

Réseaux : Introduction à TCP/IP

Laurent Signac

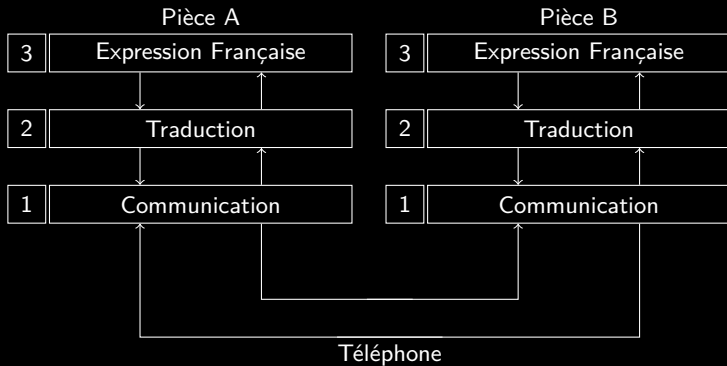
Ensiip – Université de Poitiers

`Laurent.Signac@univ-poitiers.fr`

Réseaux

- 1 Modèle en couche
- 2 Données
- 3 Algorithmes et protocoles
- 4 Machines
- 5 TCP/IP en action
- 6 Capture de trames
- 7 Détail des technos mises en jeu
- 8 La suite
- 9 Notes

Le modèle en couches



Modèle OSI



Application : services pour l'utilisateur, transfert de fichier, courrier électronique...

Présentation : mise en forme de l'information, cryptage, compression ;

Session : gestion et synchronisation du dialogue ;

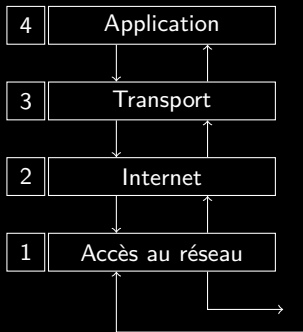
Transport : transmission de bout en bout, réassemblage des données, multiplexage, contrôle de flux ;

Réseau : routage de l'information, adressage ;

Liaison : établissement et contrôle de la liaison logique, acheminement des blocs de données, contrôle des erreurs ;

Physique : transfert des données, détails électroniques, électriques et mécaniques de la liaison ;

Modèle TCP/IP



Application (session, présentation, application) : application et processus utilisant le réseau

Transport (transport) acheminement de bout en bout (TCP ou UDP)

Internet (réseau) datagrammes et routage (IP)

Accès au réseau (physique, liaison) : routine pour accéder au réseau physique

Données et information

Les paquets transitant sur internet contiennent :

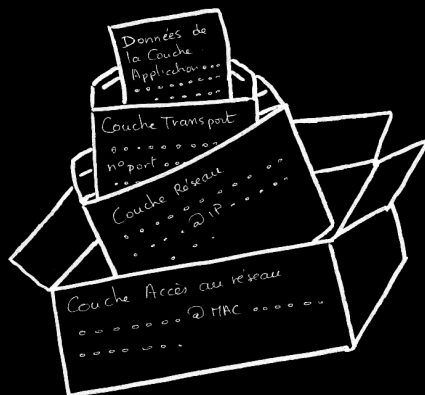
- des adresses (expéditeur, destinataire)
- des contenus (texte, image...)

Le routage et le traitement des paquets est indépendant de leur contenu (neutralité du net).

Les adresse Internet (adresses IP) sont moins utilisées par les humains que les adresses symboliques comme `wikipedia.fr`.

