

Système et réseau Cours

INSA INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
ROUEN



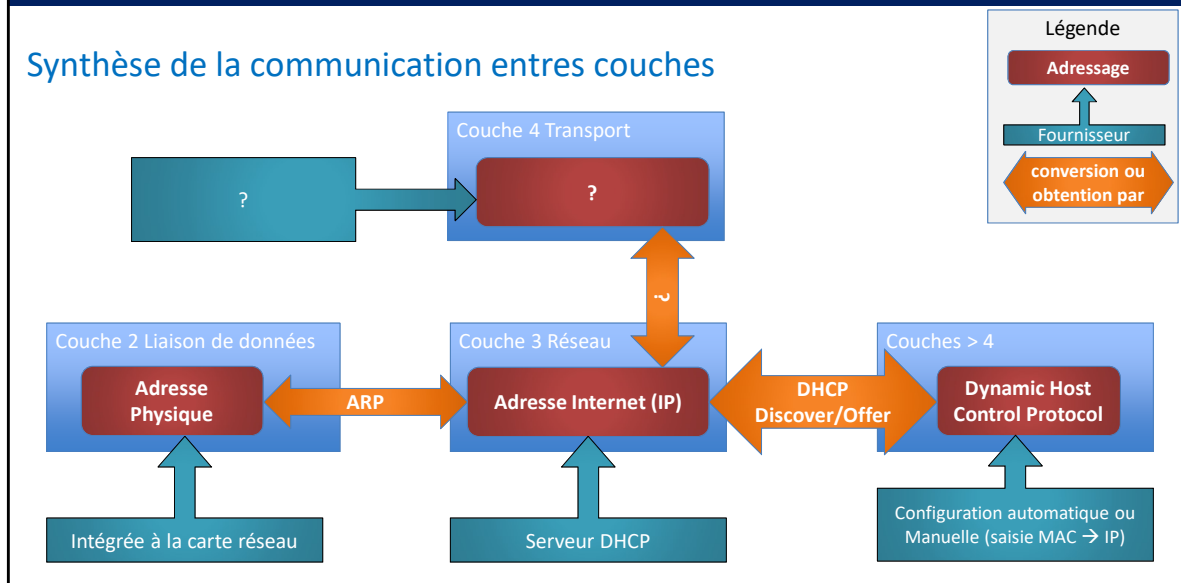
3



www.wooclap.com/NCNXRY

Repérage et protocoles dans la famille TCP/IP

Synthèse de la communication entre couches



Etat de nos connaissances actuelles.

Nous savons maintenant que l'adresse IP, si elle n'est pas forcée par l'utilisateur, nous provient d'un serveur DHCP

Couche 4 UDP & TCP

Deux protocoles
pour le transport



Application
+
Présentation
+
Session

Transport

Réseau

Liaison
de données

Physique

La couche Transport : UDP et TCP

■ PARTICULARITÉS :

- Décompose l'information en segments numérotés (⚠ Taille d'une trame)
- Utilisation **ports** pour établir le dialogue : Source vers Destination
- Le couple Adresse IP + Port est nommé Socket

■ LES PROBLÈMES LIÉS AU TRANSPORT :

- IP n'a pas de route stable
- La charge du réseau est imprévisible

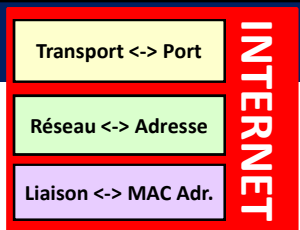
Pas de route stable : La route d'accès à un serveur en passant à travers des routeurs peut changer dans le temps.

Les ports : identification de services 57

Port Connus : 0 à 1023 sont utilisés par les OS
Enregistrés : 1024 à 49151 (par l'IANA)
Dynamique : 49152 ($2^{15}+2^{14}$) à 65535 (non enregistrable)

Une liste des ports et leur utilisation est visible dans le fichier **services**.
 (/etc/services pour Linux, et dans c:\windows\system32\drivers\etc\services pour Windows)

