



INTERNET AVANCÉ

INTRODUCTION

1

2A Apprentissage Informatique & Réseaux

Julien Fasson – julien.fasson@enseeiht.fr

PRÉSENTATION DU SUJET

- Précédemment un tour d'horizon d'Internet
 - Ce que représente Internet et son utilisation
 - Les briques de base d'Internet
 - IP et son adressage
 - Transport
 - Applications
- Mais
 - Le protocole n'est pas l'infrastructure
 - Comment y accède t'on?
 - Un réseau de réseaux signifie une interconnexion
 - Trouver son chemin
 - Version édulcorée du transport
 - Évolution du transport
 - Contrôle de congestion
 - Les applications?

PLAN

Partie 1 – L'architecture d'Internet

Découpage
Intra-FAI
Inter-FAI
Et d'autres...

Partie 2 – Les chemins d'Internet

Différentes solutions?
Les étapes d'élaboration
Les protocoles intra-FAI
Les protocoles inter-FAI
Vers l'interconnexion...

Partie 3 – La question du transport

Retour à TCP
Le contrôle de congestion
La multiplication des solutions

Partie 4 – Les applications

Client-Serveur
Pair-à-pair

Partie 5 – Autour d'IP

IPv6
Tunnel
...

RÉVISION

REPRISE DE(S) (L')EXAMEN(S)

- **Première Session**

- **Seconde Session**



INTERNET AVANCÉ I

ARCHITECTURE

5

2A Apprentissage Info&Réseaux

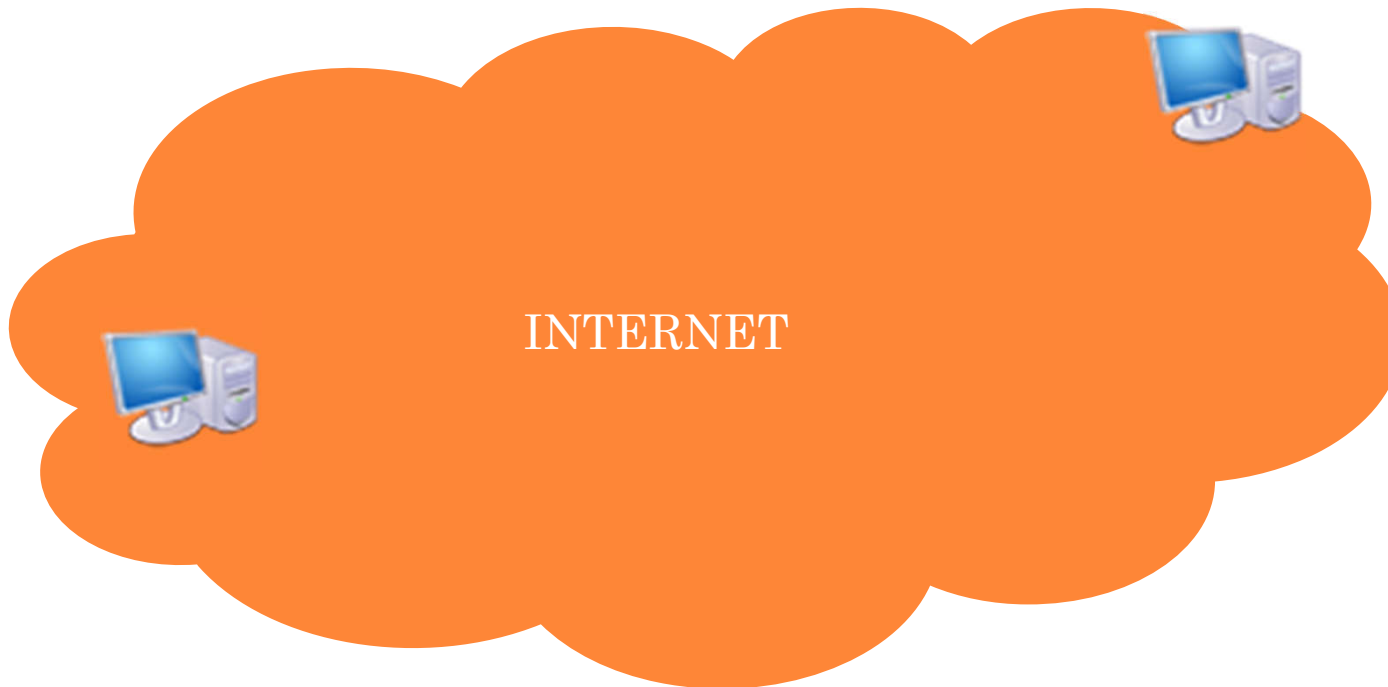
Julien Fasson – julien.fasson@enseeiht.fr

PRÉSENTATION DU SUJET (I)

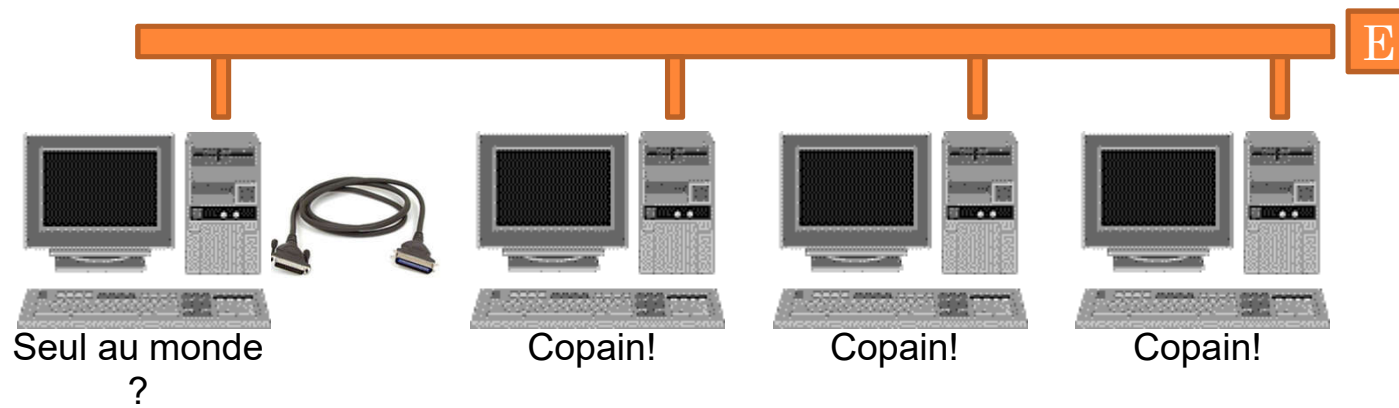
- Besoins pour communiquer entre A et B
 - Gérer le support
 - Pouvoir trouver A et B
 - Mais avant il faut pouvoir atteindre B
 - ...
- Dépendance de l'infrastructure
 - Point à point
 - Un seul réseau
 - Internet?

PRÉSENTATION DU SUJET (II)

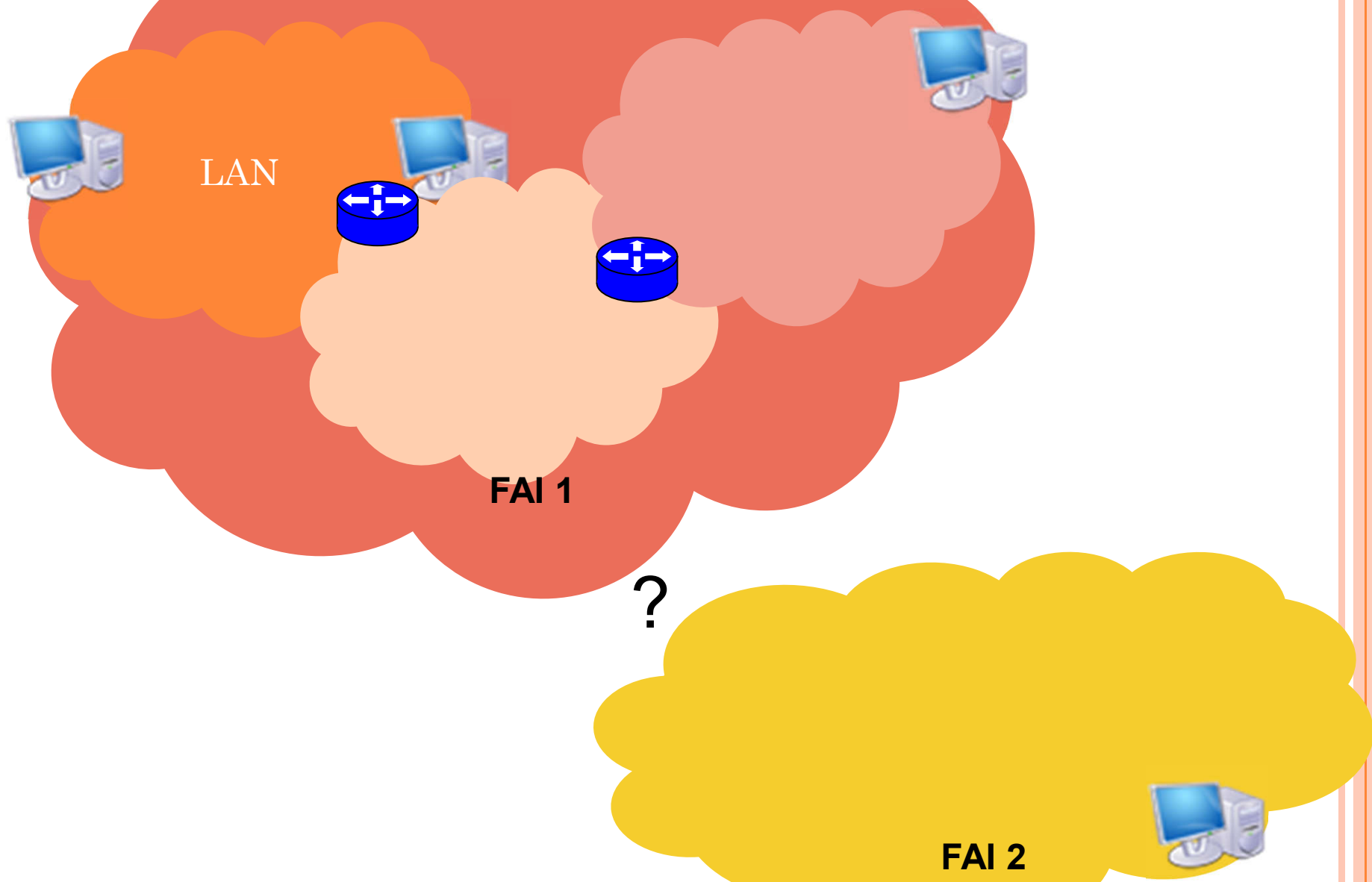
- INTERNET - Un unique réseau mondial?
 - Un lien entre toutes les entités du monde
 - Dans un réseau constitué de réseaux
 - Le plus grand problème d'interconnexion



PRÉSENTATION DU SUJET (III)



PRÉSENTATION DU SUJET (IV)



PRÉSENTATION DU SUJET (IV)

- Un réseau commun?
 - Du réseau local
 - Par un sur-réseau d'un FAI
 - Réseaux d'accès
 - Quid des technologie hétérogènes?
 - ADSL, 2G, 3G, Fibre optique, Ethernet, wifi, ...
 - Interconnexion de réseaux
 - Quid des routes?
 - A un réseau de réseaux
 - Des entités différentes
 - Gestion ?
 - Qui paie?
 - Où s'interconnecter?
 - Comment?

PLAN

- Introduction et présentation du sujet
- Partie 1 – Les réseaux d'accès
- Partie 2 – Les systèmes autonomes
- Partie 3 – Les relations inter-AS
- Conclusion

PARTIE I – LES RÉSEAUX D'ACCÈS

VOCABULAIRE

○ Définitions

- A l'origine: *ensemble des moyens servant à relier des terminaux de télécommunication à un commutateur du réseau d'infrastructure*
- Aujourd'hui : *ensemble des supports physiques et des protocoles qui permettent à un équipement client d'établir une liaison avec le premier routeur de son FAI*

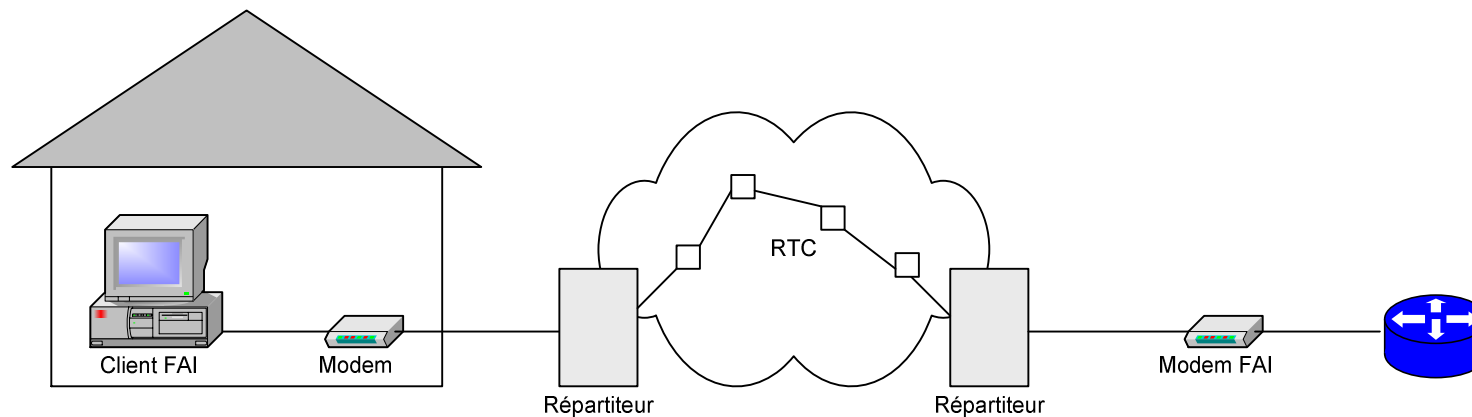
○ Termes associés

- Boucle locale
- Réseau Local *de raccordement*
 - Faux ami ≠ LAN

PARTIE I – LES RÉSEAUX D'ACCÈS

LE RÉSEAU TÉLÉPHONIQUE (I)

- A l'origine
 - Support Téléphonique
 - Paire de cuivre => boucle locale
 - Utilisation de modems



PARTIE I – LES RÉSEAUX D'ACCÈS

LE RÉSEAU TÉLÉPHONIQUE (II) - TD

○ Question 1


- 1.1 Quelle est la technologie qui était classiquement utilisée dans sur la boucle locale des réseaux téléphoniques?
- 1.2 Qu'en est-il dans le réseau cœur téléphonique?

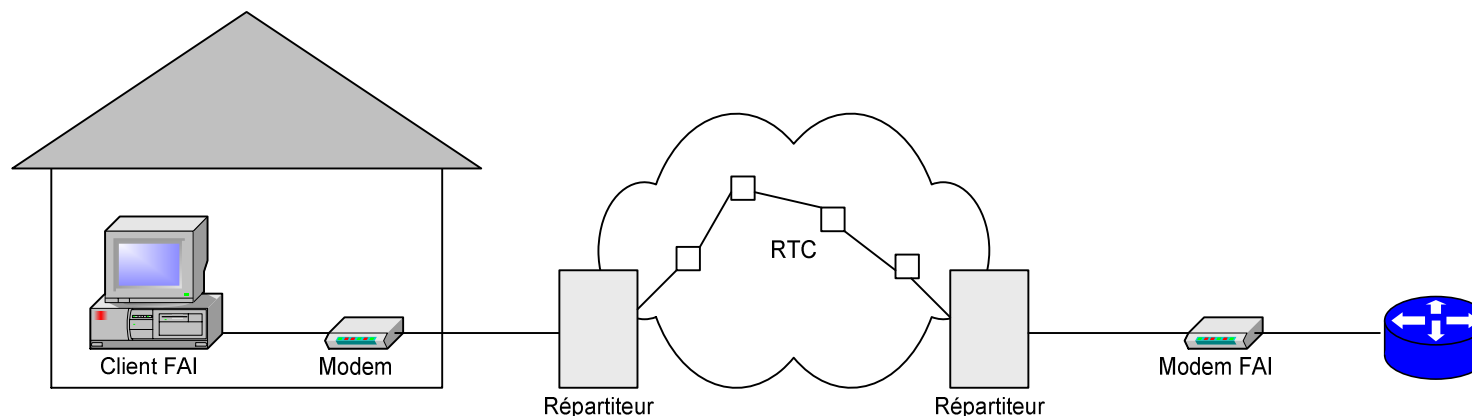
○ Question 2

- 2.1 Quel rôle assure le modem dans le réseau d'accès?
- 2.2 Est-il indispensable?
- 2.3 Pourquoi avoir besoin de deux modems?
- 2.4 Le modem FAI s'occupe-t'il de plusieurs utilisateurs du FAI? Pourquoi?

