Interactions entre couches 2 et 3

★ Table de routage

• Définition

La table de routage est un regroupement d'informations permettant de déterminer le prochain routeur à utiliser pour accéder à un réseau précis sur lequel se trouvera la machine avec laquelle on souhaite dialoguer. Elle les regroupe par ligne en indiquant pour un réseau donné par où il faut passer.

5.1.3.2. Eléments constitutifs d'une table de routage

Chaque entrée d'une table de routage classique comporte :

- l'adresse de destination du réseau à atteindre (où se trouve la machine de destination)
- le masque de sous-réseau du réseau de destination
- le routeur (la passerelle) à utiliser pour aller vers le réseau de destination
- l'interface à utiliser pour aller vers le réseau de destination
- la métrique (l'accessibilité d'une destination) c'est-à-dire le nombre de routeurs de réseau à franchir pour atteindre le réseau de destination.

Les interfaces peuvent être identifiés par leurs adresses ou par leur type.

Les réseaux sont identifiés par l'adresse du réseau et le masque associé.

Pour atteindre l'adresse réseau (colonne 1) de masque réseau (colonne 2), je passerai par la passerelle (colonne 3) en utilisant la carte réseau d'adresse IP (colonne 4) en passant par x routeurs (colonne 5).
Exemple : étude d'une table de routage (route print)

5.1.3.3. Quelques adresses particulières

Les adresses de diffusion générale (255.255.255.255) ne passent pas les routeurs.

L'adresse 0.0.0.0 est l'adresse par défaut (default sous unix), elle signifie "ailleurs", dans le sens où on utilise cette ligne de table pour router les paquets dont l'adresse de destination ne correspond à aucune adresse de la table de routage. C'est donc la route par défaut qui sera utilisée lorsque aucune route spécifique pour aller vers la destination n'aura été trouvée.

L'adresse 127.0.0.1 est l'adresse de loopback, elle permet à un poste de "s'auto adresser".

Chaque ligne de la table de routage se lit de la façon suivante :

5.1.4. Routage statique

Utilisation de la commande sous DOS : ROUTE

5.1.5. Routage dynamique

Il existe plusieurs protocoles de routage tels que RIP, RIP2, OSPF

Protocole RIP (Routing Information Protocol) est un protocole de routage de type vecteur de distance. C'est-à-dire les messages échangés par des routeurs voisins contiennent un ensemble de distances entre routeur et destinations qui permet de réactualiser les tables de routage. Ce protocole utilise une métrique simple : la distance entre une source et une destination est égale au nombre de sauts qui les séparent. Elle est comprise entre 1 et 15, la valeur 16 représentant l'infini. Ce protocole ne peut donc être utilisé que dans des réseaux pas trop étendus.

6. Notions de cryptographie

6.1. Définition

La cryptographie, ou chiffrement, est un processus de brouillage mathématique qui s'effectue par l'application de conventions secrètes, qu'on appelle aussi « clefs », et qui convertit une information intelligible en une information inintelligible. L'opération inverse ne peut, normalement, être réalisée que par celui qui en possède la clef.

De nombreux procédés cryptographiques permettent aujourd'hui de protéger et d'authentifier l'échange d'informations. L'on peut recourir à deux techniques principales.

- la cryptographie dite " à clé secrète " ou " symétrique " permet de chiffrer et de déchiffrer des données à l'aide d'une clé unique. Un problème se pose alors : sans méthode de cryptage préalable, les acteurs devront recourir à d'autres moyens pour procéder secrètement à l'échange des clés. La seconde méthode pallie à cet inconvénient.

- la cryptographie " à clé publique " ou " asymétrique " propose un système mettant en scène deux clés. Celle qui permet l'encodage des données est mise à la disposition du public. La personne, ou l'entreprise destinataire du document ainsi crypté est en possession de la seconde clé dite " privée ", destinée à décoder le contenu des messages.