Port	Utilisation	Port	Utilisation
20,21	FTP (File Transfert Protocol)	22	SSH (Secure Shell = terminal distant sécurisé)
23	Telnet (Terminal distant non sécurisé)	25	SMTP (Simple Mail Transfert Protocol)
53	DNS (Domaine Name System)	68	DHCP (Dynamic Host Control Protocol)
80	HTTP (Hyper Text Transfert Protocol)	110	POP3 (Post Office Protocole)
137-139	Netbios Windows	143	IMAP (Internet Message Access Protocol)
443	HTTPs (HTTP sécurisé par certificats)	993	IMAPs
995	POP3s (Post Office Protocol)	389	Annuaire LDAP (Lightweight Directory Access P.)
3389	RDP (Remote Desktop : bureau distant)	5900	VNC (contrôle distant)



Les 1024 premiers ports sont difficilement utilisable si vous n'êtes pas administrateur du poste.

L'IANA est Internet Assigned Numbers Authority : société a but non lucratif qui supervise en autre l'attribution des adresses IP.

Les ports dynamiques sont utilisés aléatoirement par le système d'exploitation lors d'une connexion à un service, qui lui sera fixe, exemple, la connexion a du HTTP va utiliser un port entre 49152 et 65535 (client) mais va directement aller sur le port 80 (serveur).
 $49152 = 2^{16} - 2^{14}$. On utilise les 2^{14} (16384) derniers ports pour la partie dynamique

Protocole UDP : User Datagram Protocol

■ CARACTÉRISTIQUES UDP :

- Protocole simple et efficace
- Débit élevé
- Aucune garantie : **Mode non connecté** et non fiable
- L'information peut arriver dans le désordre



■ EXEMPLES D'UTILISATION

- Un seul échange
- Temps réel
- Faible empreinte du code, etc.

■ APPLICATIONS

- DNS (Port 53)
- TFTP (Port 69)
- SNMP (Port 161) / Trap SNMP (Port 162)



TFTP = Trivial File Transfert Protocole (protocole simple pour le transfert de fichiers=
SNMP = Simple Network Management Protocol (utilisé pour la gestion d'hôte réseau)

Protocole TCP : Transmission Control Protocol



■ CARACTÉRISTIQUES TCP :

- Transport bidirectionnel et fiable
- **Connexion obligatoire** entre les deux interlocuteurs
- Indépendant des caractéristiques des réseaux traversés (Ethernet, ADSL ...)
- Informations délivrées dans l'ordre, sans perte ni doublon
(le contenu de l'information est sans aucune importance => transparence)

TCP Transmission Control Protocol



■ CARACTÉRISTIQUES TCP :

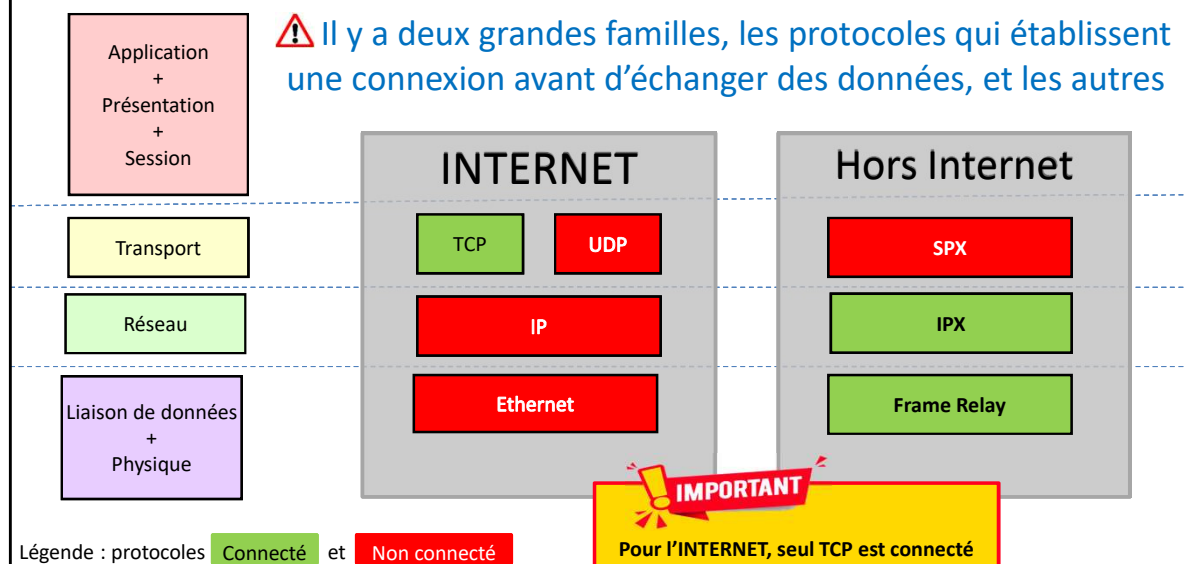
- Prise en compte des caractéristiques des ressources réseaux (délai de connexion, débit, temps de transport, taux d'erreur)
- C'est TCP qui décide de la taille des données
- Découpe / assemble en segments les données à transmettre
- MSS (Maximum Segment Size) déterminé à l'ouverture de connexion
- Fournit un contrôle de flux dynamique (dialogue récepteur