PARTIE I – LES RÉSEAUX D'ACCÈS

LE RÉSEAU TÉLÉPHONIQUE (III) - TD

- Question 3 – Lister et classer les fonctionnalités à mettre en place au niveau du modem
- Question 4
 - 4.1 Quel protocole est classiquement utilisé?
 - 4.2 Expliquez son fonctionnement 
 - 4.3 Existe t'il d'autres protocoles de ce type?



PARTIE I – LES RÉSEAUX D'ACCÈS

EVOLUTION DES RÉSEAUX D'ACCÈS (I)

- L'évolution du support téléphonique
 - RNIS/ISDN (*Integrated Services Digital Network*)
 - ADSL (Asymmetric Digital Subscriber Line) (*voir exposé*)
 - xDSL
 - Fibre optique - FTTH (*Fiber To The Home*)
 - PON (Passive Optical Network)
 - Partage d'une fibre entre utilisateurs (Jusqu'à 128 utilisateurs sur une fibre par NRO)
 - Fibre par utilisateur (Point à Point Passif)

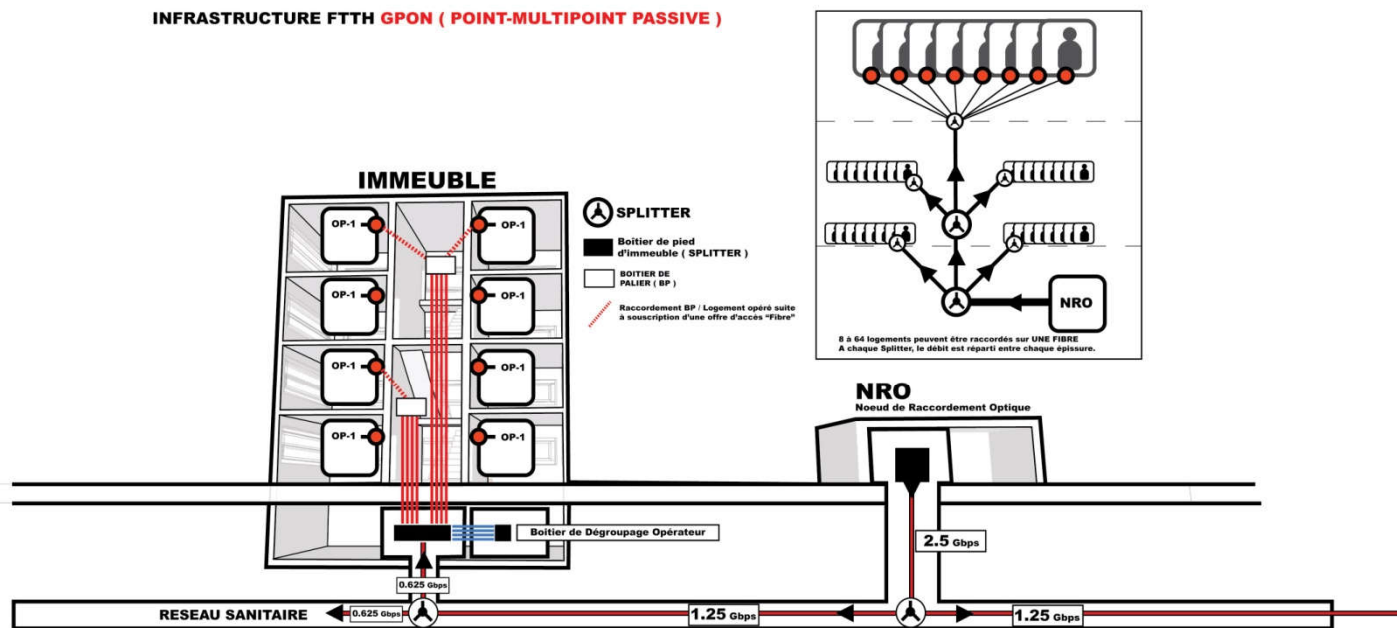
- Illustration P2P passif



PARTIE I – LES RÉSEAUX D'ACCÈS

EVOLUTION DES RÉSEAUX D'ACCÈS (III)

○ Illustration PON

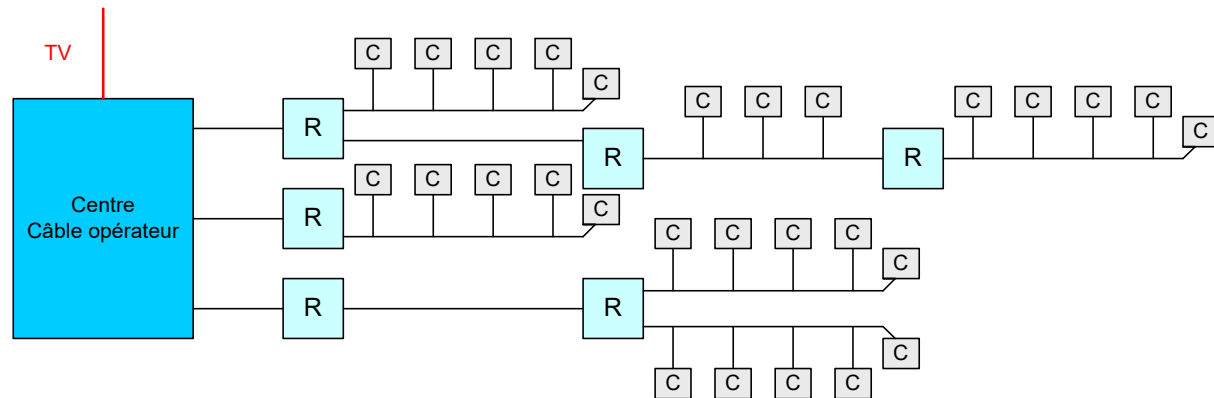


PARTIE I – LES RÉSEAUX D'ACCÈS

EVOLUTION DES RÉSEAUX D'ACCÈS (IV)

○ Le câble

- Analogique
- Numérique
- Fibre optique



○ Les réseaux locaux

- Technologie prédominante = Ethernet
- Réseaux d'entreprise, réseaux universitaire, réseaux de services
- Raccordement
 - Ligne louée
 - Optique
 - xDSL...

PARTIE I – LES RÉSEAUX D'ACCÈS

EVOLUTION DES RÉSEAUX D'ACCÈS (V)

- Les réseaux sans-fil
 - WLAN (wifi essentiellement)
 - Réseaux de téléphonie mobile
 - GSM, GPRS, EDGE, UMTS, CDMA2000
 - Vers LTE
 - Satellite (DOCSIS, DVB-RCS, ...)
 - FSOW (*Free Space Optical Wireless*)
 - Wimax
 - Réseau Hertzien
 - DVB-T, DVB-H, DVB-SH
 - PAN (Personal Area Network)
 - ZigBee, Bluetooth
 - ...

PARTIE I – LES RÉSEAUX D'ACCÈS

CONCLUSION

- Utilisation classique de PPP
 - Établissement d'une liaison point-à-point au routeur sur le réseau d'accès
 - Problème de l'hétérogénéité du réseau d'accès
- Multiplication des technologies d'accès
 - Des technologies loin du mode paquet
 - Des technologies très différentes
 - Lourdeur
- Le réseaux d'accès = un premier problème d'interconnexion

PARTIE II – LES SYSTÈMES AUTONOMES

INTRODUCTION

- A qui appartient Internet?
 - Aux gros opérateurs
 - Aux FAIs
 - A tout le monde car chacun a sa part
 - FAI
 - ISP
 - Collectivités
 - Utilisateurs
- Mais qui gère?
 - Pas d'entité unique
 - Notion d'AS

PARTIE II – LES SYSTÈMES AUTONOMES

DÉFINITION (I)

- Système Autonome – Autonomous System - AS
 - Ensemble de réseaux administrés par la même entité, généralement un FAI
 - Ensemble de routeurs IP interconnectés et régis par un opérateur réseaux qui dispose d'une politique de routage unique et clairement définie

- Conclusion
 - Plan de gestion commun
 - Protocole de routage unique

PARTIE II – LES SYSTÈMES AUTONOMES

DÉFINITION (II)

- Entité administrative
 - Unité technologique?
 - Pas forcément
 - 1 AS / entité?
 - Dépend de l'entité
 - Petit FAI ou fournisseur de service ou entreprise = 1 AS
 - FAI important = plusieurs AS

PARTIE II – LES SYSTÈMES AUTONOMES

LES DIFFÉRENTS TYPES D'AS

- Stub AS
 - AS cul-de-sac
 - Ce type d'AS n'est connecté qu'à un seul
- Multihomed AS
 - Connectivité avec plusieurs AS
 - Pas AS de transit
- Transit AS
 - Permet la connectivité entre les AS
 - Service payant?

PARTIE II – LES SYSTÈMES AUTONOMES

GESTION DES AS (I)

- Numérotation d'AS
 - Réglementation comme les adresses IP
 - Attribution par les RIRs (*Regional Internet Registries*)
 - En Europe RIPE-NCC
 - Numérotation
 - 16 bits
 - 32 bits depuis 2006
 - Attribution en fonction des besoins

PARTIE II – LES SYSTÈMES AUTONOMES

GESTION DES AS (II)

- Gestion des AS par les FAI
 - Le protocole de routage
 - Equipements
 - OS / Drivers / Licences / Cartes / ...
 - Base de données
 - Utilisation de SNMP pour obtenir les données
 - Gestion de la base
 - Centralisation
 - Tri des données et événements
 - Trafic
- Combien d'AS?
 - *Relation inter-AS*

PARTIE II – LES SYSTÈMES AUTONOMES

EXEMPLES D'AS

- AS3215
 - AS de transit
 - France Télécom
 - National (Métropole et DOM)

- AS5511
 - AS de transit
 - France Télécom
 - International

PARTIE III – LES RELATIONS INTER-FAI

PRÉSENTATION

○ Internet

- Pas d'entité unique gérant le réseau => Pas un unique AS
- Plusieurs acteurs => Plusieurs AS

○ Besoin

- Communiquer entre tous les clients
- Interconnecter tous les AS

○ Comment?

- Plusieurs méthodes
- Plusieurs rôles des AS et FAIs

PARTIE III – LES RELATIONS INTER-FAI

COMMUNICATION ENTRE DEUX AS- TD (I)

- Question 1 - Interconnexion de Réseaux
 - 1.1 Comment peut-on interconnecter deux réseaux?
 - 1.2 L'interconnexion entre deux AS est-elle différente? Pourquoi?

- Question 2 - Taille et rôle d'un AS
 - 2.1 Comment mesure t'on la taille d'un AS?
 - 2.2 La taille a-t-elle un lien avec son rôle?
 - 2.3 En quoi la taille d'un AS peut-elle avoir un impact sur l'interconnexion de cet AS avec un autre?

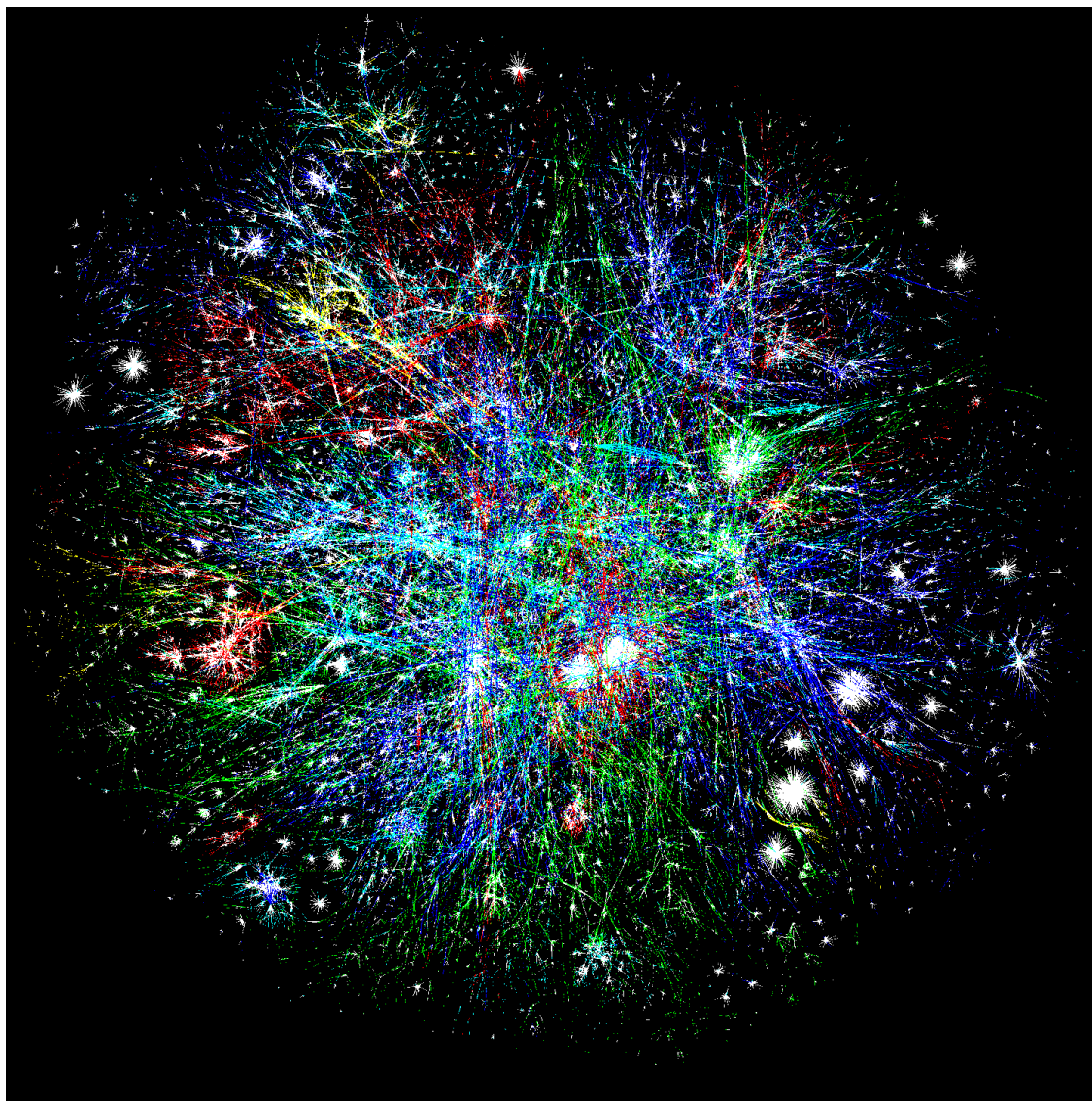
PARTIE III – LES RELATIONS INTER-FAI

COMMUNICATION ENTRE DEUX AS- TD (II)

- Question 3 – Relation inter-AS
 - 3.1 Existe t'il plusieurs types d'interconnexion entre AS? Pourquoi?
 - 3.2 Que nécessite physiquement une interconnexion entre FAI?

PARTIE III – LES RELATIONS INTER-FAI

DESSINE MOI INTERNET!