6.2. Confidentialité

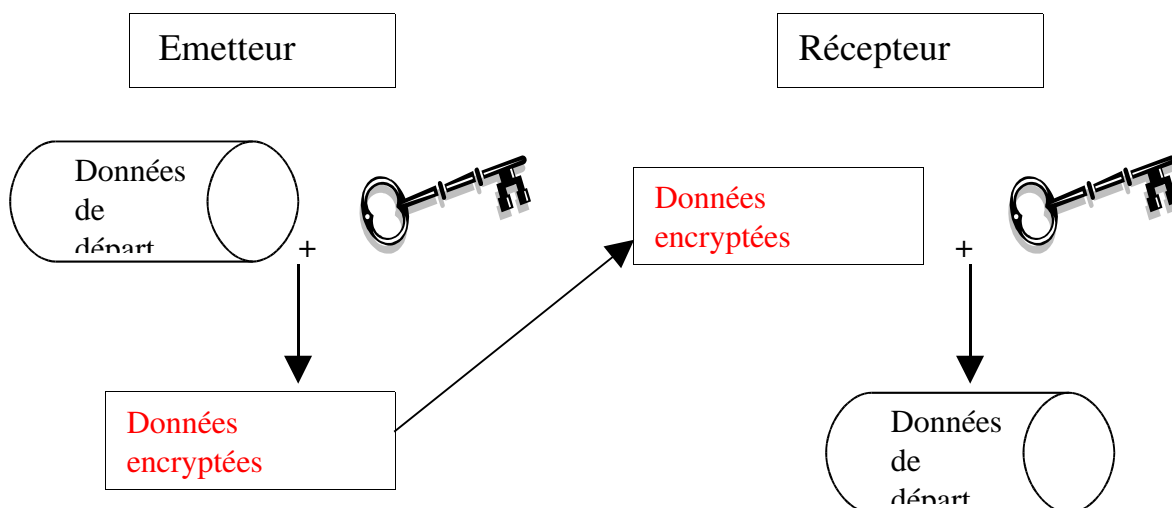
6.2.1. Clé symétrique (cryptage à clé secrète)

La même clé est utilisée pour l'encryptage et le décryptage. Elle existe depuis longtemps et a un gros problème la transmission de la clé entre les communicants.

La sécurité d'une méthode de chiffrement est « forte » si :

16. la sécurité dépend du secret de la clé et non du secret de l'algorithme
17. on dispose d'un grand espace de clés
18. la distance de chiffrement est grande.

Schéma :



L'idée générale du chiffrement par blocs est la suivante:

Remplacer les caractères par un code binaire (par exemple le [code ASCII](#) en base 2). On obtient ainsi une longue chaîne de 0 et de 1.

Découper cette chaîne en blocs de longueur donnée, par exemple 64 bits.

Chiffrer un bloc en l'additionnant bit par bit à une clef.

Déplacer certains bits du bloc.

Recommencer éventuellement un certain nombre de fois l'opération 3. On appelle cela une ronde.

Passer au bloc suivant et retourner au point 3 jusqu'à ce que tout le message soit chiffré.

Quelques exemples d'algorithmes de chiffrement par blocs:

6. DES : clé de 56 bits et de 16 rondes.

7. 3DES : clé de 112 bits et de 48 rondes. Il applique 3 fois le DES à chaque bloc.

8. [AES](#) (Advanced Encryption Standard) ou Rijndael : standard de cryptage symétrique destiné à remplacer le DES qui est devenu trop faible au regard des attaques actuelles. Il supporte différentes combinaisons [longueur de clé]-[longueur de bloc] : 128-128, 192-128 et 256-128 bits (en fait, Rijndael supporte également des tailles de blocs variables, mais cela n'est pas retenu dans le standard). Voir site : <http://www.securiteinfo.com/crypto/aes.shtml>

6.2.2. Clés asymétriques (cryptage à clé publique)

Développées pour éviter le problème de transfert de clé (clé symétrique).

Les clés existent par paires :

9. une clé publique P pour le cryptage

10. une clé privée (secrète) S pour le décryptage

Chaque utilisateur possède son propre couple de clés différentes (S, P).

La clé S est gardée secrète par le propriétaire qui l'utilise pour sa propre procédure de déchiffrement des messages reçus ou de signatures de messages.

La clé P, dérivée de la clé S par une fonction à sens unique (facilement calculable dans un sens mais dont l'inversion est difficile) est rendue publique. Elle permet donc à tout autre utilisateur de lui (personne ayant publiée sa clé publique) envoyer des messages chiffrés ou de vérifier ses signatures.

Un message chiffré à l'aide d'un algorithme asymétrique et d'une clé privée, qui constitue l'un des paramètres de l'algorithme, ne peut être déchiffré qu'avec la clé publique correspondante, et inversement. La clé publique doit donc être connue de tous, tandis que la clé privée reste secrète.