Encapsulation

- Lors du passage des couches supérieures vers les couches inférieures, les données sont placées dans une nouvelle enveloppe contenant de nouvelles informations.
- Lors de la remontée dans les couches, les enveloppes sont décachetées



Protocoles

Protocole

Un protocole est un ensemble de règles strictes nécessaires et suffisantes à la réalisation d'un service particulier

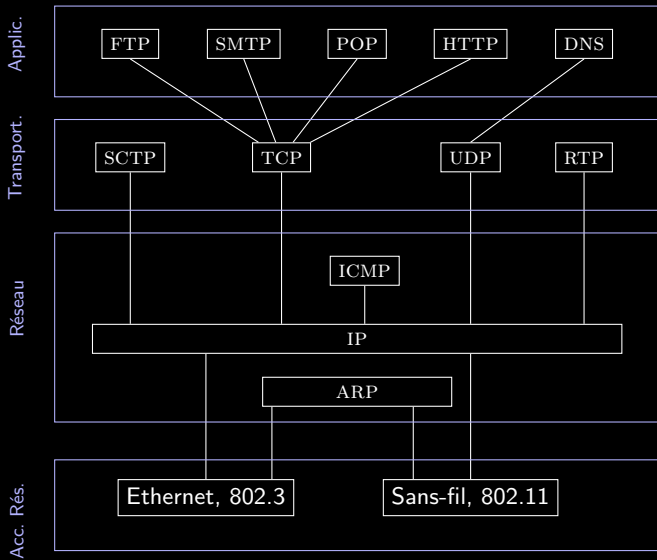
Dans les 4 (ou 5) couches qui constituent la pile TCP/IP, vivent un certain nombre de protocoles. La plupart sont décrits **très précisément** par des RFC :

- <http://www.ietf.org/rfc.html>
- Exemple de la RFC d'HTTP :
<http://www.rfc-editor.org/rfc/rfc1945.txt>

http://fr.wikipedia.org/wiki/Suite_des_protocoles_Internet

Autres algorithmes

Internet repose sur d'autres algorithmes que les protocoles de communication, en particulier les algorithmes de routage qui permettent d'aiguiller les paquets (voir plus loin)



Internet : logiciel ou matériel ?

Les protocoles spécifiques à Internet sont logiciels, placés dans les couches au dessus de la couche Physique.

⇒ Internet peut fonctionner sur tout type de machine / réseau physique.

TCP/IP en action : une page Web

On consulte :

`http://deptinfo-ensip.univ-poitiers.fr/demo/page.html`
(page simple, sans redirection, avec du texte et une image...)

URL

L'*Uniform Resource Locator* (adresse réticulaire) identifie une ressource et le moyen de l'obtenir :

- document /demo/page.html
- sur la machine deptinfo-ensip.univ-poitiers.fr
- en utilisant le **protocole HTTP** (qui utilise par défaut le port 80).

L'adresse est rentrée par l'utilisateur, dans un navigateur. Le navigateur implémente le protocole HTTP de la couche application et satisfait la requête.

Mais comment fait-il ?

Capture des trames


Capture réalisée avec Wireshark :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	IntelCor_cl:ec:ab	Broadcast	ARP	42	Who has 172.16.111.252? Tell 172.16.102.64
2	0.001701282	IntelCor_21:20:ac	IntelCor_cl:ec:ab	ARP	56	172.16.111.252 is at 00:15:17:21:20:ac
3	0.001712610	172.16.102.64	193.55.138.46	DNS	91	Standard query 0x6bf2 A deptinfo-ensip.univ-poitiers.fr
4	0.001721569	172.16.102.64	193.55.138.46	DNS	91	Standard query 0xa6dd AAAA deptinfo-ensip.univ-poitiers.fr
5	0.002995311	193.55.138.46	172.16.102.64	DNS	190	Standard query response 0x6bf2 A deptinfo-ensip.univ-poitiers.fr A 194.254.43.242 NS
6	0.003596480	193.55.138.46	172.16.102.64	DNS	145	Standard query response 0xa6dd AAAA deptinfo-ensip.univ-poitiers.fr SOA thetis.univ
7	0.003762492	172.16.102.64	194.254.43.242	TCP	74	32826 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2297403 TSecr=0 W
8	0.005176966	194.254.43.242	172.16.102.64	TCP	74	80 → 32826 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1300 SACK_PERM=1 TSval=815266
9	0.005209789	172.16.102.64	194.254.43.242	TCP	66	32826 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2297403 TSecr=815266921
10	0.005288163	172.16.102.64	194.254.43.242	HTTP	238	GET /demo/page.html HTTP/1.1
11	0.006984745	194.254.43.242	172.16.102.64	TCP	66	80 → 32826 [ACK] Seq=1 Ack=173 Win=30080 Len=0 TSval=815266921 TSecr=2297403
12	0.008295369	194.254.43.242	172.16.102.64	HTTP	505	HTTP/1.1 200 OK (text/html)
13	0.008308640	172.16.102.64	194.254.43.242	TCP	66	32826 → 80 [ACK] Seq=173 Ack=440 Win=30336 Len=0 TSval=2297404 TSecr=815266922
14	0.009270075	172.16.102.64	194.254.43.242	TCP	66	32826 → 80 [FIN, ACK] Seq=173 Ack=440 Win=30336 Len=0 TSval=2297404 TSecr=815266922
15	0.010441886	194.254.43.242	172.16.102.64	TCP	66	80 → 32826 [FIN, ACK] Seq=440 Ack=174 Win=30080 Len=0 TSval=815266922 TSecr=2297404
16	0.010455628	172.16.102.64	194.254.43.242	TCP	66	32826 → 80 [ACK] Seq=174 Ack=441 Win=30336 Len=0 TSval=2297405 TSecr=815266922