PARTIE III – LES RELATIONS INTER-FAI

LES DIFFÉRENTS TYPES DE FAIS

- Répartition « classique »
 - Tier-One Provider – échelle mondiale
 - Tier-Two Provider – échelle continentale/nationale
 - Tier-Three Provider – échelle moindre
- Tier-One
 - « Cœurs » d'Internet
 - Quelques Tier-One
 - Level 3 Communications - AS3356
 - Qwest - AS209
 - Sprint - AS1239
 - Tata Communications - AS6453
 - Verizon Business - AS701

PARTIE III – LES RELATIONS INTER-FAI

L'INTERCONNEXION ENTRE LES AS

- Principalement l'interconnexion entre les FAIs
- Le Liant de l'Internet
- Quid des relations inter-FAIs?
 - Politiques?
 - Commerciales?
 - Où les mettre en place et par qui?
 - Comment les réaliser techniquement?

PARTIE III – LES RELATIONS INTER-FAI

RELATION COMMERCIALE OU PEERING? (I)

○ Relation Commerciale

- Service de connectivité payant
 - 1 Fournisseur
 - 1 Client
- Le fournisseur
 - se charge du trafic sortant/reentrant du client
 - facture le service au client
- Quid de la facturation?
 - Forfait?
 - Décompte?
 - Débit entrant et/ou sortant?
- Le client revend généralement ce service à ses propres clients

PARTIE III – LES RELATIONS INTER-FAI

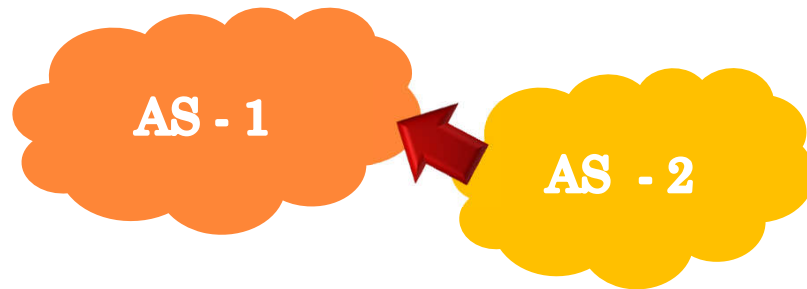
RELATION COMMERCIALE OU PEERING? (II)

○ Peering

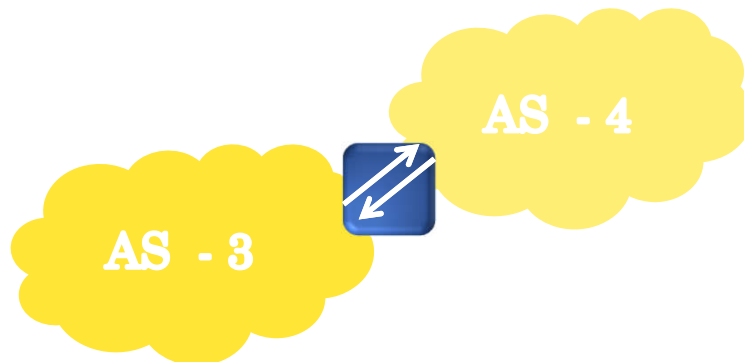
- Relation « d'égal à égal » pour un bénéfice mutuel
 - Achemine une part de trafic de l'autre
 - Dans un degré équivalent
 - Equilibre
- Gestion de l'équilibre?
 - Dépendance du niveau de peering
 - Accords souvent contraignants pour garantir l'équité de l'échange
 - Le peering n'est pas du TRANSIT!

PARTIE III – LES RELATIONS INTER-FAI

RELATION COMMERCIALE OU PEERING? (III)



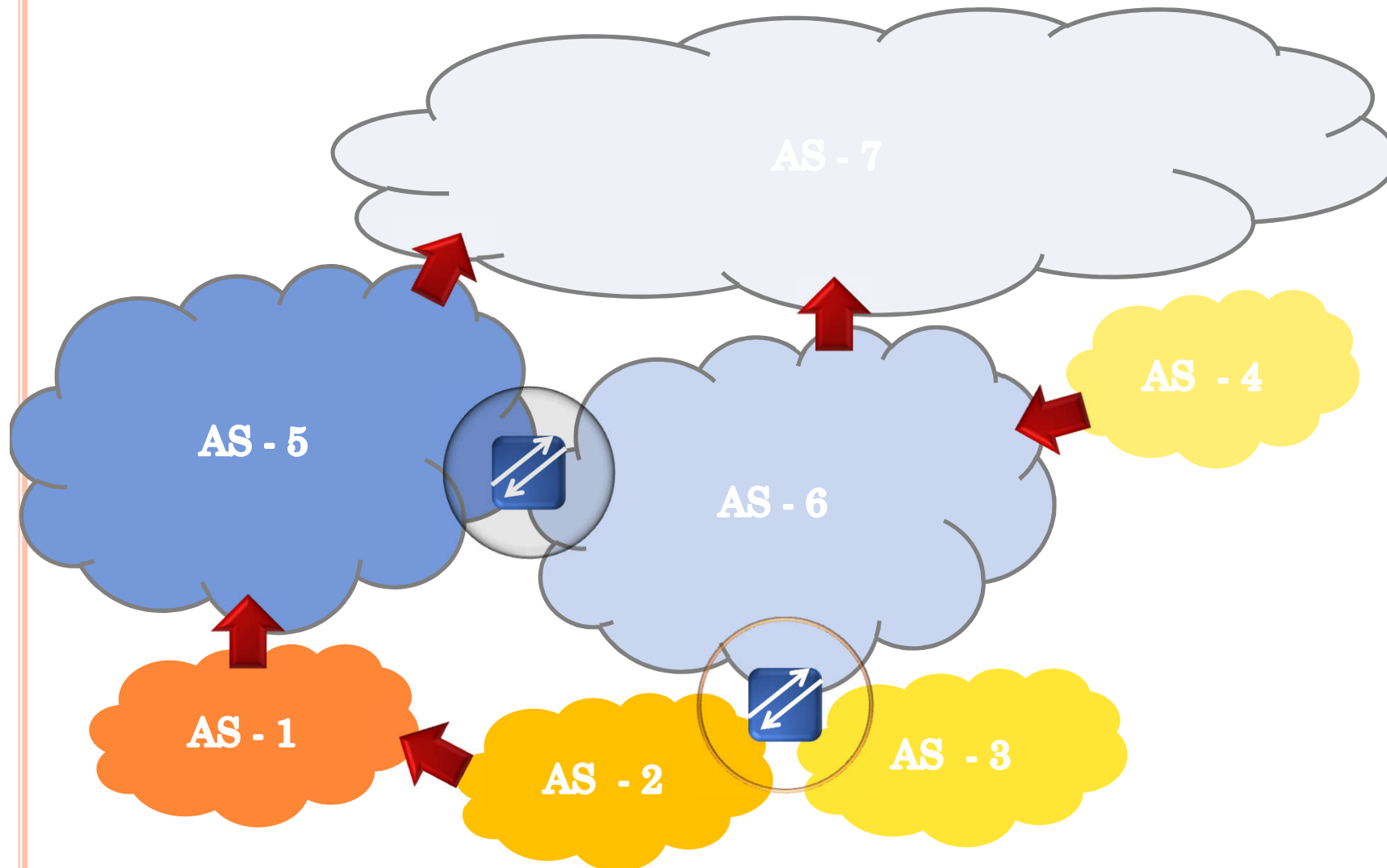
- AS – 1 = FAI de l'AS – 2
- Types d'AS :
 - AS – 1 = AS de transit
 - AS – 2 = AS stub
- Informations échangées entre les AS
 - Ensemble des réseaux de AS-2 (R2)
 - R1 à AS2
 - Ensembles des réseaux accessibles par AS-1 ou par défaut?



- AS – 3 peering avec AS – 4
- Types d'AS :
 - AS – 3 = AS stub
 - AS – 4 = AS stub
- Informations échangées entre les AS
 - R3
 - R4

PARTIE III – LES RELATIONS INTER-FAI

DIFFÉRENTS TYPES DE PEERING



PARTIE III – LES RELATIONS INTER-FAI

OÙ ET QUI? (I)

○ Le besoin

- Lieu de co-localisation entre les deux entités
 - Lieu physique
 - Lien
 - Entité tiers d'interconnexion
- Réalité à tous les niveaux
 - Entre un client et son FAI
 - Entre deux pairs

○ Problèmes:

- Les coûts?
 - Location/achat du lieu, des câbles, du matériel
 - Mise en œuvre
 - Supervision et maintenance
- Mise en place et contrôle de l'accord?

PARTIE III – LES RELATIONS INTER-FAI

OÙ ET QUI? (II)

○ Les relations commerciales

- En fonction de la relation commerciale
- Généralement
 - Le client est en charge d'acheminer son trafic jusqu'à un ou plusieurs Point of Presence (POP ou NAP) de son FAI
 - Le FAI est en charge du POP
 - Équipements
 - Configuration, supervision et maintenance
 - Mais il peut le sous-traiter
- Où
 - Notion de Carrier Hotel ou de Colocation Center (> 5000m²)
 - Mutualisation des moyens
 - Proposition de services pour
 - Les FAI et les fournisseurs de services (Web et Stockage)



PARTIE III – LES RELATIONS INTER-FAI

OÙ ET QUI? (III)

○ Le peering

- Point de rencontre des AS
- (Global) Internet eXchange Point (IX ou IXP ou GIX)
 - Entité propre à l'IX avec contribution des principales entités créatrices
 - L'IX est le lieu de peering mais les accords sont traités entre les différents pairs
 - L'IX peut aussi être le lieu
 - De DNS (racine)
 - De POP FAI
 - De services différents (NTP, web, sécurité, VLAN, VPN, multicast...)
- Où
 - Un IX peut être réparti sur plusieurs sites
 - Exemple PARIX, LYONIX, TOUIX, SFINX, REUNIX

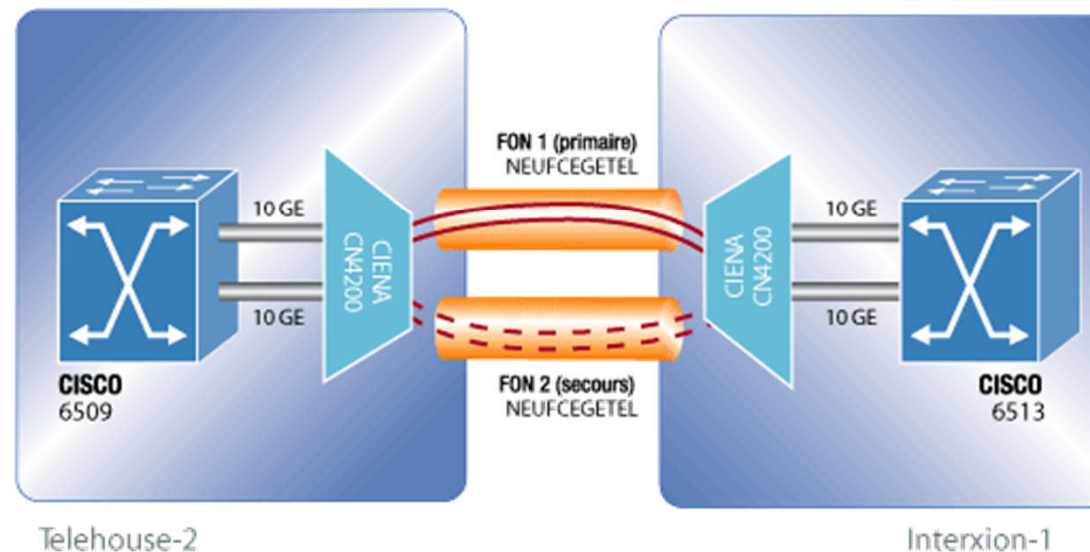
PARTIE III – LES RELATIONS INTER-FAI

OÙ ET QUI? (IV)

- Un exemple d'IX : LyonIX
 - LyonIX c'est à la fois
 - Un GIX
 - Un NAP pour s'interconnecter à des AS de transit
 - Plus de 30 entités dont Level 3 (tier 1) ou CCC-Lyon (palais des congrès)
 - Localisation
 - Deux sites Lyon Nord (campus la Doua) et Lyon Sud (Vénitieux)
 - GigaEthernet
 - Services et avantages
 - Interconnexion de LAN
 - Augmentation des débits
 - Réduction de l'utilisation des accès Internet entre les membres
 - Diminution du délai

PARTIE III – LES RELATIONS INTER-FAI *OÙ ET QUI? (V)*

- Un autre Exemple SFINX – RENATER
 - Redondance
 - Interconnexion entre site haut-débit
 - Interfaces FAI FastEthernet, GigaEthernet ou 10 GigaEthernet



PARTIE III – LES RELATIONS INTER-FAI

LES ACCORDS DE PEERING

- Accord au cas par cas
 - Dépendance des gestionnaires de l'AS
 - De la taille de l'AS
- Communément
 - Pas de Peering avec un AS dont on est le client
 - Le Peering
 - Échange des routes internes des deux AS
 - Pas d'échange des routes d'autres AS avec qui on est en peering
 - Quid des AS dont on est le FAI?
 - Un débit entrant et sortant vers les AS en peering à garantir
 - Ne pas saturer le lien
 - Mais ne pas le sous-utiliser

PARTIE III – LES RELATIONS INTER-FAI

COMMENT GARANTIR?

- Protocole d'échange de route avec politique
 - BGP
- Utilisation de la supervision et de la métrologie
 - Contrôle et maintenance
 - Accords papiers

PARTIE III – LES RELATIONS INTER-FAI

BILAN

- Apports du peering
 - Une plus grande souplesse dans les relations inter-FAI
 - Fin du Tu me paies et Je te paies
 - Economie
 - Mutualisation des moyens
 - Economie de la ressource FAI pour les échanges locaux
 - Opportunité pour les fournisseurs de services de tout type
 - Opportunité pour les pays en voie de développement où la bande passante extérieure est chère
 - Mais
 - Accords peuvent être complexes
 - Rend la topologie d'Internet un peu complexe encore

PARTIE III – LES RELATIONS INTER-FAI

EXEMPLES DES RELATIONS D'UN AS (I)

- Sources :

- <http://www.robtex.com/as>

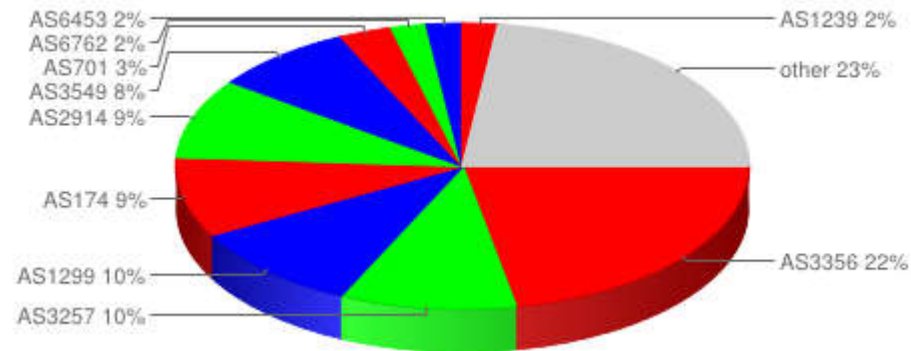
- <http://as-rank.caida.org/>

- AS 5511 Opentransit de FT

Mise à jour du 23/08/2012

Peering Exchange Points (AS 5511)

PARIX	198.32.247.12
LINX Juniper LAN	195.66.224.83
NOTA	198.32.124.67
Equinix Singapore	202.79.197.5



PARTIE III – LES RELATIONS INTER-FAI

EXEMPLES DES RELATIONS D'UN AS (II)