Schéma :

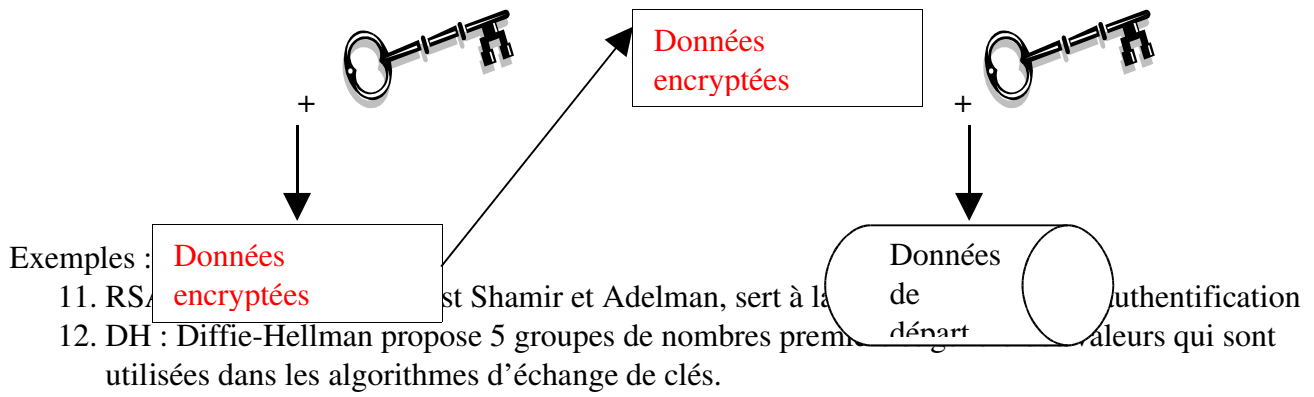


Doit connaître
du destinataire



P. destinataire

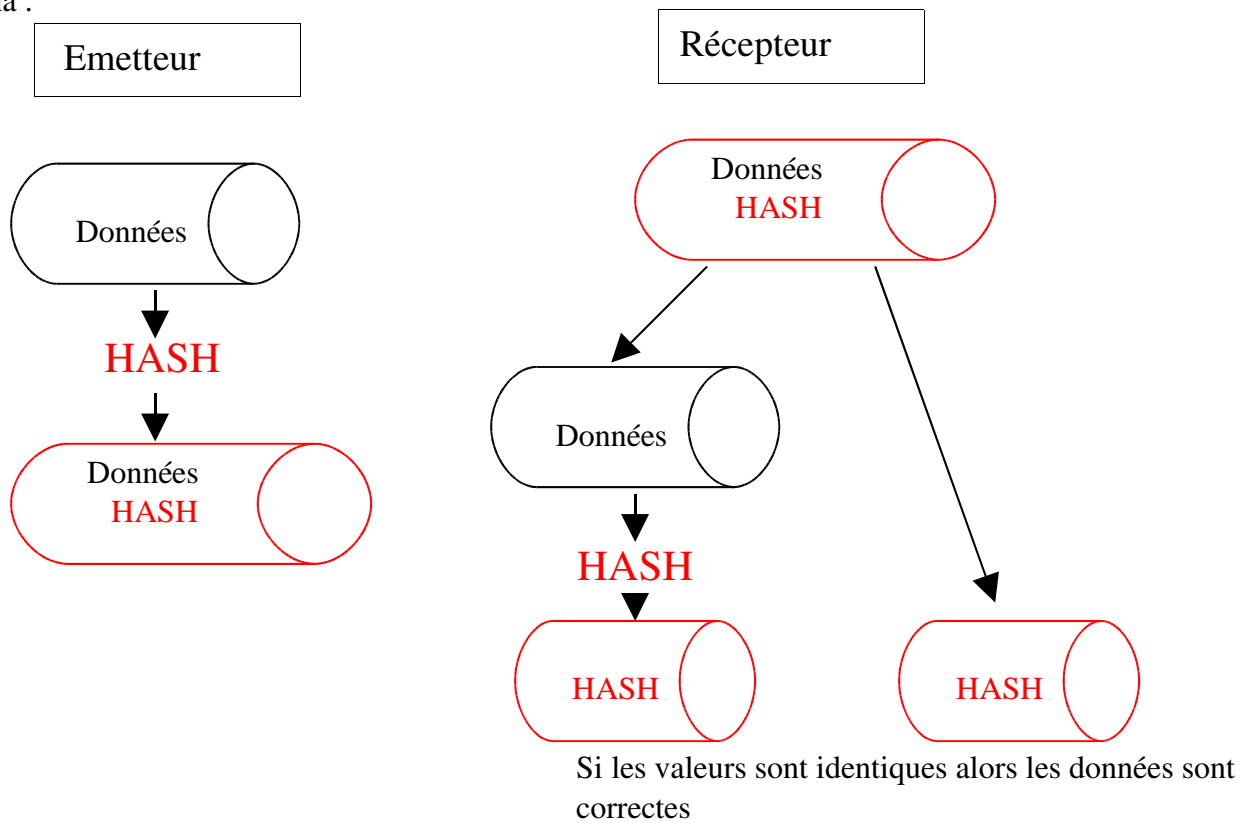
S. destinataire



6.3. Intégrité des données

Les fonctions de hachage sont utilisées pour donner des services d'intégrité de données. Le hachage applique un deuxième élément pour vérifier que le contenu de l'envoi n'est pas modifié. Une fonction de