Déroutement des opérations....

- obtenir `http://deptinfo-ensip... ?` besoin de l'@ IP
- obtenir l'@ IP ? consulter le serveur de noms¹
- joindre `193.55.138.46 ?` rechercher une route
- route vers `193.55.138.46 ?` consulter la table de routage
- utiliser `172.16.111.252` comme intermédiaire ? quelle est son adresse physique ?
- obtenir l'adresse physique de `172.16.111.252 ?` Requête ARP (réception de la réponse : `00 :15 :17 :21 :20 :AC`)
- poster la requêtes DNS pour `193.55.138.46` en mettant comme destinataire : `00 :15 :17 : :21 :20 :AC`
- réception réponse DNS : l'IP de `deptinfo-ensip...` est `194.254.43.242`
- joindre `194.254.43.242 ?` rechercher une route
- route vers `194.254.43.242 ?` consulter la table de routage
- utiliser `172.16.111.252` comme intermédiaire - son adresse physique est dans le cache.
- établissement d'une connexion TCP sur le port 80 de la machine `194.254.43.242`, @ physique de destination `00 :15 :17 :21 :20 :AC`
- communication avec `194.254.43.242` en utilisant le protocole HTTP : `GET /documents/page.html`
- récupération de la page au format HTML... et des autres éléments nécessaires.
- affichage dans le navigateur

La suite...

1. configuration réseau, un serveur de nom est configuré : `193.55.138.46` 

Adresse IP

- Permet d'identifier une machine reliée à Internet.
- IPv4 : Adresses de 4 octets.
- Chaque machine appartient à un réseau. L'@ IP donne l'adresse du réseau, et le numéro de la machine dans ce réseau :
 - Réseau : rue
 - Numéro de machine : maison dans la rue.

Masque

Le masque permet de couper une @ IP en deux : nom rue + numéro dans la rue

Exemple

172.16.102.64/20 (@IP, masque sur 20 bits) :

$\underbrace{10101100.00010000.0110}_{20 \text{ bits, nom rue}} \quad \underbrace{0110.01000000}_{\text{numéro dans la rue}}$

- ce réseau peut contenir $2^{12} - 2$ machines au plus
- l'adresse du réseau est 172.16.96.0/20
- l'adresse de diffusion est 172.16.111.255/20

Autre notation du masque

En décimal pointé, masque de 20 :

11111111.11111111.11110000.00000000 \Rightarrow 255.255.240.0

Rechercher une route

- Quel chemin va prendre le courrier (papier) pour aller du point A (Poitiers) au point B (Auckland) ?
 - Bal – Centre de tri Poitiers – Paris – New-York – Sidney – Auckland ?
 - Bal – Centre de tri Poitiers – Paris – Honk-Hong – Auckland ?
- Celui qui poste dans la boîte l'ignore.
- Il dépose juste sa lettre dans la boîte la plus près de chez lui. C'est l'adresse de cette boîte qu'on cherche lorsqu'on cherche une route.