AS 5511 (eTel Austria Gesmbh u. CO KG)

country: US

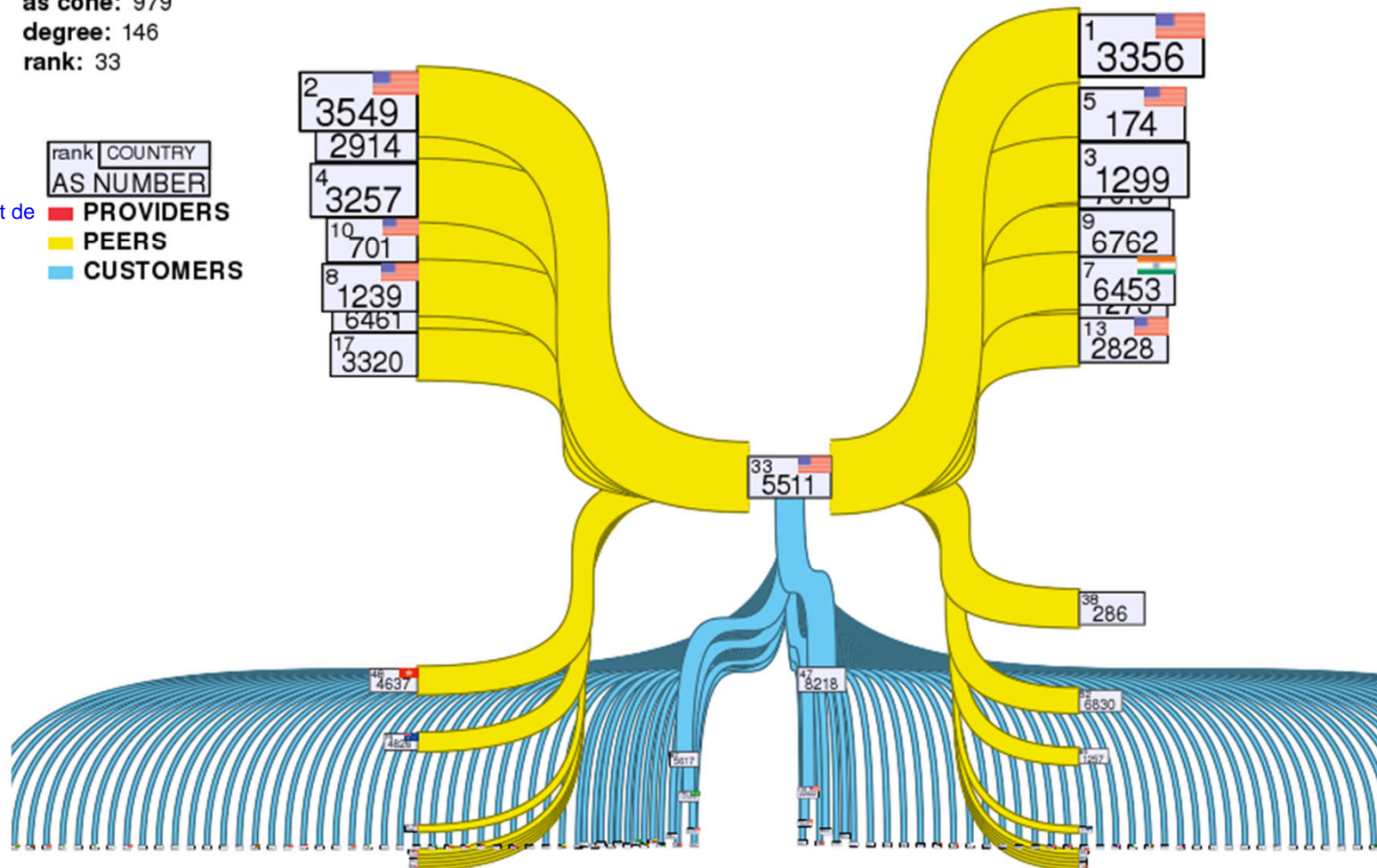
as cone: 979

degree: 146

rank: 33

Client de

rank	COUNTRY
AS NUMBER	
PROVIDERS	
PEERS	
CUSTOMERS	



PARTIE III – LES RELATIONS INTER-FAI

EXEMPLES DES RELATIONS D'UN AS (III)

○ AS 3215 Orange France

Mise à jour du 23/08/2012

Peering Exchange Points (AS 5511)

PARIX 198.32.247.1

AS 3215 (eTel Austria Gesmbh u. CO KG)

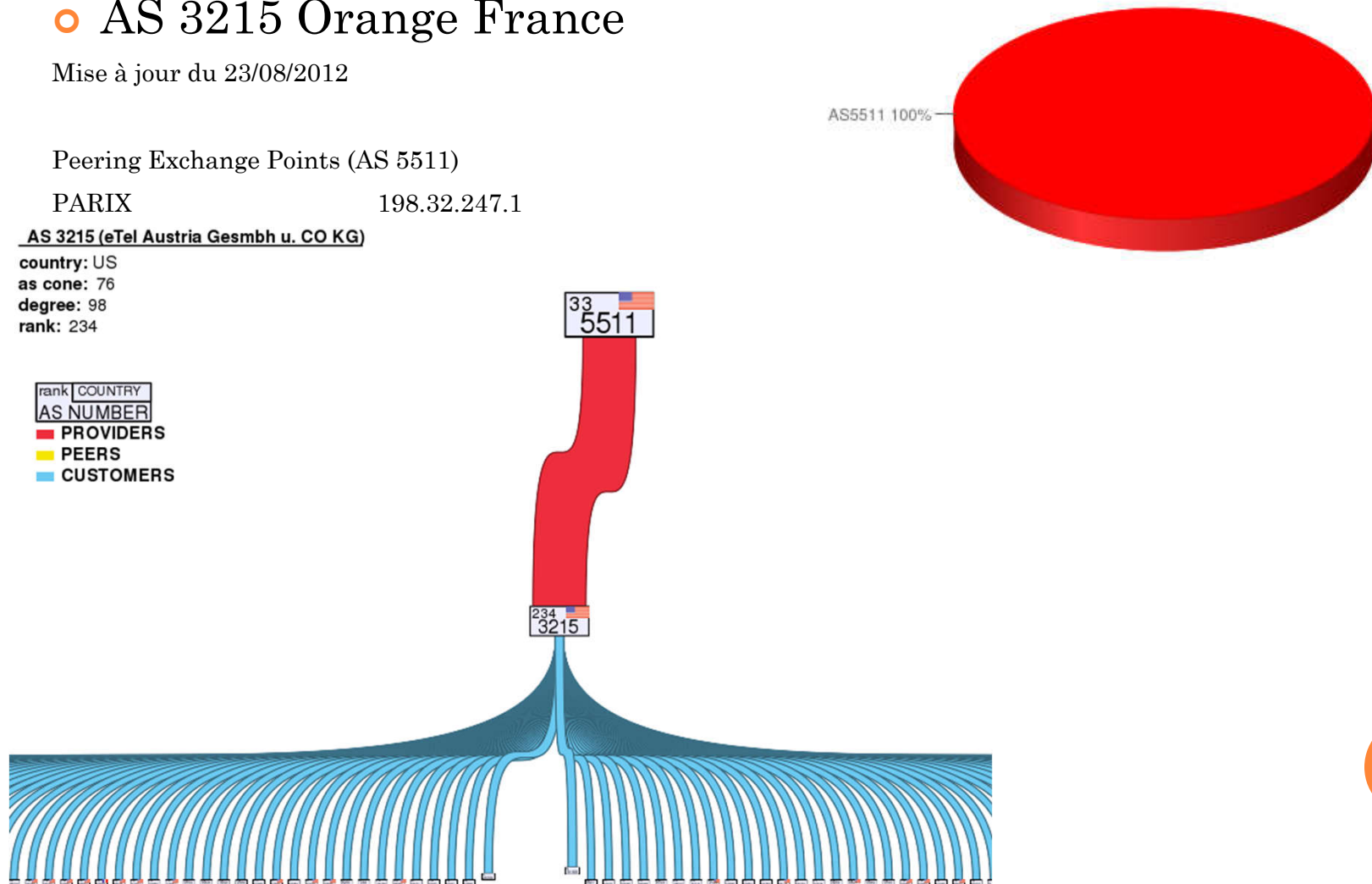
country: US

as cone: 76

degree: 98

rank: 234

rank	COUNTRY
AS NUMBER	
PROVIDERS	
PEERS	
CUSTOMERS	



PARTIE III – LES RELATIONS INTER-FAI

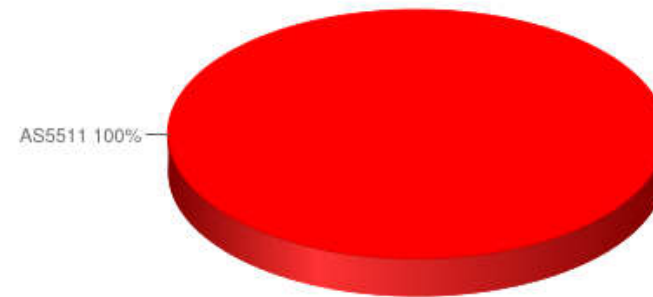
EXEMPLES DES RELATIONS D'UN AS (IV)

○ AS 12322 PROXAD (FREE)

Mise à jour du 23/08/2012

Peering Exchange Points (AS 12322)

FreeIX	213.228.3.225
AMS-IX1	195.69.144.251
LINX Juniper	195.66.224.191
DE-CIX	80.81.192.223
Equinix Ashburn	206.223.115.160
NOTA	198.32.124.192
Equinix Palo Alto	198.32.176.197
Equinix New York	198.32.118.197



AS 12322 (PROXAD)

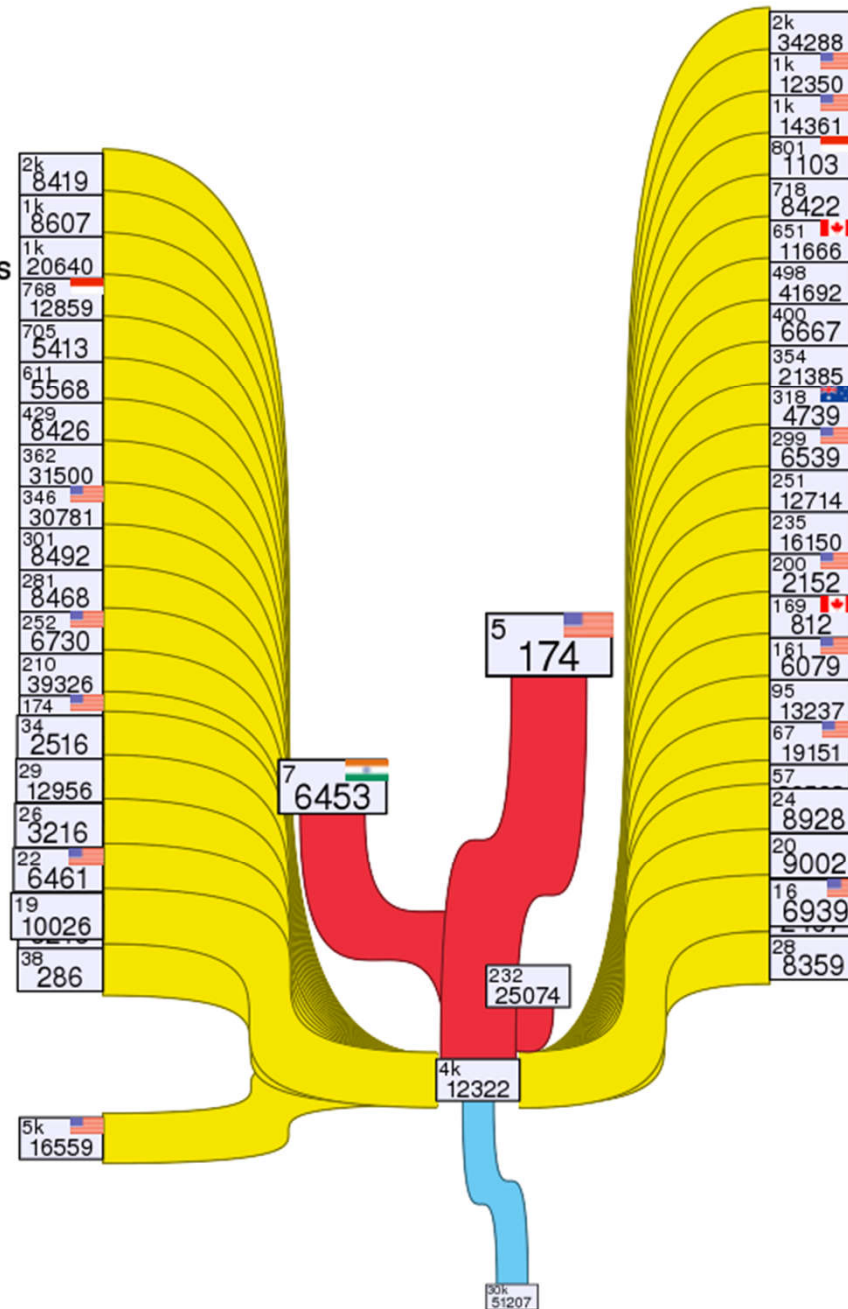
country:

as cone: 2

degree: 56

rank: 4355

rank COUNTRY
AS NUMBER
PROVIDERS
PEERS
CUSTOMERS



AS 3356 (Level 3 Communications, Inc.)

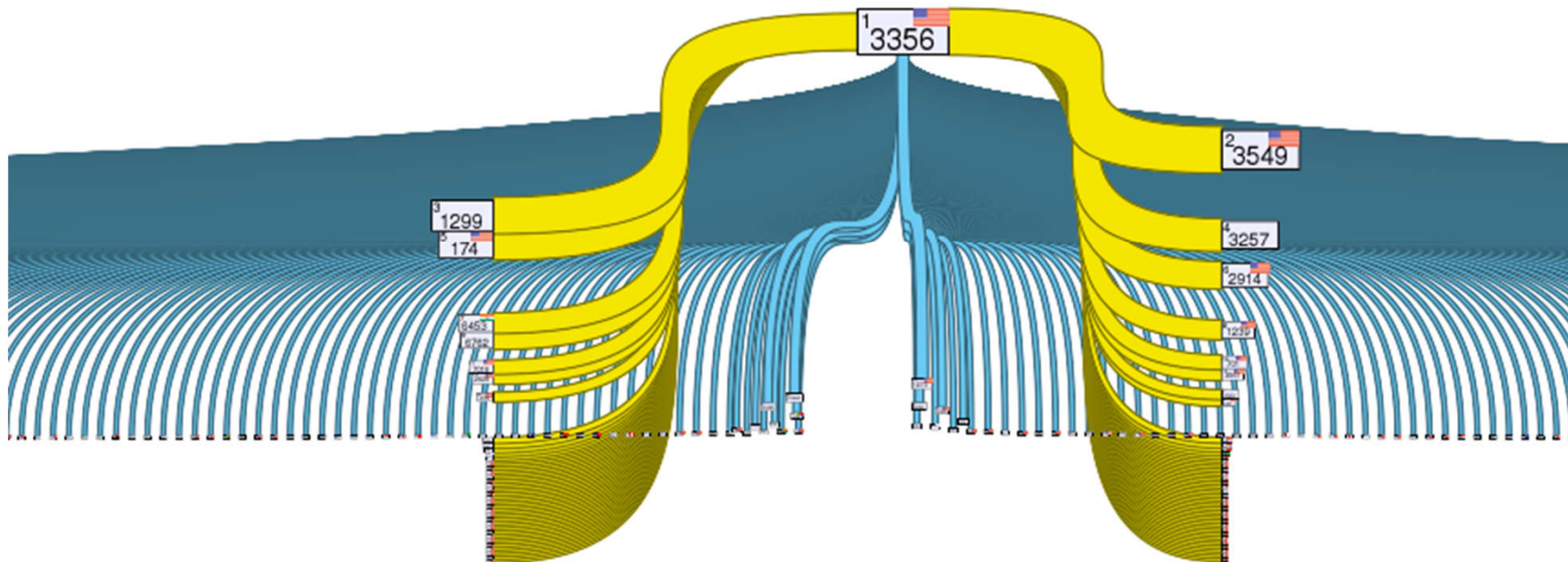
country: US

as cone: 24632

degree: 3331

rank: 1

rank	COUNTRY
AS NUMBER	
PROVIDERS	
PEERS	
CUSTOMERS	



AS 15169 (Google Fiber Inc.)