hachage permet d'obtenir un condensé d'un texte et doit être telle qu'elle associe un seul haché au texte en clair.

Schéma :



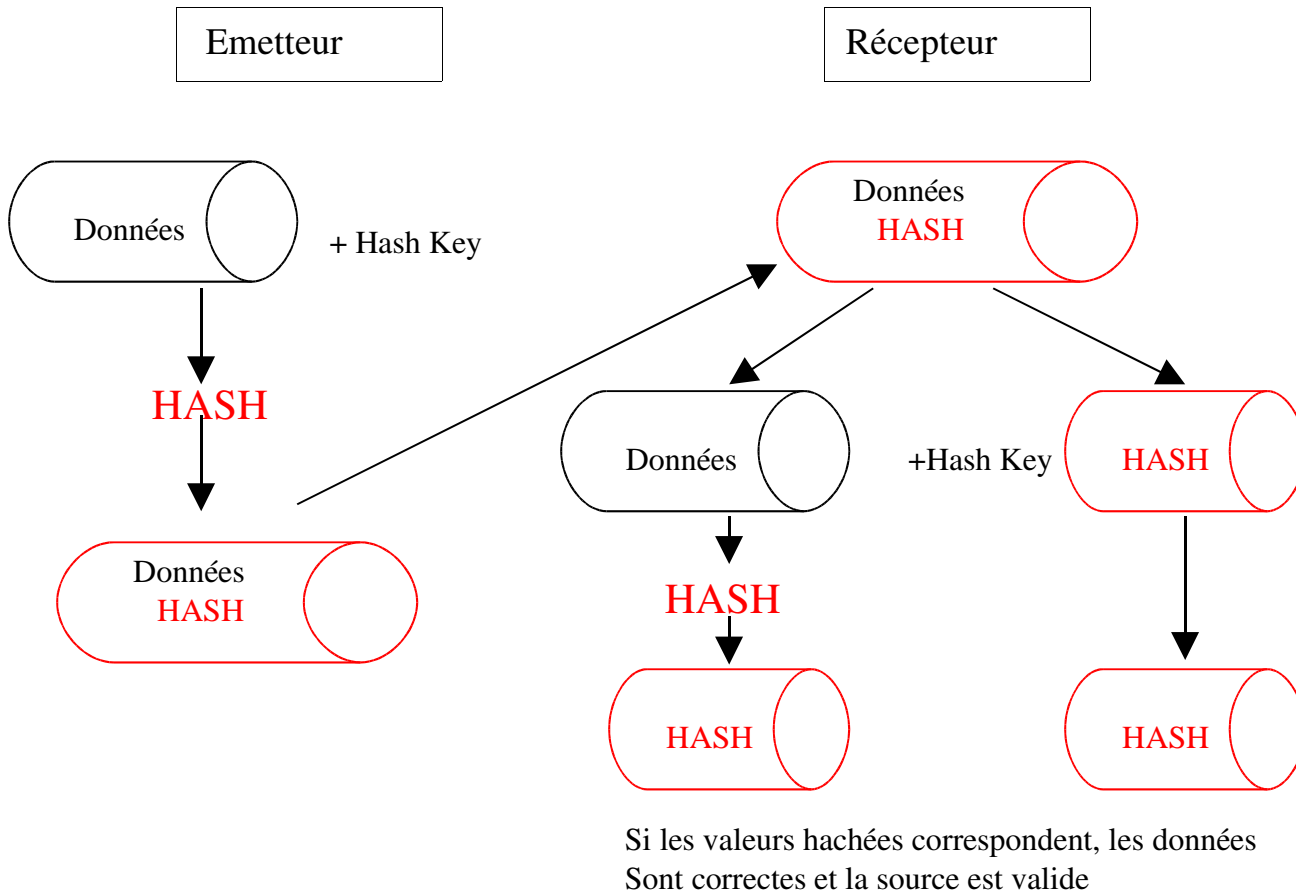
Exemples :

- MD5 : Message Digest créant une empreinte digitale de 128 bits
- SHA : Secure Hash Algorithm créant une empreinte digitale de 160 bits
- salt hash

6.4. Authentification

Il faut être sûr de l'identité de l'auteur.