Multiplexage : plusieurs conversations des couches supérieures dans une seule connexion

TCP effectue un dialogue client/serveur et connaît la taille des données maxi à transférer.

En cas de perte de données, le protocole s'adapte et réduit ses émissions

Synthèse des protocoles connectés de l'Internet



Si le protocole UDP est utilisé, alors seul les couches supérieures peuvent palier un problème de connexion. C'est au développeur de prendre en charge.

Nous ne parlons en cours que des protocoles liés à Internet, mais il en existe d'autres, qui peuvent fonctionner différemment tel IPX qui est sur la couche 3 mais connecté, contrairement à IP.

Des services TCP/IP indispensables

- DHCP (Dynamic Host Configuration Protocol)

IPAM

Application
+
Présentation
+
Session

Transport

Réseau

Liaison
de données

Physique

DHCP (Dynamic Host Configuration Protocol)

Fonctions d'un serveur DHCP :

- Configuration automatique des paramètres IP
- Attribution d'une adresse IP et d'un masque
- Attribution d'une passerelle
- Informe sur le ou les serveurs DNS
- Autres informations optionnelles...



DHCP (Dynamic Host Configuration Protocol)

Fonctionnement

- → Envoi par l'hôte client d'un datagramme **DHCP Discover**
- ← Un serveur DHCP répond un **DHCP Offer**
avec une proposition d'adresse et de masque
- → Le client envoie un **DHCP Request**
- ← Le serveur valide par un **DHCP Ack**



Un datagramme est un paquet de données transmis avec ses adresses de source et de destination par un réseau de télécommunications.
C'est une communication SANS CONNEXION

DHCP (Dynamic Host Configuration Protocol)

Informations

- Ports utilisés **67** (serveur) et **68** (client)
- Broadcast de l'adresse **0.0.0.0** sur **255.255.255.255**
- Protocole de transport **UDP**
- Sans un relais particulier, le message **ne traverse par les routeurs**
- Des dizaines d'informations complémentaires en plus de l'IP et du masque sont possibles : **passerelle, serveurs DNS, WINS, Boot etc.**
- Durée de vie de l'adresse liée à un bail



Capture des requêtes DHCP

Filtre : bootp

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp.dhcp

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover Transa
2	0.001374	192.168.1.1	192.168.1.44	DHCP	DHCP Offer Transa
3	0.003956	0.0.0.0	255.255.255.255	DHCP	DHCP Request Transa
4	0.005482	192.168.1.1	192.168.1.44	DHCP	DHCP ACK Transa

Frame 1 (346 bytes on wire, 346 bytes captured)

- Ethernet II, Src: CadmusCo_d4:ae:76 (08:00:27:d4:ae:76), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
- User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
- Bootstrap Protocol

DHCP

Routage

- Sortir vers Internet
- Trouver son chemin

Toute Direction
10.0.0.0/24
Mon réseau

Application
+
Présentation
+
Session

Transport

Réseau


Liaison
de données

Physique

Routage IP

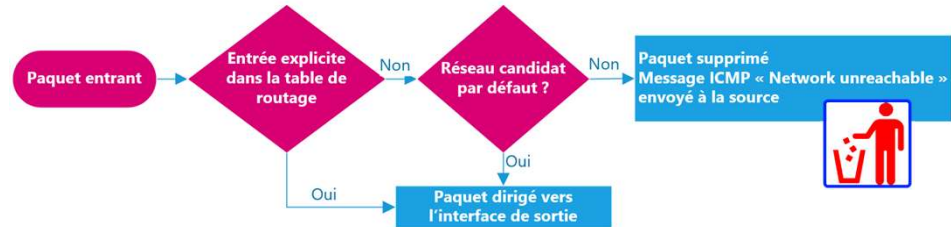


■ PRINCIPES :