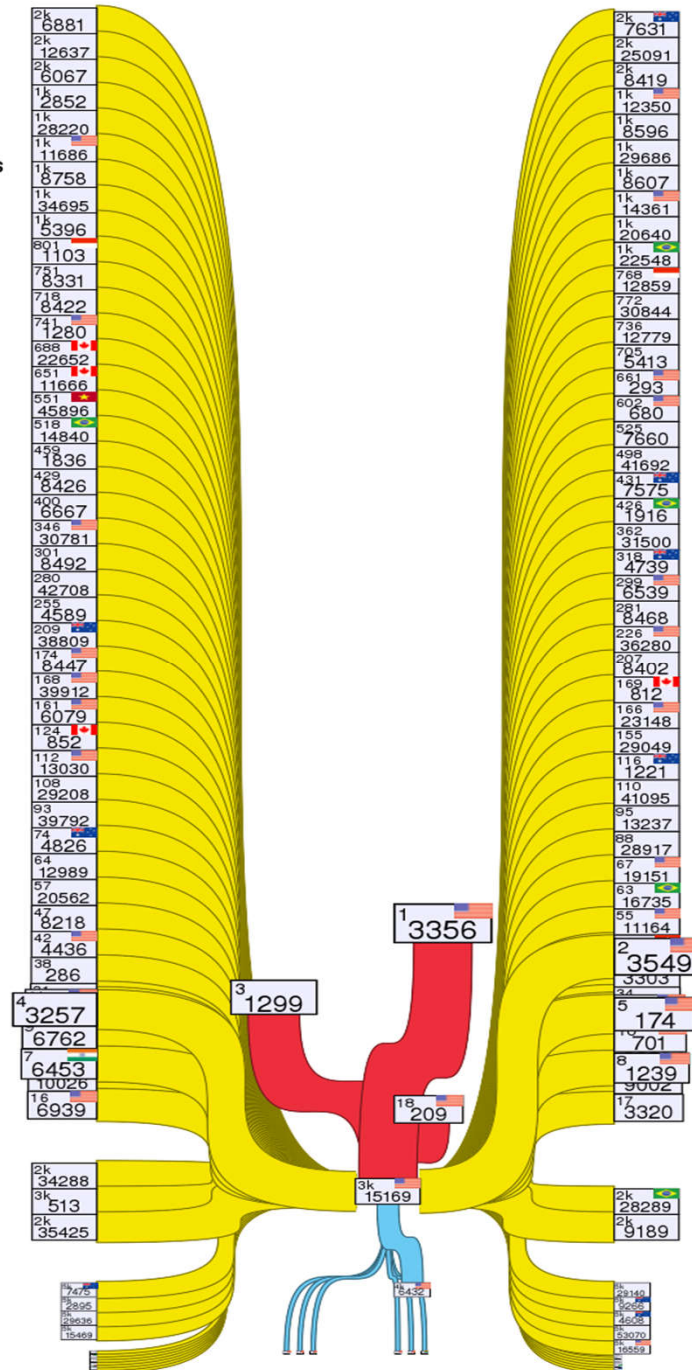
country: US

as cone: 3

degree: 134

rank: 3159

rank COUNTRY
AS NUMBER
PROVIDERS
PEERS
CUSTOMERS



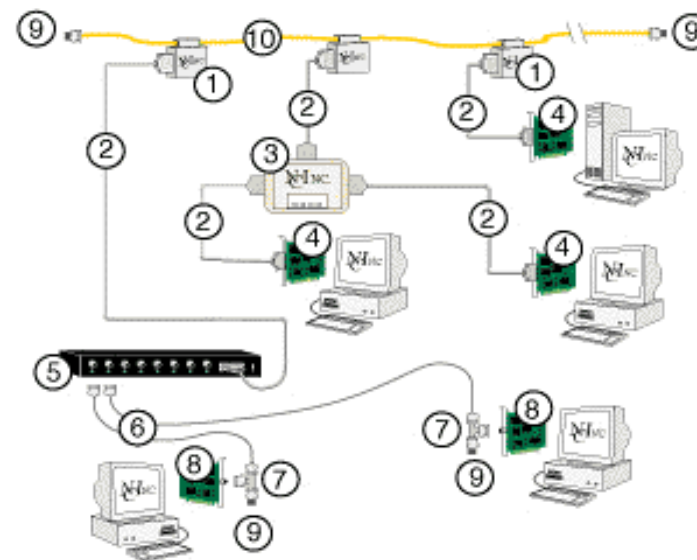
CONCLUSION

- Internet = problème d'interconnexion
 - Interconnexion du client final avec son FAI
 - Diversité des réseaux d'accès
 - Utilisation de sur-couches protocolaires comme PPP
 - Interconnexion des réseaux via une même entité administrative
 - Souvent un FAI
 - Notion d'AS
 - Utilisation d'outil et d'un protocole de routage
 - Interconnexion entre les FAIs/AS
 - Payer pour transiter
 - Echanger selon un accord (peering)

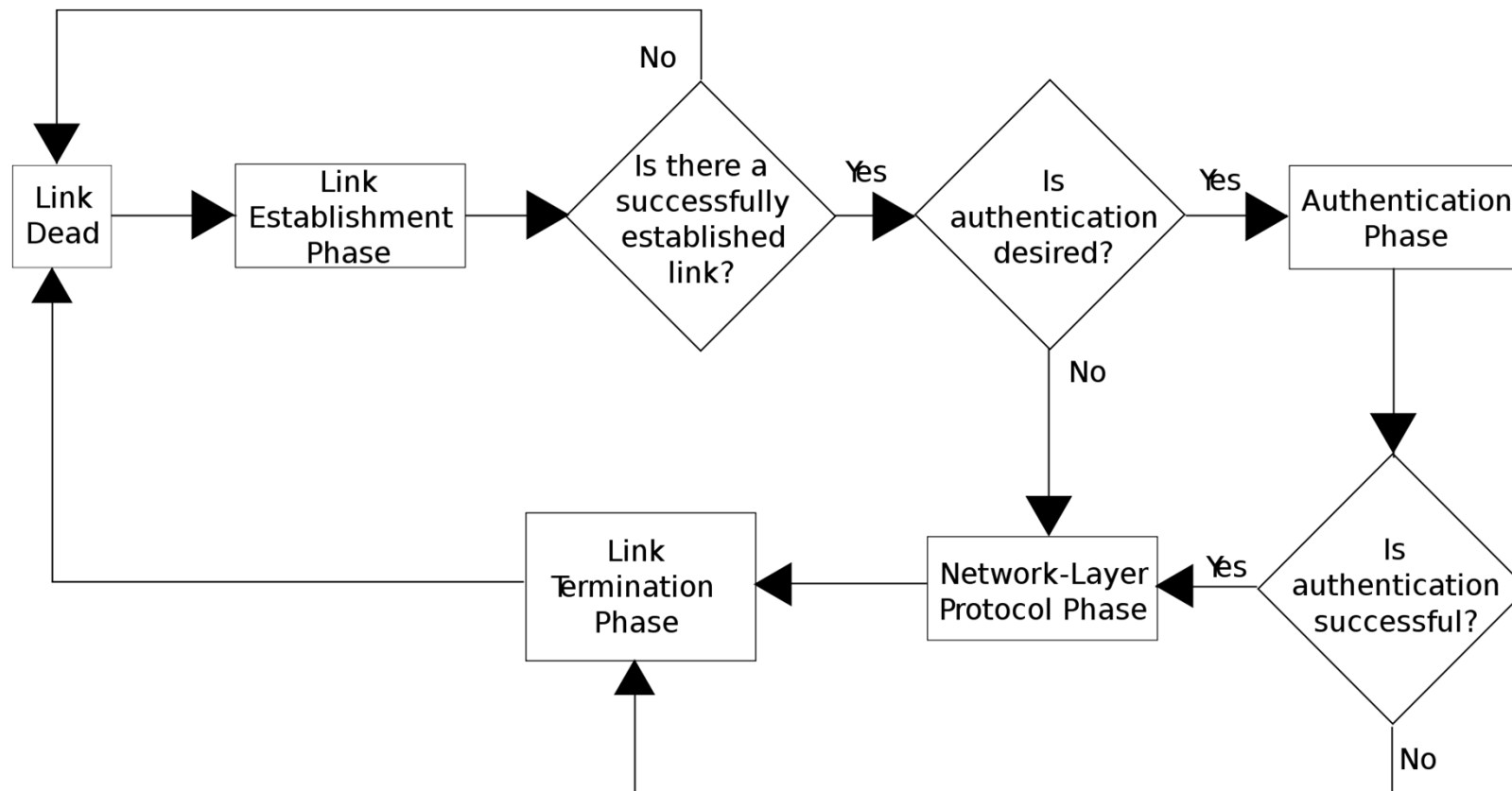
ANNEXE I – ILLUSTRATION THICK ETHERNET



10 BASE 5



ANNEXE II – PPP



ANNEXE III – EXEMPLE DE CARRIER HOTEL

CI HOST - 3550 WILSHIRE BLVD., LOS ANGELES, CA 90010



- Diesel-powered generators
- Multiple POEs (Point of Entry) for fiber, electricity and generator inputs with n+3 redundancy
- Capacity Planning - No fiber optic link will ever peak at more than 33% of its capacity. The capacity-load-ratio of C I Host's network connectivity has always been at least 3:1
- 100Mbps connections to C I Host's routers and switches from your server. 1000Mbps (GigE) connections from our routers and switches to the Internet fiber connectivity
- Instant growth and scalability - we scale and grow as your business demands it - upgrades take less than 1 hour
- 24/7 Armed Guards
- 24/7 Secured access with key swipe entry, biometric thumb print verifier and a double-locking man-trap at every door within the datacenter and on exterior
- 24/7 on-site maintenance staff with spare parts for all server configurations
- Multiple DS-3, OC-3 and OC-12 fiber optic connections to multiple, redundant carriers - Internet connectivity NEVER goes down
- Security system with live monitored internal cameras
- Instant on dry-pipe fire protection systems
- 19" and 23" seismically braced racks
- Category 5 & Category 6 Cable
- Full daily client-content backups and hourly system backups ensure no data loss to any housed server.



INTERNET AVANCÉ II

LES CHEMINS D'INTERNET

58

2A Apprentissage Info&Réseaux

Julien Fasson – julien.fasson@enseeiht.fr

Remerciements à Emmanuel Chaput

PRÉSENTATION DU SUJET

○ Précédemment

- Internet = ensemble d'ensemble de réseaux
 - Interconnexion du client => réseau d'accès
 - Interconnexion de réseaux au sein d'un AS
 - Etablissement des routes?
 - Interconnexion entre AS
 - Peering & Relation commerciale
 - Echanges de routes?

○ Etablissement des chemins

- Plusieurs solutions
 - Différents besoins
 - Différentes méthodes
- Protocoles
 - Apprentissage de la topologie
 - Calcul d'une table de routage

PLAN

- Partie 1 – Généralités
 - Routage, principes et objectifs
 - La notion de table de routage
 - *Définition*
 - *Mise à jour*
 - Protocoles dynamiques
 - *Différents types*
 - *Principales étapes*
- Partie 2 – Routage Intra-FAI
 - Configuration des machines d'extrémité
 - Routing Information Protocol
 - Open Shortest Path First
- Partie 3 – Routage inter-FAI
 - Border Gateway Protocol

PARTIE I – GÉNÉRALITÉS

ROUTAGE, PRINCIPES...

- Recherche d'un chemin (une route)
 - Besoin d'une connaissance minimale du réseau
 - Application d'un algorithme (théorie des graphes)
 - Contraintes éventuelles pour changer le poids des différentes routes
- Permettant d'acheminer les données au sein d'un réseau
 - Quelle qu'en soit la structure
- Associé à la commutation des données
 - Pas de commutation sans routage

PARTIE I – GÉNÉRALITÉS

... *ET OBJECTIFS*

- Choix d'un chemin optimal : notion de critères
 - Fiabilité
 - Économie
 - Bande passante
- Adaptation à la dynamique du réseau
 - Reconfiguration
 - Charge (rejoint critères)
 - Pannes
 - Mobilité
- Implantation réaliste Algo doit pas être trop lourd
 - Traitement algorithmique
 - Charge de communication

PARTIE I – GÉNÉRALITÉS

LA NOTION DE TABLE DE ROUTAGE (I)

○ Route

- Adresse destination avec son masque
- Interface IP vers laquelle aiguiller le datagramme
- Adresse du prochain routeur si nécessaire

○ Table de routage

- Ensemble de routes

Destination	Passerelle	Genmask	Indic	Metric	Iface
147.127.80.0	0.0.0.0	255.255.240.0	U	1	eth0
0.0.0.0	147.127.80.200	0.0.0.0	UG	0	eth0

PARTIE I – GÉNÉRALITÉS

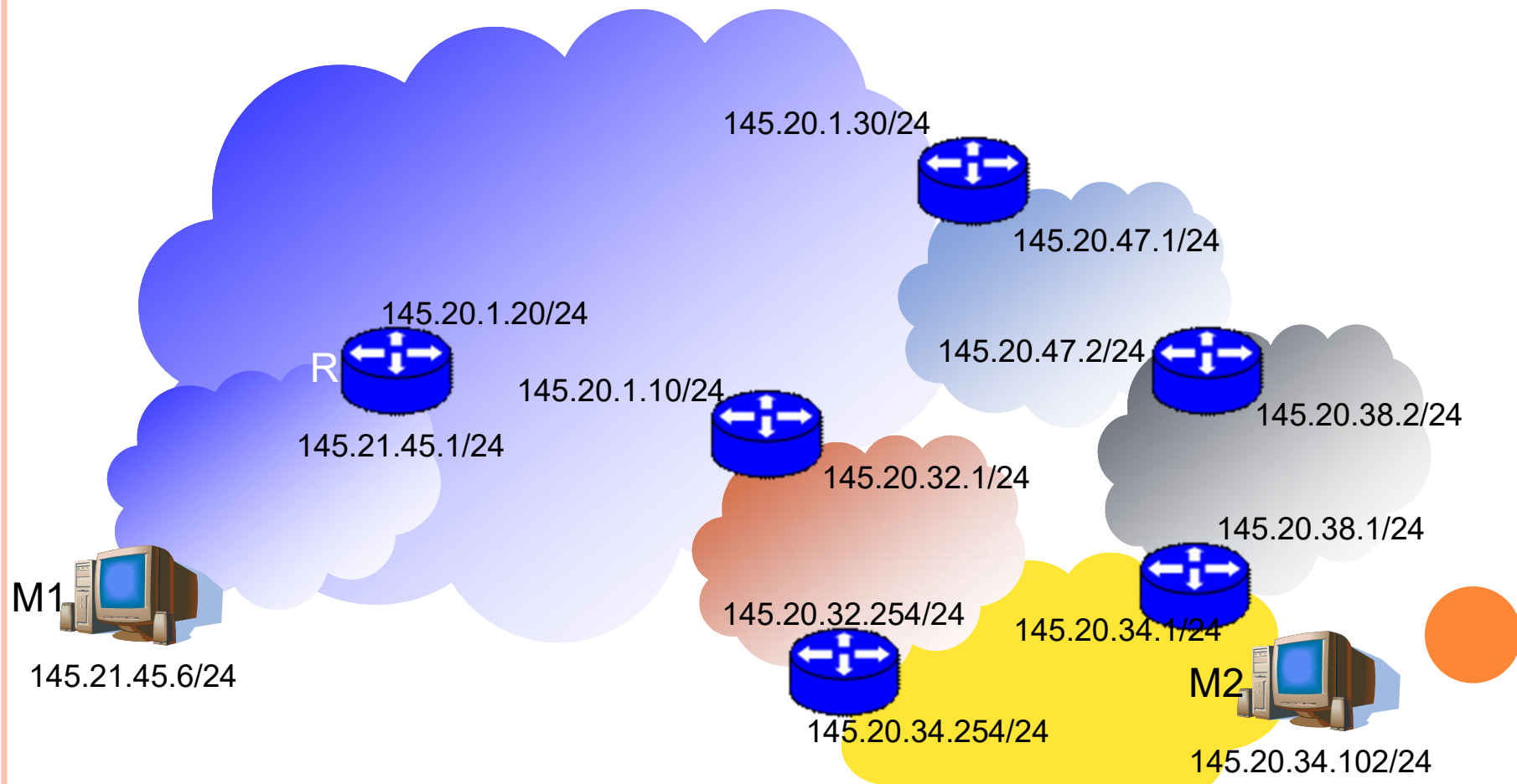
LA NOTION DE TABLE DE ROUTAGE (II)