Schéma :



Exemples :

- HMAC : Hashed Message Authentication Code ajoute une clé pré-partagée et pré-hachée au processus de hachage

6.5.1. Signature électronique

Vérifie l'intégrité du message et garantit l'authenticité de l'expéditeur.

Pour la signature, il faut aussi un cryptage à clé asymétrique. L'émetteur génère une signature d'un message à partir de la clé privée. Le destinataire à l'aide de la clé publique de l'émetteur vérifie son authenticité.

6.5.2. Certificat et autorité de certification

6.6. Algorithmes d'échanges de clés PKI et PKCS

PKI : Public Key Infrastructure travaille avec des paires de clés (privée, publique)

PKCS : Public Key Certification System oblige l'utilisation d'une autorité de certification

6.7. Les logiciels PGP et GNUPG

PGP est un mélange entre PKI et les clés secrètes.

6.8.2. Protéger sa clé privée

Le clé privée est la donnée la plus critique; si elle est compromise l'utilisation de la cryptographie n'a plus aucun sens (c'est comme si le mot de passe administrateur d'un serveur était connu de tous les utilisateurs). La clé privée n'est évidemment pas stockée en clair mais est elle-même cryptée, et protégée par un mot de passe (ou une phrase de passe).

La phrase de passe devient le seul moyen d'accéder à la clé privée. Pour signer un message l'utilisateur doit taper cette phrase, qui est alors comparée avec son hachage (*hash*) et donne accès à la fonction demandée. Cette phrase est également demandée pour toute action sur le trousseau de clés (*keyring*). Il est donc critique de bien choisir cette phrase; PGP aide ce choix en donnant une indication sur la qualité de la phrase tapée.

6.8.3. Obtenir une clé publique

C'est la première opération (qui peut parfois sembler difficile). Plusieurs solutions:

la clé a été envoyée par mail

la clé est disponible sur une page

la clé est disponible sur un serveur de clés

Prenons le cas général, c'est à dire que la clé est déposée sur un serveur de clés; le clé peut alors être trouvée des manières suivantes:

PGP permet de chercher une clé sur un (ou plusieurs) serveurs de clés avec certains critères:

le nom

l'adresse e-mail

l'ID de la clé (unique)

l'empreinte de la clé (*fingerprint*) également unique

Exemple

pour trouver ma (mes) clé(s) on peut faire une recherche (prenons <http://pgpkeys.mit.edu:11371>):

16. [recherche par nom](#) (retourne mes deux clés publiques)
17. [recherche avec l'ID 0x50AF9EB9](#) (clé RSA) (retourne la clé publique RSA)
18. [recherche avec l'ID 0x8453223F](#) (clé DSS) (retourne la clé publique DSS)

Il est important de comprendre comment la recherche fonctionne afin de publier l'information correctement; évidemment, si l'utilisation de PGP se limite à un cercle d'amis ce n'est pas nécessaire de procéder de manière formelle mais dès qu'on sort de ce cercle c'est important.

6.8.4. Enregistrer une clé publique dans son trousseau (*keyring*)

Cette opération consiste, après avoir identifié un destinataire (ou expéditeur) à ajouter les informations qui le concernent (nom, e-mail, clé publique) dans son environnement; il sera ainsi possible de:

- choisir le destinataire d'un message crypté
- authentifier l'expéditeur d'un message

Cette opération se fait en sélectionnant la clé publique (le reste de l'information est contenue dedans) et de l'ajouter dans le trousseau de clés (*keyring*) avec le gestionnaire de clés (ou avec la commande appropriée).

Notes (à lire attentivement)

Une fois la clé ajoutée il faut également lui fixer un niveau de confiance (*trust level*); cette opération est souvent oubliée et conduit à de mauvaises interprétations des messages d'erreur ou d'alerte de PGP. Par défaut une clé ajoutée est invalide (attribut *Invalid*) ce qui signifie qu'aucune confiance ne peut être donnée à cette clé. cet attribut permet néanmoins d'encrypter vers ce destinataire et de vérifier des messages signés par lui, mais PGP indiquera qui la clé, même si elle vérifie la signature, est invalide.