- Toute machine utilisant IP gère une table de routage
- Cette table utilise les adresses réseaux pour diriger les trames vers le destinataire
- Un hôte ne réémet jamais des trames qui ne le concerne pas 
- Le routeur retransmet les trames vers l'une de ses cartes réseaux (au moins 2 sur un routeur)

Routage par défaut

Routage des paquets en fonction des entrées dans la table de routage



■ ALGORITHME DE ROUTAGE IP :

- L'adresse IP complète est elle dans la table ? Oui → Envoi
- Sinon : l'adresse de réseau (IP ET Masque) ? Oui → Envoi
- Sinon envoi à l'adresse de l'entrée par défaut (default) si elle existe
- Sinon message ICMP "host/network unreachable"
- Décision prise sur le principe de la correspondance la plus longue. Si plusieurs entrées existent alors la plus précise sera choisie.



Mise à jour de la table de routage des routeurs

- **Routage statique**

Implique des mises à jour manuelle (commande route sur un PC).

Viable sur un petit réseau uniquement.

- **Routage dynamique**

Construction automatique de la table de routage par un dialogue avec les autres routeurs (multicast)

Deux approches :

- Vecteur de distance : Distance Vector Routing
- Etat de liens : Link State Routing



Commandes système liées au routage

- Voir la table de routage

`netstat -nr`

Note : le métrique ajoute une notion de coût à la communication.
Le plus faible est le prioritaire en cas d'ambiguïté.

IPv4 Table de routage de la machine d'IP 192.168.1.24

Itinéraires actifs :

Destination réseau	Masque réseau	Adr. passerelle	Adr. interface	Métrique
0.0.0.0	0.0.0.0	192.168.1.254	192.168.1.24	25
192.168.1.0	255.255.255.0	On-link	192.168.1.24	291
192.168.1.24	255.255.255.255	On-link	192.168.1.24	291
192.168.1.255	255.255.255.255	On-link	192.168.1.24	291
224.0.0.0	240.0.0.0	On-link	192.168.1.24	291
255.255.255.255	255.255.255.255	On-link	192.168.1.24	291

0.0.0.0/0 Toutes les communications vont vers la passerelle 192.168.1.254 en utilisant la carte réseau d'IP 192.168.1.24

192.168.1.24 /24 Pour atteindre ce réseau, utilisation directe de la carte réseau d'IP 192.168.1.24

Pour atteindre spécifiquement cette carte réseau, utilisation directe de la carte réseau d'IP 192.168.1.24

- Suivre une route

`tracert` (windows)

`traceroute` (linux)

Cette commande montre les routeurs traversés pour atteindre la destination, le temps et éventuellement la résolution DNS inverse de l'IP du routeur

`tracert moodle.insa-rouen.fr`

Détermination de l'itinéraire vers moodle-2018.insa-rouen.fr [193.49.10.217]

avec un maximum de 30 sauts :

1	1 ms	2 ms	2 ms	bbox.lan [192.168.1.254]
2	5 ms	4 ms	5 ms	i19-les03-th2-31-37-224-2.sfr.lns.abo.bbox.fr [31.37.224.2]
3	9 ms	8 ms	8 ms	be21.cbr01-ntr.net.bbox.fr [212.194.171.28]
4	*	*	*	Délai d'attente de la demande dépassé.
5	16 ms	7 ms	9 ms	renater.par.franceix.net [37.49.236.19]
6	8 ms	9 ms	7 ms	xe-1-0-9-parisl-rtr-131.noc.renater.fr [193.51.177.146]
7	10 ms	10 ms	9 ms	te0-1-0-2-ren-nr-rouen-rtr-091.noc.renater.fr [193.51.177.31]
8	14 ms	9 ms	13 ms	sythano-vi3201-te4-3-rouen-rtr-021.noc.renater.fr [193.51.184.129]
9	12 ms	11 ms	10 ms	insa-ser-s3.sythano.net [194.57.245.90]
10	10 ms	10 ms	10 ms	moodle-2018.insa-rouen.fr [193.49.10.217]

Itinéraire déterminé.