- Mise à jour
 - Quand?
 - Configuration d'une interface
 - Ajout manuel
 - Ajout automatique (configuration dynamique)
 - Pourquoi?
 - Changement de topologie
 - Pannes
 - Taille du réseau
 - Traitement différents
 - Machines d'extrémité
 - Routeurs

PARTIE I – GÉNÉRALITÉS

REEMPLISSAGE MANUEL D'UNE TABLE DE ROUTAGE

- Donner la table de routage de R et de M1 et M2



PARTIE I – GÉNÉRALITÉS

REPLISSAGE MANUEL D'UNE TABLE DE ROUTAGE

○ M1

Destination	Passerelle	Genmask	Indic	Metric	Iface
145.21.45.0	0.0.0.0	255.255.255.0	U	1	eth0
0.0.0.0	145.21.45.1	0.0.0.0	UG	0	eth0

○ M2

Destination	Passerelle	Genmask	Indic	Metric	Iface
145.20.34.0	0.0.0.0	255.255.255.0	U	1	eth0
145.20.38.0	145.20.34.1	255.255.255.0	UG	2	eth0
145.20.47.0	145.20.34.1	255.255.255.0	UG	3	eth0
0.0.0.0	145.20.34.254	0.0.0.0	UG	0	eth0

○ R

Destination	Passerelle	Genmask	Indic	Metric	Iface
145.21.45.0	0.0.0.0	255.255.255.0	U	1	eth0
145.20.1.0	0.0.0.0	255.255.255.0	U	1	eth1
145.20.32.0	145.20.1.10	255.255.255.0	UG	2	eth1
145.20.47.0	145.20.1.30	255.255.255.0	UG	2	eth1
145.20.34.0	145.20.1.10	255.255.255.0	UG	3	eth1
145.20.38.0	145.20.1.30	255.255.255.0	UG	3	eth1

PARTIE I – GÉNÉRALITÉS

LES PROTOCOLES DYNAMIQUES (I)

- Différents types de protocoles
 - IGP = Interior Gateway Protocol
 - Routage au sein d'un AS
 - RIP, OSPF, EIGRP, IS-IS, . . .
 - EGP = Exterior Gateway Protocol
 - Routage entre plusieurs AS
 - BGP-4
- Pour différents besoins
 - Réseaux nombreux et variés
 - En taille et en besoins
 - AS
 - Routage interne et routage externe
 - Différents types d'AS
 - Relations économiques complexes
 - Natures très différentes

PARTIE I – GÉNÉRALITÉS

LES PROTOCOLES DYNAMIQUES (II)

- Principales étapes
 - Collecte d'information
 - Calcul des routes
 - Utilisation des routes
 - Commutation d'IP
- Collecte d'information
 - Administration manuelle (fastidieux)
 - Protocole
 - À vecteur de distances
 - Algorithme Bellman Ford
 - À états des liaisons
 - Algorithme de Dijkstra

PARTIE I – GÉNÉRALITÉS

LES PROTOCOLES DYNAMIQUES (III)

- Calcul des routes
 - Centralisé
 - Décentralisé
 - Distribué chacun contrôle un morceau
- Utilisation
 - Commutation IP après consultation de la table
 - Plusieurs chemins?
 - Critères
 - TOS / QoS
 - Coût de la route
 - Partage de charges

PARTIE II – ROUTAGE INTRA-FAI

CONFIGURATION DES MACHINES D'EXTRÉMITÉS

○ ICMP

- Router Advertisement ==> Route par défaut
- Redirect ==> Correction d'une route

○ On y préfère

- DHCP
- PPP avec sa partie IPCP

PARTIE II – ROUTAGE INTRA-FAI

RIP - PLAN

- Routing Information Protocol
 - Principes
 - Format des messages
 - Problèmes

PARTIE II – ROUTAGE INTRA-FAI

RIP – PRINCIPE (I)

- Routing Information Protocol
 - IGP à vecteur de distances
 - Information de base : distance à une destination
 - Meilleure route = plus courte
 - Distance exprimée en “sauts” (hops)
 - Protocole applicatif
 - Implanté sur UDP, port 520
 - Messages courts
 - Recherche d'efficacité
 - Décrit dans
 - RFC 1058 en 1988
 - RFC 1388 en 1993
 - Ajout du support des masques
 - Ajout de l'authentification des routeurs

PARTIE II – ROUTAGE INTRA-FAI

RIP – PRINCIPE (II)

- Garder une base de donnée avec une entrée pour chaque entité du système
 - Adresse IP destination
 - Distance en nombre de hop
 - Utilisation de timers
- Émission périodique d'un extrait de la base de donnée
 - Chacune des interfaces
 - TTL 0 Time to leave

PARTIE II – ROUTAGE INTRA-FAI

RIP – PRINCIPE (III)

- A l'initialisation

- Chaque routeur connaît ses voisins immédiats
 - Interface IP
 - Distance de 0

On connaît toutes les interfaces de la machine

- Découverte du réseau par envoi périodique d'extraits de sa base de donnée

Tous les routeurs (qui font du RIP) vont envoyer périodiquement ce qu'ils connaissent du réseau

PARTIE II – ROUTAGE INTRA-FAI

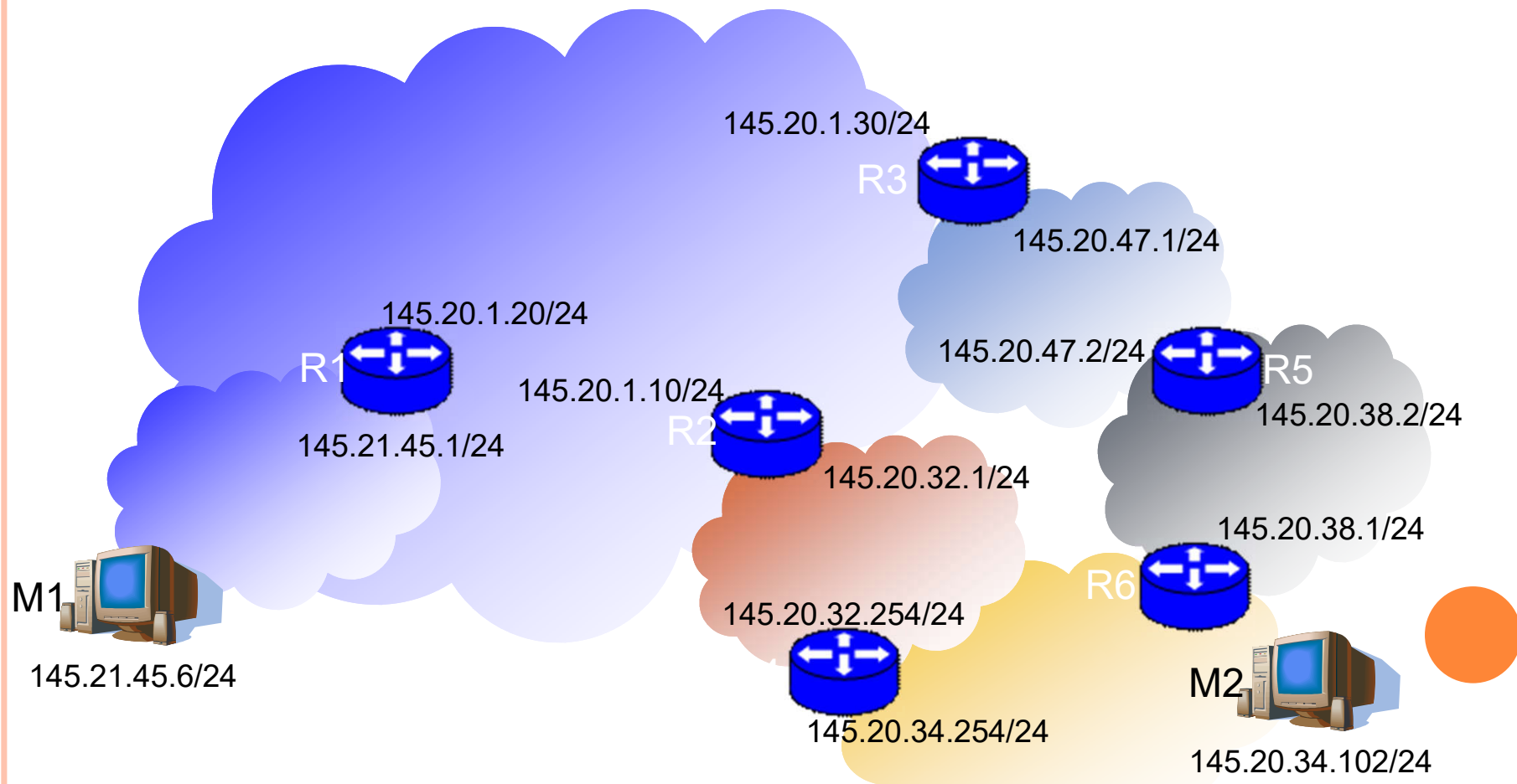
RIP – PRINCIPE (IV)

- Lors de la réception d'une route, comparaison avec les entrées de la base de donnée
 - si destination inconnue et la métrique reçue n'est pas infinie alors
 - ajout de la route avec
 - Gateway = émetteur
 - Métrique = métrique +1
 - sinon si nouvelle route meilleure alors
 - remplacement de la route
 - sinon si même chemin (mise à jour)
 - route modifiée
 - sinon
 - rien

PARTIE II – ROUTAGE INTRA-FAI

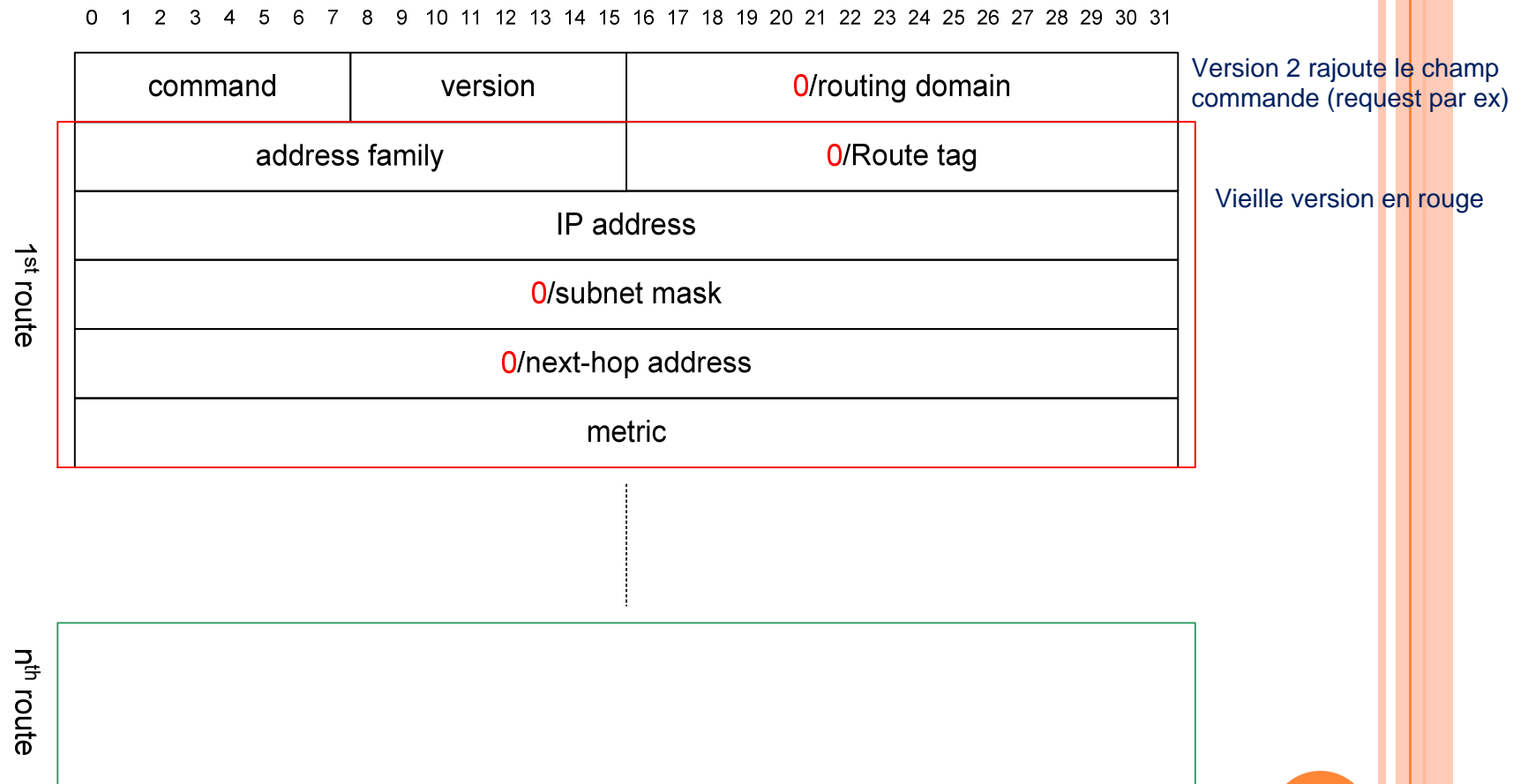
MISE EN ŒUVRE DE RIP

- Appliquer RIP sur cet exemple



PARTIE II – ROUTAGE INTRA-FAI

RIP – FORMAT DES MESSAGES (I)



Longueur max = 512 B
De 1 à 25 routes

PARTIE II – ROUTAGE INTRA-FAI

RIP – FORMAT DES MESSAGES (II)

○ En-tête

- 1 mot
- Command
 - 1 – Demande
 - Partielle en précisant l'adresse (metric = 16)
 - Complète (address family = 0 + metric = 16)
 - 2 – Réponse
 - Suite à la réception d'un message 1
 - Périodique
 - Spontané (changement de topologie)
- Version
 - RIP 1 ou RIP 2
- Routing domain
 - 0 par défaut
 - Appartenance possible à plusieurs domaines d'un routeur

PARTIE II – ROUTAGE INTRA-FAI

RIP – FORMAT DES MESSAGES (III)

- Address family
 - Format d'adressage (2 = IP)
- Route tag
 - Informations pour routage inter-domaine (EGP)
- IP address
 - L'adresse de destination (réseau, sous-réseau ou host)
 - En fonction de subnet mask
- HostID
 - Adresse IP du routeur de la route
 - Pas forcément l'émetteur