L'étape suivante consiste à signer la clé et ensuite à lui donner un niveau de confiance (*trust level*); cette signature peut être locale mais on peut également l'envoyer à un serveur de clés afin de faire connaître le fait qu'on reconnaît une valeur à cette clé (c'est pour cela que les serveurs existent). Cette information sera alors un complément pour celui qui trouvera la clé, puisqu'il connaîtra (on lira fera confiance) éventuellement une des personnes ayant signé la clé; dès lors une confiance plus grande pourra être accordée à cette clé publique.

La plupart des utilisateurs novices ignorent cette étape et occultent ainsi un des aspects les plus importants et intéressants de PGP...

C'est "Pretty Good Privacy" (en anglais : "Plutôt bonne intimité"). Il s'agit d'un logiciel de cryptographie renforcée qui est particulièrement bien adapté à l'utilisation sur Internet. Il est gratuit et très sûr. PGP a été créé en 1991 par Philip Zimmermann, un informaticien américain.

GnuPG (GPG), pour GNU Privacy Guard (gardien de la vie privée), est la version GNU de PGP. En raison de sa licence GNU/logiciel libre, GnuPG peut être librement utilisé pour un usage commercial.

6.8.5. PGP, ça marche comment, concrètement ?

Le principe : la cryptographie À CLEF PUBLIQUE

* LA PAIRE DE CLEFS : PGP génère une paire de clefs : clef publique + clef secrète.

La clef publique est distribuée au plus grand nombre, la clef secrète reste sur l'ordinateur de son propriétaire.

La clef publique sert à chiffrer.

La clef secrète sert à déchiffrer.

Les correspondants de X lui envoient leurs fichiers cryptés avec sa clef publique.

Ce qui a été chiffré avec la clef publique de X, ne peut être déchiffré que par la clef secrète de X. X est seul détenteur de cette clef secrète et doit saisir un long mot de passe (une phrase) à chaque fois qu'il

veut l'utiliser.

Le fichier de clefs secrètes contient en principe une seule clef; le fichier de clefs publiques contient la clef de chacun de ses correspondants.

L'utilité : la CONFIDENTIALITÉ...

* LA CONFIDENTIALITÉ : Quiconque peut envoyer un message chiffré à X, même s'il ne l'a jamais rencontré, dès lors qu'il est en possession de sa clef publique (de nombreux serveurs de clefs publiques existent sur le Web, aux [États-Unis](#) mais aussi dans chaque pays de l'Union Européenne). Seul X pourra déchiffrer ce message.

... et la SIGNATURE DIGITALE

* L'AUTHENTIFICATION : PGP permet d'apposer une signature digitale sur les documents. Cette signature, effectuée par X à l'aide de sa clef secrète, est vérifiée par son correspondant à l'aide de la clef publique de X.

Voir en complément le site suivant :

http://sylvestre.ledru.info/howto/securite/tunnels_et_vpn/

7. Réseau privé virtuel (VPN)

Le VPN, Virtual Private Network, permet d'établir des connexions (tunnels VPN) entre des sites distants en se servant de l'infrastructure d'un réseau public comme si elle était privée. Il permet d'abstraire le réseau public à la dimension d'un routeur.

La mise en place d'un VPN permet de connecter de façon sécurisée des ordinateurs distants au travers d'une liaison non fiable (Internet) comme s'ils étaient sur le même réseau local.

7.1. Objectifs du VPN

Les objectifs sont de :

- transmettre les données de manière authentifiée
- transmettre les données de manière secrète
- faut-il authentifier les connexions ?
- utiliser différents protocoles de tunnels tels que PPTP (Point to Point Tunneling Protocol), L2F (Layer 2 Forwarding), L2TP (Layer 2 Tunneling Protocol), IPSec.

Les 3 principales inquiétudes quand on envoie des données sur un réseau public sont :

- C : la Confidentialité c'est-à-dire les informations doivent rester cachées aux personnes qui ne peuvent y accéder
- I : l'Intégrité c'est-à-dire les données ne peuvent être modifiées
- A : l'Authentification c'est-à-dire il faut que les informations reçues viennent bien de quelqu'un de qui on peut recevoir des informations.

Voir chapitre 6 sur la cryptographie.

7.2. Principes de base

7.2.1. Technologies VPN

Elles utilisent l'encapsulation ; le datagramme original est encapsulé dans un nouveau datagramme qui est envoyé d'un point du tunnel à l'autre. Le point du tunnel récepteur décapsule les données et transmet le datagramme original.