Traceroute

```
> traceroute to 193.55.138.46 (193.55.138.46), 30 hops max, 60 byte packets
 1  172.16.111.252 (17.16.111.252) 0.892 ms 1.200 ms 1.536 ms
 2  193.55.138.46 (193.55.138.46) 28.922 ms 29.643 ms 30.119 ms
```

► Infos ↔

Table de routage

Table de routage :

```
> route -n
Table de routage IP du noyau
Destination    Passerelle      Genmask          Indic Metric Ref    Use Iface
0.0.0.0        172.16.111.252 0.0.0.0          UG    0      0      0 eth0
172.16.96.0    0.0.0.0         255.255.240.0   U     1      0      0 eth0
```

► Infos ↔ Sous windows : route print

<http://qpleple.com/routing/>

Adresse Physique

L'adresse physique :

- identifie de manière unique le matériel
- l'adressage physique n'est pas hiérarchique (rien n'indique dans l'@ physique si deux matériels sont proches).

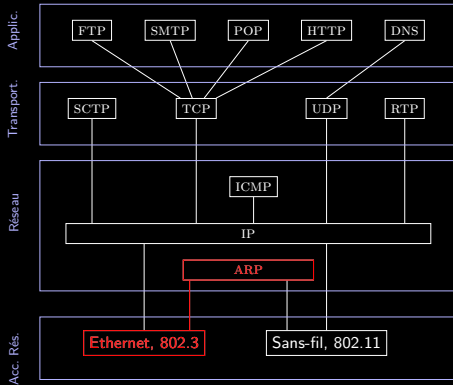
Pourquoi a-t-on besoin des @ physiques en plus des @ IP ?

- l'@ physique est gérée par les couches basses, par le matériel, donc très rapidement, et juste à l'entrée de la carte réseau
- l'@ physique est en tout début de trame, donc très facilement/rapidement accessible

► Infos ↔

http://arsene.perez-mas.pagesperso-orange.fr/reseaux/tcpip/arp/adresses_mac.htm

Address Resolution Protocol (ARP)



<http://www.rfc-editor.org/std/std37.txt>
 Permet à une machine de questionner son réseau pour obtenir une adresse physique.

Salut à tous^a, qui est 172.16.111.252 (ac :10 :6f :fc) ?

a. à tous : ff :ff :ff :ff :ff :ff

Format des trames Ethernet :

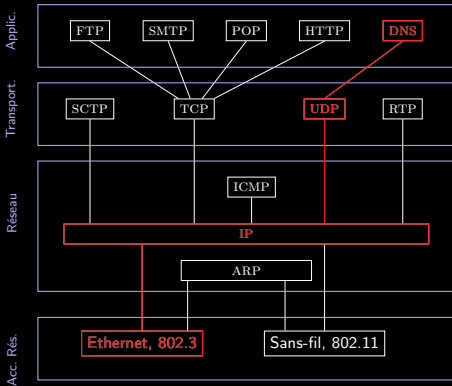
- @ Dest. [6]
- @ Source [6]
- Type (ARP=0x806, IP=0x800) [2]

Format des requêtes ARP :

- Type @ matérielle (1=Ethernet) [2]
- Type @ protocole (0x0800=IP) [2]
- Lg @ mat [1]
- Lg @ proto [1]
- Code (1=Request 2=Reply) [2]
- @ Mat. Source
- @ Proto. Source
- @ Mat. Dest
- @ Proto. Dest

► Infos ↩

Domain Name System



DNS : protocole application, port 53, utilise un transport non fiable (UDP)

Requête / réponse :

- Quelle est l'IP associée au nom deptinfo....fr ?
- L'ip associée est : 194.254.43.242

► Infos ↩

Cache ARP

```
> arp -n
Address          Hwtype HWaddress          Flags Mask Iface
172.16.111.252  ether  00:15:17:21:20:AC  C           eth0
```