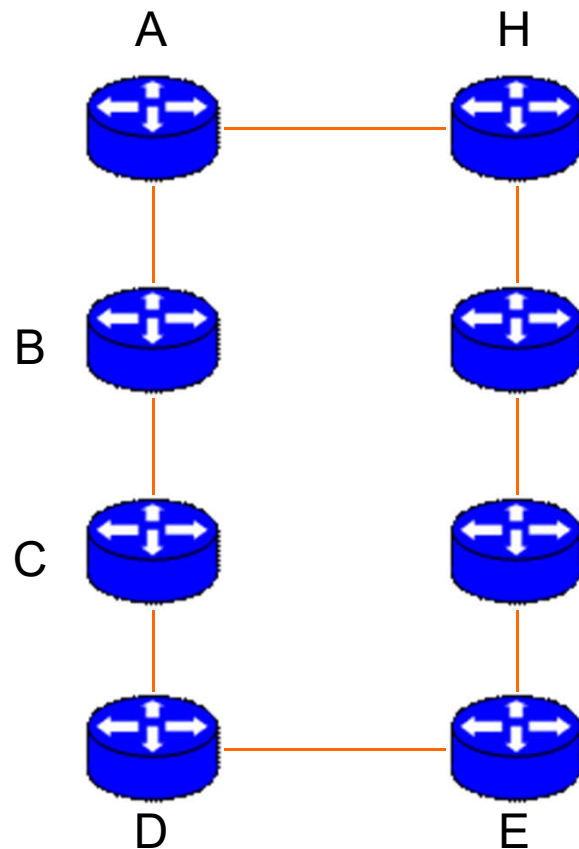
PARTIE II – ROUTAGE INTRA-FAI

RIP – PROBLÈMES (I)

- Protocole basé sur une topologie fixe
 - Pour s'adapter aux changements...
 - ... il faudrait déjà détecter le changement!
- Protocole simple
 - Problèmes semblables à **Spanning Tree**
 - Boucles infinies distances infinies
 - Distances infinies
 - Fiabilité?
 - Sécurité?
 - Détection de messages corrompus
 - Détection de pannes de routeurs

PARTIE II – ROUTAGE INTRA-FAI

ANALYSE DES PROBLÈMES DE RIP (I)

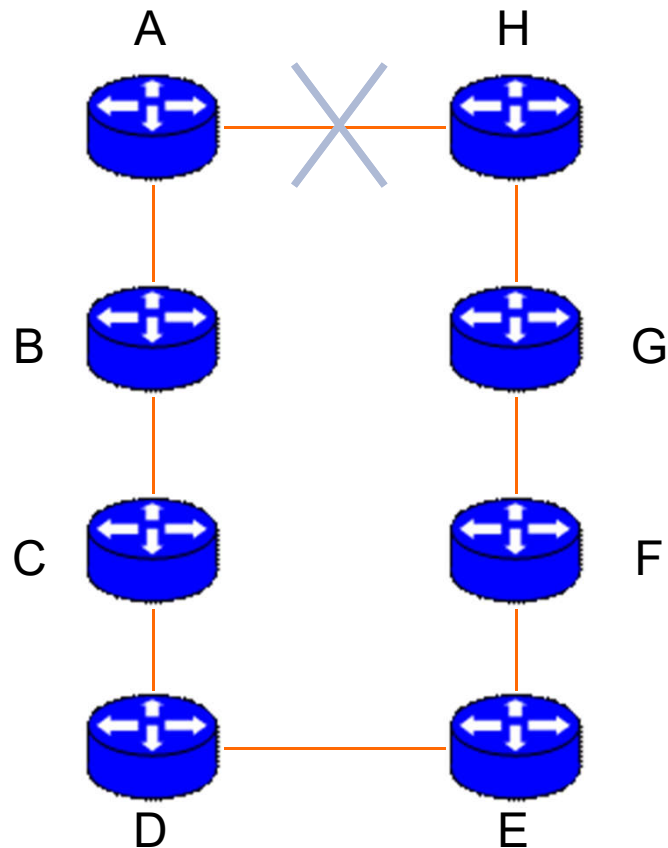


Hypothèses : pour des raisons de simplicité, on va établir la table de routage pour aller aux routeurs (et non aux réseaux)

Q1: Etablir la table de routage de chacun des routeurs

PARTIE II – ROUTAGE INTRA-FAI

ANALYSE DES PROBLÈMES DE RIP(II)



Le lien reliant A à H tombe.

Q2: Que devient la table de routage de H lorsqu'elle s'en rend compte?

Supposant qu'à ce moment G diffuse périodiquement sa table de routage.

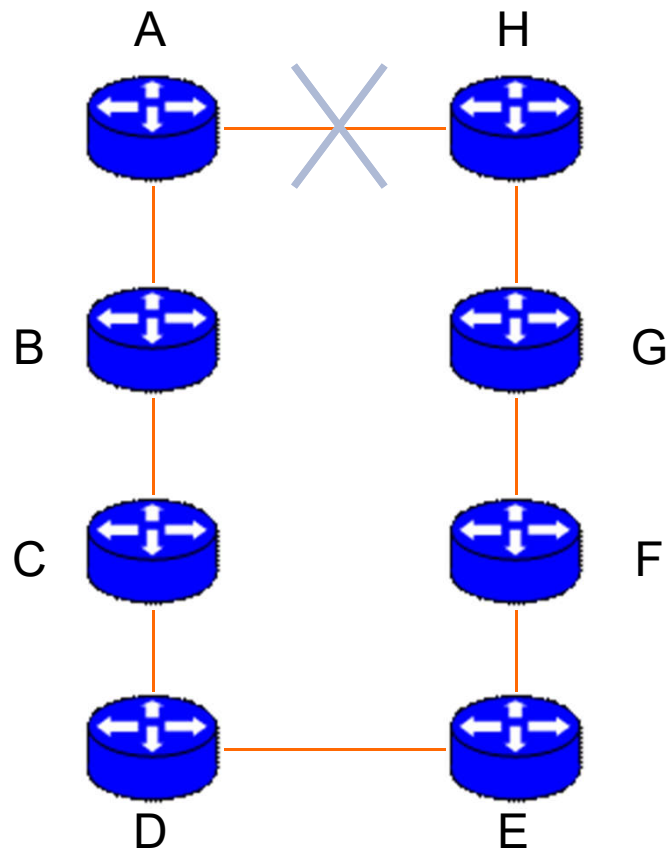
Q3: Que devient alors la table de routage de H?

Q4: Que devient alors un datagramme partant de F et allant vers A?

Q5: D'où vient alors le problème? Proposer une solution (ou plusieurs) pouvant le résoudre.

PARTIE II – ROUTAGE INTRA-FAI

ANALYSE DES PROBLÈMES DE RIP(II)



H envoie alors sa table de routage

Q6: Quel est l'impact de cette mise à jour dans le réseau? Expliquer les différentes mise à jour et messages échangés.

Q7: Quand est-ce que l'erreur sera résolue?

Q8: Que se passe-t'il entre G et H pendant ce temps?

Q9: Proposer une solution (ou plusieurs) pouvant résoudre ce problème.

PARTIE II – ROUTAGE INTRA-FAI

RIP – SOLUTIONS (I)

○ Limiter l'infini

- Réduit la durée de comptage
- L'infini c'est 16!
- Inconvénient: Limite l'AS à 15 bonds

○ Split horizon

- Ne pas informer une station voisine des routes qui passent par elle
- Avantages
 - messages de routage différents en fonction des destinataires
 - Messages plus courts
- Mais ne résout que partiellement le problème du rebond dès que l'on a plus de 2 stations

○ Triggered update

- Diffusion immédiate d'une route suite à la détection de panne

PARTIE II – ROUTAGE INTRA-FAI

RIP – SOLUTIONS (II)

- Détection des stations inaccessibles
 - Route time-out
 - Entrées de la table de routage à durée bornée (3 mn)
- Figurer l'inaccessibilité
 - Entrée à l'infinie pour 4 périodes de maj (2 mn)
- Diffusion de l'inaccessibilité
 - Poison Reverse empêcher les autres d'apprendre les routes qu'on vient d'apprendre par eux
 - Ajout des routes inaccessibles au message de routage
 - Amélioration du Split Horizon
 - On envoie à une station voisine une route infinie pour chacune des routes où l'on passe par elle
 - Inconvénient = augmentation de la taille des messages

PARTIE II – ROUTAGE INTRA-FAI

OSPF - PLAN

- Généralités
- Principe
 - Découpage en zone
 - Types de routeur OSPF
 - Description de la topologie
- Principales étapes
- Messages et mécanismes
 - Type
 - Format

PARTIE II – ROUTAGE INTRA-FAI

OSPF – GÉNÉRALITÉS

- IGP à état de liaisons
 - Calcul distribué du plus court chemin dans un graphe
 - Application de l'algorithme de Dijkstra
- Prise en compte de gros AS
 - Par une hiérarchie
- Routage multi-critère, multi-route On peut choisir et rajouter des critères, capable d'avoir plusieurs routes pour le même truc
- Support des préfixes de longueur variable, du multicast, . . .
- Intègre des mécanismes d'authentification
- Défini dans
 - RFC 1131 en 1989
 - RFC 2328 & 2329 1998 (version 2)
- Implanté au dessus d'IP (surprise!)

PARTIE II – ROUTAGE INTRA-FAI

OSPF – PRINCIPE (I)

○ Les outils

- Le découpage en zone
 - Bonne définition des zones = bonne performance du système
 - Une réalité? Ou pas?
- Les bases de données
 - Topology Information Base (TIB)
 - Adjacencies database
 - Liste des routeurs voisins
 - Link-State database
 - Différents types de liens
 - Routing Information Base (RIB) & FIB
 - Extrait de la RIB pour le forwarding = table de routage
- Les mécanismes et unités protocolaires
 - Hello pour le voisinage
 - Database description Une première vision du réseau au tout début de la communication
 - Link State message Message pour dire l'état des liens que le routeur connaît

Liste des routeurs qu'on a en voisin

Liste des différents liens (réseaux)

-> donne la carte globale du réseau

PARTIE II – ROUTAGE INTRA-FAI

OSPF – PRINCIPE (II)

○ La notion de zone

- Découpage du réseau en différentes zones pour
 - Unifier certains réseaux et particulariser d'autres
 - Diviser pour mieux régner
 - Image précise par zone
 - Réduire les messages échangés
 - Économie
- Différents types de zone
 - La zone backbone – zone 0
 - Unique et obligatoire
 - Permet l'interconnexion entre les zones - fédératrice
 - Notion d'Area Border Router Routeur de bordure d'une zone, dans la zone 0
 - Stub area Route qui n'a pas besoin de route externe pour travailler
 - Pas de route extérieure à l'AS diffusée (route externe)
 - Différent Stub AS!
 - Zone Classique

PARTIE II – ROUTAGE INTRA-FAI

OSPF – PRINCIPE (III)

- Les types de routeurs OSPF
 - Internal Router
 - Mise en place du Shortest Path First pour la zone
 - Area Border Router
 - Routage inter-zone
 - Mise en place de SPF par zone
 - Résumé envoyé à l'autre zone
 - ... et ce même dans le cas des stubs areas!
 - Toujours dans la zone 0
 - AS boundary router
 - Routage entre AS
 - Récupère les routes externes à un AS
 - Backbone router
 - Routeurs de la zone 0
 - Pas forcément des ABR

PARTIE II – ROUTAGE INTRA-FAI

OSPF – PRINCIPE (IV)

- La description de la topologie
 - En fonction du type de lien
 - Router links
 - Liens (interfaces) d'un routeur
 - Type de routeur (interne, frontalier, . . .)
 - Network links
 - Liste des routeurs attachés
 - Annoncé par le DR du réseau
 - Summary links
 - Réseaux de l'AS
 - Routeurs de frontière de l'AS
 - External links
 - Destinations extérieures
- Description effectuée par les Link State Advertisements

PARTIE II – ROUTAGE INTRA-FAI

OSPF – PRINCIPE (V)

- La métrique
 - Par défaut fondée sur la bande passante des liens
 - Coût du lien = $10^8/\text{Débit}$
 - En bit/s
 - Ethernet 10M → $10^8/10^7=10$
 - Modem 56K → 1785
 - ADSL 512Kb/s → 195
 - Chaque lien peut se voir attribué un coût spécifique

PARTIE II – ROUTAGE INTRA-FAI

OSPF - *PRINCIPALES ÉTAPES (I)*

- 1 - Etat initial
 - État des liaisons
 - Remonté par les couches inférieures
 - Insertion de l'information dans la Topology Information Base (TIB)

PARTIE II – ROUTAGE INTRA-FAI

OSPF - *PRINCIPALES ÉTAPES (II)*

- 2 - Découverte des voisins
 - Objectif: Lister la topologie à un saut d'un routeur afin
 - De gérer les échanges d'information sur chacun des réseaux
 - D'obtenir une première image de la topologie
 - De savoir avec qui communiquer
 - Mécanisme: les messages Hello
 - Annonce au monde des routeurs ospf sa présence
 - Hello
 - Multicast – 224.0.0.5 = ensemble des routeurs ospf (TTL fixé à 1)
 - Réponse unicast des routeurs
 - Période d'émission = 10 s par défaut
 - Remplissage d'une base de donnée
 - La table d'adjacence = ensemble des routeurs voisins
 - Appartient à la TIB
 - Base d'OSPF => état de liens

PARTIE II – ROUTAGE INTRA-FAI

OSPF - *PRINCIPALES ÉTAPES (III)*

○ 3 - Election du Designated Router Centre d'information du réseau

- Responsable des LSA sur un réseau multipoint
- Élection d'un backup (BDR)
- Principe du DR
 - Échange d'information sur le réseau centralisé par le DR
- Objectifs
 - Réduction du trafic lié à l'échange des Link States Quand y'a un changement, envoie à LS et renvoie à tout le monde
 - Amélioration de l'intégrité de la TIB par l'unicité
 - Accélération de la convergence
- Comment
 - Pendant les messages Hello
 - DR = routeur à la plus grande priorité
 - Si égalité => adresse IP la plus grande
 - Si nouveau apparaît alors que DR est déjà désigné, il n'y a pas de réélection

PARTIE II – ROUTAGE INTRA-FAI

OSPF - *PRINCIPALES ÉTAPES (IV)*

- 4 - Synchronisation des bases de données
 - Objectif
 - Découverte de la topologie
 - Pour pouvoir calculer les routes
 - Comment?
 - Relation maître-esclave entre DR et autres routeurs
 - DR envoie un résumé de sa TIB via des LSAdvertisment
 - Le routeur envoie un LSRequest si le résumé reçu est plus récent que ses infos de TIB
 - Le DR répond par un LSUupdate
 - Le routeur peut envoyer des mises à jour au DR (via LSA)
 - Utilisation de groupe multicast
 - Esclave -> maitres (DR&BDR) 224.0.0.6
 - Maître (DR) -> esclave 224.0.0.5
 - *A étudier en TP*

PARTIE II – ROUTAGE INTRA-FAI

OSPF - *PRINCIPALES ÉTAPES (V)*

- 5 – Calcul des routes
 - Application de SPF sur la TIB
 - Augmentation de la complexité avec la taille de la zone
 - Consommation de la ressource CPU
 - Obtention de la RIB
- 6 – Extraction de la FIB

PARTIE II – ROUTAGE INTRA-FAI

OSPF – *MESSAGES (I)*

- Les différents types de messages
 - Hello
 - Découverte voisinage
 - Election du DR et BDR
 - Database Description
 - Informations résumées de description du réseau
 - Link State Request (LSR)
 - demande d'info explicite
 - Link State Update (LSU)
 - Réponse à un LSR
 - Ou spontanément
 - Volumineux
 - Link State Ack accusé de réception d'un LSU
 - Fiabilisation de la cohérence des bases

PARTIE II – ROUTAGE INTRA-FAI

OSPF – *MESSAGES (II)*

○ En-tête commune des PDUs

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31									
version								type								packet length																								
router ID																																								
area ID																																								
checksum																authentication type																								
authentication																																								
authentication																																								

Type 1 : HELLO

Type 2 : Description de la base de donnée

Type 3 : LSR

Type 4 : LSU

Type 5 : LSA

PARTIE II – ROUTAGE INTRA-FAI

OSPF – *BILAN*

- Permet d'avoir une vision d'ensemble au niveau de chaque routeur de la zone
 - Pas de dépendance vis-à-vis d'un routeur
 - Pas de risque de boucle
 - Choix individuel de chacun des routeurs
- Notion de zone
 - Permet de réduire le calcul par routeur
 - Comment les choisir?
- Charge des calculs
 - Plus importante pour les routeurs OSPF que RIP
 - Augmentation de la complexité avec la taille d'une zone
- Dans les AS
 - Souvent qu'une seule zone...