Le but des protocoles de tunnels est de sécuriser les données lorsqu'elles traversent le réseau public.

7.2.2. PPTP

Le paquet à transmettre est mis dans une trame PPP (Point-To-Point Protocol).

Cette trame PPP est cryptée et mise dans un datagramme IP de type particulier.

Ce datagramme est transmis au nœud final qui procède de manière inverse en décapsulant et décryptant.

7.2.3. L2TP

Ce protocole permet de créer des clés de sécurité. Il est issu du protocole PPTP (basé sur les lignes téléphoniques) et est une évolution de PPTP. Il permet la transmission de protocoles autres que TCP/Ip

(ipX, AppleTalk, NetBEUI). Il fonctionne sur la couche 2 du modèle OSI. Il utilise des trames pour transmettre les données (une trame ne contient aucune information sur le contrôle d'erreur).

7.2.4. IPSec

Secure IP (IPSec) est un standard pour fournir des services de sécurité et d'intégrité.

Il travaille au niveau 3 (paquet IP). Il ne traite que les paquets Ip donc se contente de transmettre le trafic TCP/IP.

Il ne permet pas de créer de clés de sécurité et doit être combiné à une autre protocole comme (ISAKMP : Internet Security Association and Key Management Protocol) ou IKE (Internet Key Exchange).

Il support le trafic unicast.

IPSec utilise 2 protocoles pour fournir du trafic sécurisé :

- ESP: Encapsulating Security Payload, permet de faire de la CIA
- AH: Authentication Header, ne permet pas l'encryption des données, il vérifie l'intégrité et l'authentification des données.

IpSec peut être implémenté en 2 modes :

- le mode transport : (liaison point à point encryptée et authentifiée, liaison entre 2 hôtes)
IPSec intervient entre le niveau transport (TCP) et le niveau réseau (IP) du modèle OSI : le PDU de la couche transport se voit appliqué les mécanismes de signature et de chiffrement puis le résultat est passé à la couche réseau (encapsulation IP) => entête IP non chiffrée..
- le mode tunnel : (liaison de gateway à gateway encryptée et authentifiée, liaisons entre 2 passerelles).

La totalité du paquet IP est encapsulé dans un paquet IPSec sécurisé. Dans ce cas, l'en-tête IP d'origine est protégée et les adresses sont masqués. Ce mode est très utilisé pour la mise en place de VPNs.

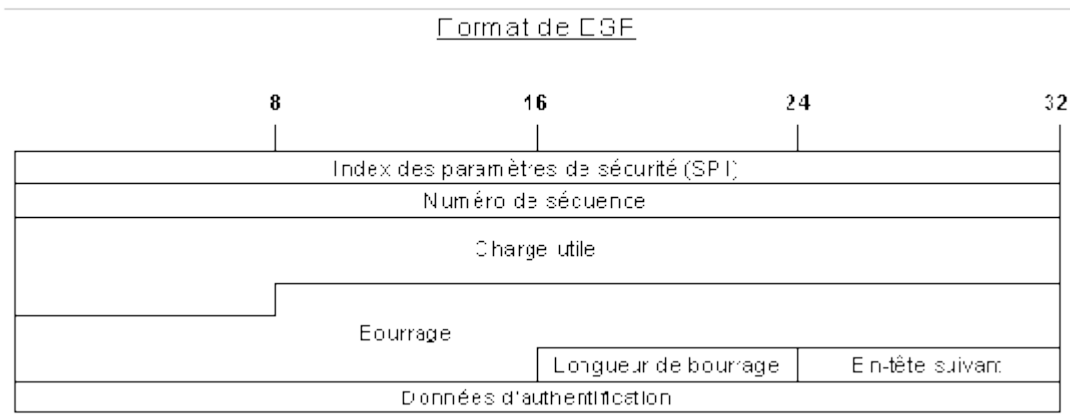
7.2.3.1. ESP(Encapsuling Security Payload)

Il fournit des services de confidentialité, d'intégrité, d'authentification et d'anti-renvoi(paquet capturé par un tiers et retransmis). Il est monté directement au sommet de IP en utilisant le numéro de protocole 50.

ESP utilise des algorithmes de clés symétriques tels que DES, 3DES ou AES et des méthodes de hachage telles que MD5 et SHA-1 qui fournissent des services de sécurité.

Il peut utiliser le mode transport et le mode tunnel.