► Infos ↔

Connexion Tcp

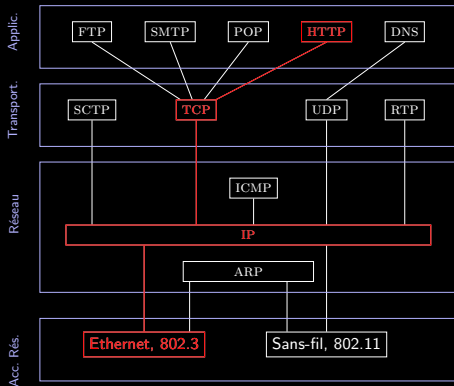
- Tcp gère le flux de l'information et synchronise.
- Tcp s'assure de la bonne réception des données
- Tcp peut réémettre des paquets perdus, ralentir la cadence etc...
- La trame Tcp contient un numéro de port, qui permet de joindre un programme de la couche application implémentant un protocole application particulier (Web, Mail etc...)

Connexion en 3 temps :

- Salut, je veux me connecter, mon numéro de séquence est X
- Salut, numéro de séquence bien reçu, mon numéro de séquence est Y
- Numéro de séquence bien reçu

... les 2 machines sont synchronisées. [▶ Infos](#) ↩

HyperText Tranfert Protocol



- **HTTP** : port 80, utilise TCP (transport sûr, fragmentation, gestion du flux...)
- HTTP est un protocole application en mode texte
- `http://www.rfc-editor.org/rfc/rfc1945.txt` (2616 pour 1.1)
- `GET /demo/page.html HTTP/1.0`

► Infos ↩

HyperText Markup Language

HTML est un langage de balises :

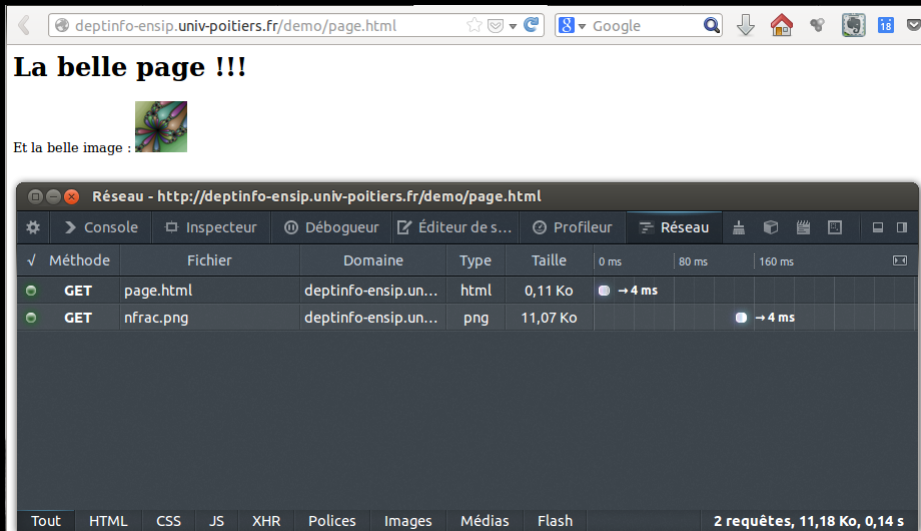
- indique la mise en forme (epaulé par CSS)
- contient du code exécutable (Javascript)

Dans un navigateur : *view source*

```
<html>
<head>
</head>
<body>
<h1> La belle page !!! </h1>
Et la belle image : 
</body>
</html>
```

► Infos ↔

Affichage dans le navigateur



The screenshot shows a web browser window with the address bar containing `deptinfo-ensip.univ-poitiers.fr/demo/page.html`. The page content includes the heading **La belle page !!!** and a colorful butterfly image. Below the page content, a network inspector window is open, displaying the following table:

Méthode	Fichier	Domaine	Type	Taille	0 ms	80 ms	160 ms
GET	page.html	deptinfo-ensip.un...	html	0,11 Ko	→ 4 ms		
GET	nfrac.png	deptinfo-ensip.un...	png	11,07 Ko		→ 4 ms	

At the bottom of the network inspector, it shows: **2 requêtes, 11,18 Ko, 0,14 s**

Simuler un navigateur (telnet)

Le programme Telnet permet d'établir une connexion TCP sur n'importe quel port et d'envoyer/recevoir des données.