NAT

Network Address Translation

Application
+
Présentation
+
Session

Transport

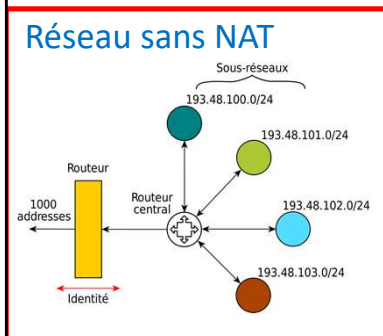
Réseau

Liaison
de données

Physique

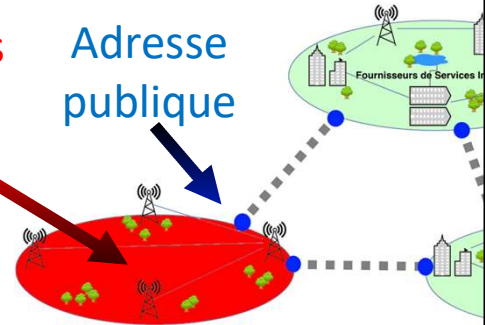
NAT : Principe général

Le **Network Address Translation** permet aux hôtes d'un réseau de partager une adresse IP publique pour dialoguer hors de leur réseau constitué d'adresses privées (qui ne sont ni uniques, ni routables sur l'internet)



Adresses
privées

Adresse
publique



NAPT – Network Address Port Translation

- RFC 3022 datant de janvier 2001
- Remplace le NAT de 1995 qui consommait trop d'adresses publiques
- Utilise une table de correspondance **“Adresse privée / numéro de port”** vers **“adresse publique / numéro de port”**
- N'utilise qu'une seule IP Publique
- Une seule adresse publique peut être utilisée
- 16384 “private ports” ports 49152 à 65535

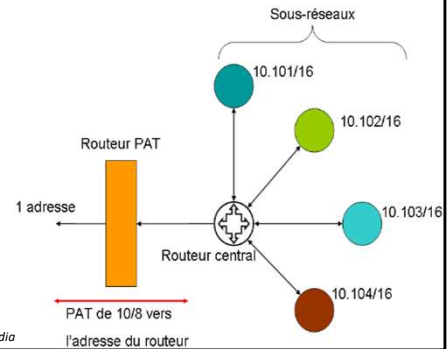


Illustration Wikipedia

NOTE : Il existe une ancienne version, non présentée ici , le Network Address Translation
NAT : RFC 1631 mai 1994 : Première version utilisant un pool d'adresse publique
Besoin d'autant d'adresses publiques que d'adresses privées devant sortir sur l'Internet
Utilise une table de correspondance adresse privée - adresse publique
Mécanisme initial utilisé pour palier à la pénurie d'adresse IPv4

NAPT – Network Address Port Translation

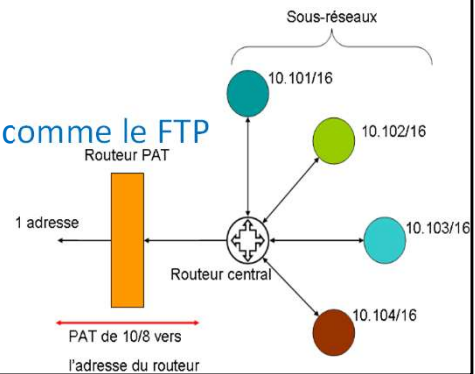
■ FONCTIONNEMENT

- Beaucoup plus lourd que le simple NAT car il y a modification des données transportées.

- Non-transparence au niveau applicatif

Ex : problème de protocole contenant une IP comme le FTP

- Délais supplémentaires



Et dans l'autre sens ? Le Port Forwarding

Fonctionnement Inverse (de l'internet vers le réseau local)

- Pour sortir du réseau, l'opération est dynamique
- Pour entrer dans le réseau, il peut être mis en place des règles statiques
- On parle alors de « port forwarding »
- Exemple : tout trafic, quelle que soit l'IP arrivant sur le port 80 sera redirigé sur l'IP 10.101.0.50

Ce système permet l'hébergement d'un serveur Web sur une IP privée.