Paquet ESP en mode tunnel :



7.2.3.2. AH(Authentication Header)

Il fournit seulement l'intégrité, l'authentification et l'anti-renvoi des données. Il est identifié par le numéro de protocole 51.

Il utilise MD5 et SHA-1 pour fournir des services d'intégrité de données.

Il peut utiliser le mode transport et le mode tunnel.

Paquet AH n mode tunnel :

En-tête suivant	Longueur	Réservé
Index des paramètres de sécurité (SPI)		
Numéro de séquence		
Données d'authentification (longueur variable)		

7.2.3.3. Etablissement d'un tunnel IPSec

- Phase 1 : Echange de clés (s'assurer que celui qui est de l'autre côté est bien celui qu'on pense)
IKE (Internet Key Exchange) Phase 1 établit un canal sécurisé entre des gateways en utilisant l'échange de clés de Diffie-Hellman (avec PKI (Certificat authentification) ou Shared Secret (même mot de passe de chaque côté)).

Quand l'identité est établit, il faut passer à la phase 2.

- Phase 2 :Etablissement des clés de sessions et de mode de cryptage (DES, AES, 3DES, MD, SHA1, ...)

IKE Phase 2 établit des associations de sécurité (SA) pour un ensemble de polices VPN.

Quand la phase 2 est réalisée avec succès, les données peuvent circuler via le tunnel IPSec. Les données sont encryptées, authentifiées, et encapsulées en utilisant les standards IPSec.

7.3. Comment fonctionne un VPN ?

Le canal VPN est une session directe temporaire (tunneling) entre 2 machines ou 2 réseaux.

Le point d'extrémité d'un VPN est l'endroit où le trafic VPN entre dans le réseau .

Le VPN peut échanger un ensemble de secrets partagés pour créer une clé de cryptage. Le trafic transmis le long du canal établi est bouclé d'un package crypté qui comporte une adresse à l'extérieur du package, mais le contenu est masqué. Le contenu original est masqué, mais il contient suffisamment d'informations pour arriver à destination. Une fois que les données sont arrivées à destination, l'enveloppe est en toute sécurité supprimée.

Une session VPN se déroule de la façon suivante :

- L'utilisateur distant demande une connexion VPN
- La machine destinataire reçoit la requête et établit un tunnel temporaire. La machine destinataire commence à configurer le tunnel.
- L'ordinateur et la machine destinataire partagent leurs clés (phase 1) et le réseau de destination définit comment le trafic va être encapsulé dans les enveloppes cryptées. Les 2 clés ont été préalablement créées, elles sont cryptés et incompréhensibles à tout intrus.
- La machine destinataire envoie un test à l'utilisateur distant pour l'authentifier.
- L'utilisateur distant utilise son ID utilisateur et son mot de passe et tout ce qui est requis pour authentifier le réseau de destination. (configurations faites lors de l'installation du

- VPN)
- Le réseau de destination vérifie l'utilisateur distant et assigne une adresse temporaire à la machine distante.
 - Le canal de communication crypté est établi (Phase 2). Les données commencent à être transmises via le VPN.

7.4. Implémentation d'un VPN

★ Implémentation d'un VPN de façon logicielle

Il faut d'un part créer le serveur VPN qui recevra les connexions entrantes et ensuite les clients VPN qui veulent communiquer avec le serveur VPN.

Voir les sites suivants :

<http://www.commentcamarche.net/pratique/vpn-xp.php3>

<http://www.generation-nt.com/index.php?cat=dossiers44>

★ Implémentation d'un VPN avec matériel

19. Configurer la phase 1 : échange de clés (IKE Gateway)
 - 19.1. Créer et configurer un Gateway IKE ; nom du Gateway, interface du VPN, adresse du gateway
 - 19.2. Configuration avancée du GateWay IKE : clé préhaché et prépartagé, numéro de groupe DH, Algorithme d'encryption et algorithme d'intégrité et authentification
20. Configurer la phase 2 : Etablissement des clés de sessions et de mode de cryptage
 - 20.1. Créer et configurer VPN IKE : nom du VPN
 - 20.2. Configuration avancée de VPN IKE : choix du groupe DH, du protocole IPSec (AH – EPS), algorithme d'encryption et algorithme d'authentification
21. Créer les objets (entrée d'adresses, services)
22. Créer les règles à respecter pour le VPN

Annexes :

En-tête AH :

En-tête suivant	Longueur	Réservé
Index des paramètres de sécurité (SPI)		
Numéro de séquence		
Données d'authentification (longueur variable)		

Pacquet ESP :