Établissons une connexion sur le port 80 du serveur Web !

```
> telnet 194.254.43.242 80
Trying 194.254.43.242...
Connected to 194.254.43.242.
Escape character is '^]'.
GET /demo/page.html HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 18 Nov 2013 09:05:51 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Wed, 03 Oct 2012 13:55:53 GMT
Accept-Ranges: bytes
Content-Length: 117
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<head>
</head>
<body>
<h1> La belle page !!! </h1>
Et la belle image : 
</body>
</html>
Connection closed by foreign host.
```

et SNT dans tout ça.... ?

Protocoles TCP/IP : paquets, routage des paquets

- Distinguer le rôle des protocoles IP et TCP
- Caractériser les principes du routage et ses limites
- Distinguer la fiabilité de transmission et l'absence de garantie temporelle

Adresses symboliques et serveur DNS

Sur des exemples réels, retrouver une adresse IP à partir d'une adresse symbolique et inversement

- outil en ligne : <https://centralops.net/co/>
- Linux : nslookup
- Powershell : Resolve-DnsName

Réseaux pair-à-pair

Décrire l'intérêt des réseaux pair-à-pair ainsi que les usages illicites qu'on peut en faire

Indépendance d'Internet par rapport au contenu physique

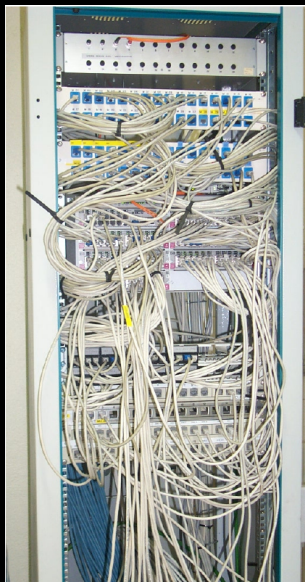
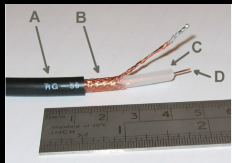
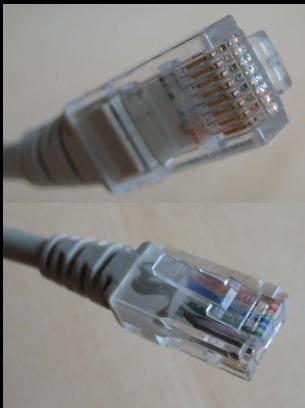
- Caractériser quelques types de réseaux physiques : obsolètes ou actuels, rapides ou lents, filaires ou non
- Caractériser l'ordre de grandeur du trafic des données sur internet et son évolution ^a

a.

- 50% du trafic pour 4 acteurs : Google, Netflix, Akamai, Facebook (01.net),
- trafic de 10^{21} oct/an source : Rapports sur l'état d'internet 2017 et 2018 de l'Arcep

Exemples d'activités

- Illustrer le fonctionnement du routage et de TCP par des activités débranchées ou à l'aide de logiciels dédiés, en tenant compte de la destruction des paquets
Routage élastique :
<https://members.loria.fr/MDuflot/files/med/routage.html>
- Déterminer l'adresse IP d'un équipement et l'adresse du DNS sur un réseau
 - Linux : `cat resolv.conf, ip addr`
 - Powershell : `Get-NetIPConfiguration`
 - Android : Paramètres / État, IP Tools
- Analyser son réseau local pour observer ce qui y est connecté
 - Tous : `ping`
 - Linux : `nmap`
 - Android : Fing, IP Tools
- Suivre le chemin d'un courriel en utilisant une commande du protocole IP



Norme	Nom	Fréquence	Portée	Débit	
802.11a	Wi-Fi 5	5 GHz	10 m	54 Mbits/s	
802.11b	Wi-Fi	2.4 GHz	300 m	11 Mbits/s	
802.11g		2.4 GHz		54 Mbits/s	
802.11i					Chiffrement des transmissions 802.11(a,b,g)
802.11n		5 et 2.4 Ghz	≈150 m	600M/s	Multi antennes

10BaseT	Paires torsadées	10 Mb/s	Ethernet	100m	802.3
10Base2	Coax fin non blindé	10 Mb/s	Ethernet	200m	802.3
10Base5	Coax épais blindé	10 Mb/s	Ethernet	500m	802.3
10BaseF	Fibre optique	10 Mb/s	Ethernet	2km	802.3
100BaseTX	2 paires torsadées	100 Mb/s	F. Ethernet	100m	802.3u
100BaseT4	4 paires torsadées	100 Mb/s	F. Ethernet	100m	802.3u
100BaseFX	2 Fibres optique	100 Mb/s	F. Ethernet	2km	802.3u
1000BaseT	4 paires torsadées	1 Gb/s	G. Ethernet	100m	802.3ab
1000BaseF	Fibre optique	1 Gb/s	G. Ethernet	5km	802.3z
1000BaseLX	Paire de fibres optique	1 Gb/s	G. Ethernet	5km/550m	802.3z
1000BaseSX	Paire de fibres optique	1 Gb/s	G. Ethernet	550m/275m	802.3z
1000BaseCX	2 paires torsadées	1 Gb/s	G. Ethernet	25m	802.3z
		10 Gb/s	10 G. Ethernet		802.3ae

From - Tue Dec 6 09:34:17 2005
X-Account-Key: account4
X-UIDL: 17
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
Return-Path: <Laurent.Signac@univ-poitiers.fr>
Received: from smtp.laposte.net (10.150.9.34) by mx.laposte.net (7.2.060.1)
id 43839F38008C24CD for laurent.signac@laposte.net; Tue, 6 Dec 2005 09:33:49 +0100
Received: from chewbacca.univ-poitiers.fr (195.220.223.33) by smtp.laposte.net (7.2.056.5)
id 43953B68000168F9 for laurent.signac@laposte.net; Tue, 6 Dec 2005 09:33:46 +0100
Received: from goldorak.univ-poitiers.fr (goldorak.univ-poitiers.fr [195.83.66.83])
by chewbacca.univ-poitiers.fr (Postfix) with ESMTP id C0137206C4
for <laurent.signac@laposte.net>; Tue, 6 Dec 2005 09:33:45 +0100 (CET)
Received: from localhost (localhost.localdomain [127.0.0.1])
by goldorak.univ-poitiers.fr (Postfix) with ESMTP id 74C272996
for <laurent.signac@laposte.net>; Tue, 6 Dec 2005 09:33:45 +0100 (CET)
Received: from goldorak.univ-poitiers.fr ([127.0.0.1])
by localhost (goldorak.campus.univ-poitiers.fr [127.0.0.1]) (amavisd-new, port 10024)
with ESMTP id 13966-01 for <laurent.signac@laposte.net>;
Tue, 6 Dec 2005 09:33:43 +0100 (CET)
Received: from [10.16.90.70] (unknown [10.16.90.70])
(using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
(Client did not present a certificate)
by goldorak.univ-poitiers.fr (Postfix) with ESMTP id A94CF29A2
for <laurent.signac@laposte.net>; Tue, 6 Dec 2005 09:33:43 +0100 (CET)
Message-ID: <43954CEB.1070505@univ-poitiers.fr>
Date: Tue, 06 Dec 2005 09:33:47 +0100
From: Laurent Signac <Laurent.Signac@univ-poitiers.fr>
User-Agent: Debian Thunderbird 1.0.2 (X11/20051002)
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: laurent.signac@laposte.net
Subject: Test
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit
X-Virus-Scanned: amavisd-new at univ-poitiers.fr

Qques points non abordés

- adresse Ip spéciales, classes d'adresses
- découpage en sous réseaux
- matériel d'interconnexion (concentrateur, commutateur, routeur) (hub, switch)
- tables de routage plus complexes
- protocoles ICMP POP SMTP
- cryptographie (historique, méthodes actuelles symétriques et asymétriques, applications)
- translation d'adresse
- ~~comment TCP contrôle le flux ?~~
- ~~qqes infos sur les normes (câbles, sans fil)~~