PARTIE III – ROUTAGE INTER-FAI

BGP - *PRINCIPES*

- Border Gateway Protocol
- EGP à vecteur de chemins
- Granularité : système autonome
- Implanté au dessus de TCP
- Opportunités
 - Agrégation de routes
 - Définition de politiques de routage
- BGP v4
 - RFC 4271

PARTIE III – ROUTAGE INTER-FAI

BGP – *FONCTIONNEMENT GÉNÉRAL*

- Établissement de connexions avec pairs
 - Connexions de longue durée

- Apprentissage de chemins
 - Depuis pairs extérieurs ou intérieurs

- Choix des chemins en fonction de la politique définie
 - Modification de la table de routage
 - Interaction avec les IGP



INTERNET AVANCÉ- III

APPROFONDISSEMENT TCP

103

2A Apprentissage Info&Réseaux

Julien Fasson – julien.fasson@enseeiht.fr

PRÉSENTATION DU SUJET

○ Précédemment

- Les deux fonctions de l'adresse IP
 - Localisation
 - Identification
- La fonctionnalité de routage IP
- Les autres fonctions d'IP = peu utilisées
 - IP = BEST EFFORT
- Autour d'IP
 - En dessous ARP
 - Au contrôle ICMP
 - L'annuaire DNS

○ Mais...

- La nature Best Effort du réseau IP => aucune garantie
- Besoin de mise en place d'un contrôle de bout en bout
- Besoin de différencier et de multiplexer les applications

PLAN

- Partie 1 – Révision +
 - La notion de socket
 - Le format des segments TCP
 - La connexion TCP
 - Les fenêtres TCP
 - Exercice TCP
- Partie 2 – Le contrôle de congestion dans TCP
 - Origine
 - Cas d'utilisation
 - D'autres versions de TCP

I.1 – LA NOTION DE SOCKET

LE BESOIN

- Une interface réseau
 - Envoie de datagrammes dans des trames sur un niveau 2
 - Tag les datagrammes du bon numéro de protocole
 - ICMP, RTP, UDP, TCP...
- Problèmes
 - Comment utiliser un protocole de transport pour plusieurs applications?
 - Comment différencier les communications sur la même entité?
 - Applications différentes
 - Applications identiques

I.1 – LA NOTION DE SOCKET

LA NOTION DE PORT

- Point d'accès
 - au niveau transport
 - pour les applications
- Identifié par un numéro (2B)
 - Numérotation officiel des ports
 - de 1 à 1024 à l'origine
 - de 1 à 49151
 - Attribution par l'IANA
 - 80 serveur web – 23 serveur Telnet
 - 25 serveur mail – 22 serveur SSH
 - 53 serveur DNS
 - Avantage : pas d'annuaire dynamique
 - Défaut : statique

I.1 – LA NOTION DE SOCKET

LA NOTION DE SOCKET

- Objectif
 - Identifier une communication
- Identifier les entités communicantes
 - Identification par l'adresse IP
 - Source
 - Destination
 - Protocole utilisé
 - Numéro de protocole dans l'entête IP
 - Identification de l'application
 - Port applicatif
- Information regroupée sous le nom de socket
 - Adresse IP + numéro de protocole + port applicatif
 - Non indépendance des couches
- Une communication est caractérisée par un couple de socket

I.2 – LE FORMAT DES SEGMENTS TCP

EN-TÊTE OBLIGATOIRE (I)

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Source Port																Destination Port															
Sequence Number																															
Ack Number																															
Header Length		Reserved								U	A	P	R	S	F	Window Size															
Checksum																Urgent Pointer															
Option ...																															
Data ...																															

I.2 – LE FORMAT DES SEGMENTS TCP

EN-TÊTE OBLIGATOIRE (II)

- En-tête
 - Multiple de 4 octets
 - 20 octets d'en-tête obligatoire

- En-tête Obligatoire
 - Source port et destination port
 - Identification unique d'une connexion avec couple sockets
 - Non indépendance des couches
 - Sequence number et ACK number
 - Taille de l'en-tête en mots de 4 octets
 - Flags
 - URG, ACK, PSH, RST, SYN et FIN
 - Window size = advertized window
 - Checksum
 - Urgent Pointer

I.2 – LE FORMAT DES SEGMENTS TCP

LES FLAGS

○ URG

- Le bit URG valide
 - la présence du pointeur Urgent Pointer
 - En-tête optionnelle
- Urgent Pointer pointe sur le premier octet de données après les données urgentes
- Utilisation non spécifiée

○ PSH

- Objectif : délivré au plus vite
- Comment?
 - Pas de concaténation sur l'émetteur
 - Transmission directe à l'application du côté du récepteur

○ RST

- Réinitialisation de la connexion
- Tentative d'ouverture d'une connexion déjà ouverte
- Réception de données sur une connexion inconnue
- Accusé de réception de données non émises

I.2 – LE FORMAT DES SEGMENTS TCP

EN-TÊTE OPTIONNEL

- Mots de 4 octets
- Option courante
 - Maximum Segment Size (MSS)
 - Négociée pendant le SYN
 - Objectif : Ne plus fragmenter au niveau IP
 - Window scaling
 - Illustration du maximum théorique
 - Multiplicateur sur les tailles de fenêtre

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Kind = 2								Length = 4								MSS															

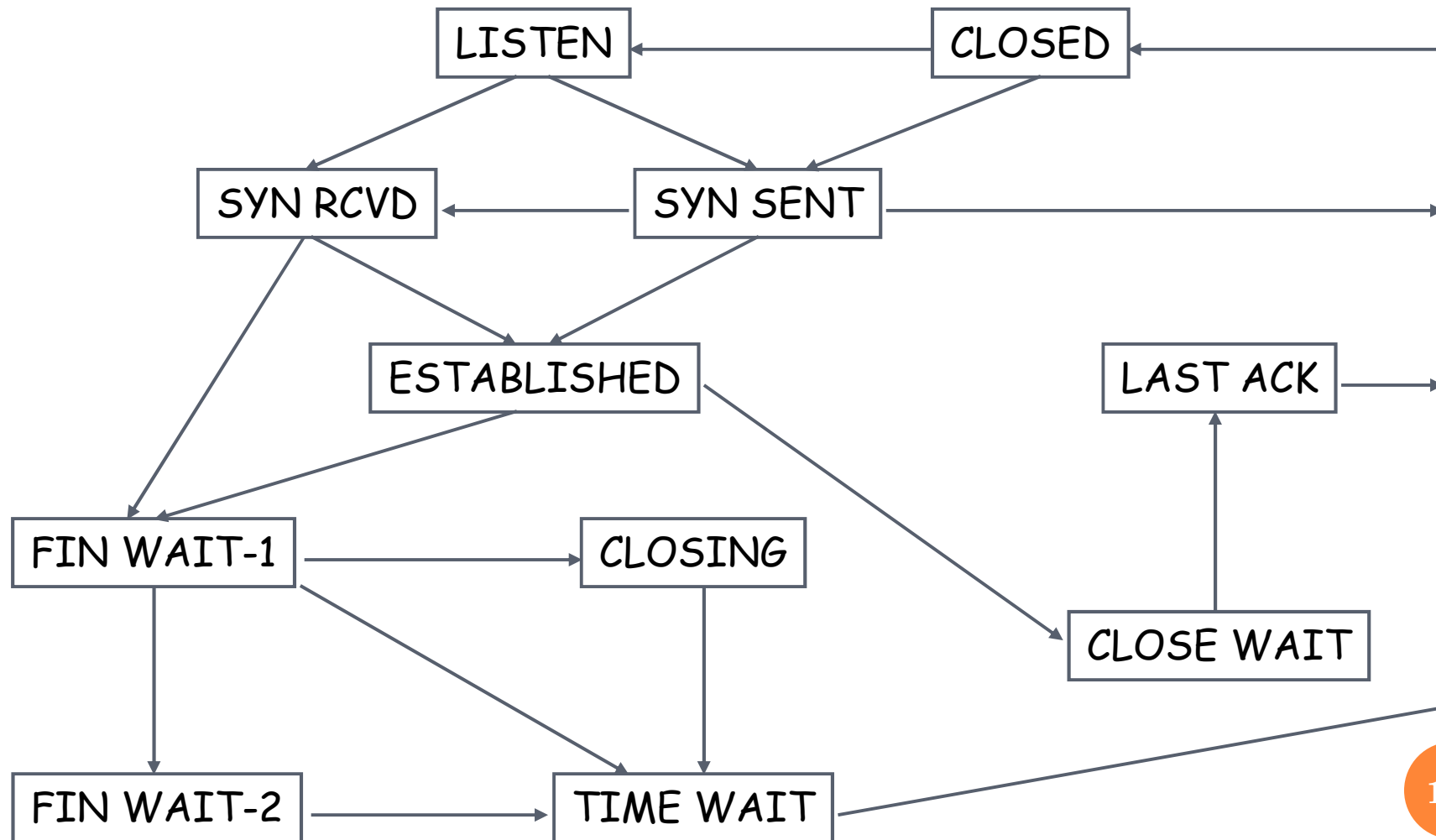
I.3 – LA CONNEXION TCP

RÉSUMÉ

- Ouverture de la connexion
 - « Three-Way Handshake »
 - Trois temps
 - Bidirectionnelle
 - Négociation des paramètres
- Communication
 - Segments du flot d'octets
 - Mécanisme à fenêtre coulissante
- Terminaison
 - Fermeture indépendante des sens de communication
 - Connexion unidirectionnelle (semi-fermeture)
- Réinitialisation
 - Drapeau RESET
 - Détection d'un dysfonctionnement

I.3 – LA CONNEXION TCP

ETAT D'UNE CONNEXION TCP



I.4 – LA GESTION DE LA FENÊTRE TCP

ECHANGE DE DONNÉES

- Flux d'octets segmenté

- Numérotation des segments Numéro du premier octet contenu dans la donnée
- Octet par octet

- Buffer de réception Taille maximale annoncée par la fenêtre de réception advertised window
Le récepteur indique la taille de fen maximale pour ne pas être submergé

- Stockage des segments hors s'équence
- Contrôle de flux

- Buffer d'émission

- Stockage des segments non acquittés
- Contrôle de flux et reprise sur perte

I.4 – LA GESTION DE LA FENÊTRE TCP

NOTATIONS

- Caractéristiques d'un émetteur
 - SND.UNA Premier octet non acquitté
 - SND.NXT Prochain octet à émettre
 - SND.WND Taille de la fenêtre d' émission

- Caractéristiques d'un récepteur
 - RCV.NXT Prochain octet attendu
 - RCV.WND Taille de la fenêtre de réception

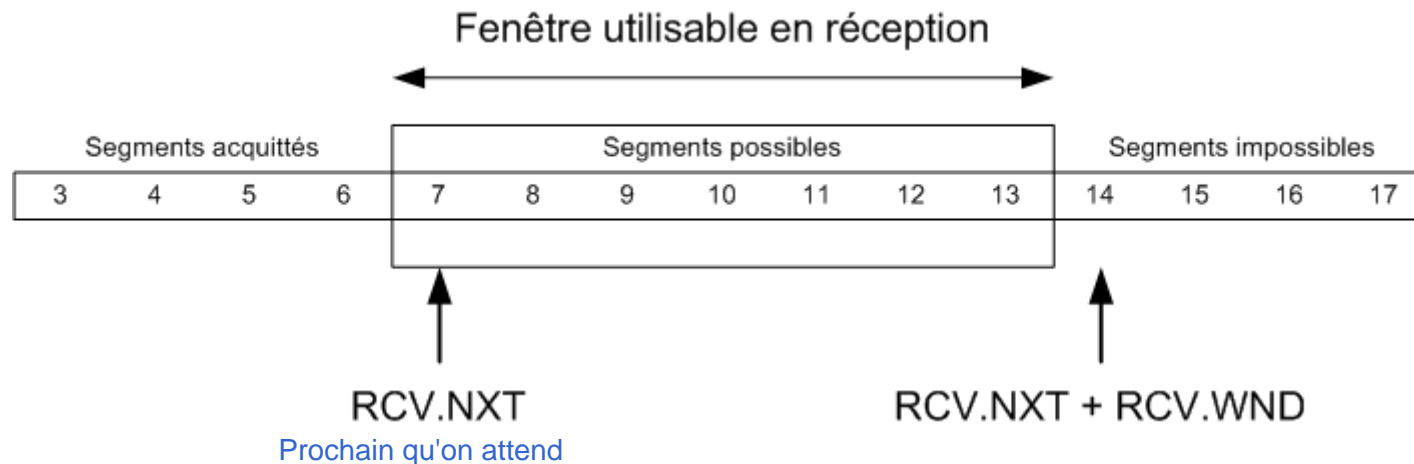
- Caractéristiques d'un segment
 - SEG.ACK Prochain octet attendu par l'émetteur
 - SEG.LEN Nombre d'octets du segment
 - SEG.SEQ Numéro du premier octet du segment
 - SEG.WND taille de la fenêtre de réception véhiculée

I.4 – LA GESTION DE LA FENÊTRE TCP

LA FENÊTRE EN RÉCEPTION

- Evolution de RCV.NXT
 - Réception d'un segment en séquence
- Evolution de RCV.WND
 - Réception d'un segment dans la fenêtre hors séquence
 - Consommation de données par l'application
- Accusé de réception (immédiat ou piggy-backé)
 - Réception d'un segment en séquence
 - SEG.ACK reçoit RCV.NXT (une fois RCV mis à jour)
 - SEG.WND reçoit RCV.WND (aka awnd)
- $RCV.NXT + RCV.WND$ ne doit jamais décroître

Si le segment n'est pas en séquence, ça ne change pas. Si on attend le 5 et qu'on reçoit 10, on attend toujours 5.

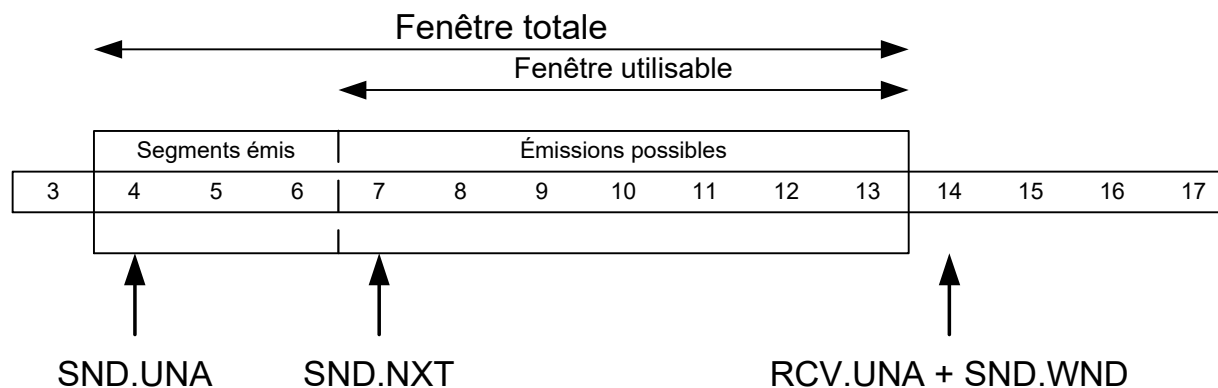


Si on reçoit un truc là, il y a un problème

I.4 – LA GESTION DE LA FENÊTRE TCP

LA FENÊTRE EN ÉMISSION

- Fenêtre glissante
- Évolution de SND.UNA sur accusé de réception
 - Recevable si $\text{SND.UNA} < \text{SEG.ACK} \text{ } \text{SND.NXT}$
- Évolution de SND.NXT sur demande de l'application
- Évolution de SND.WND sur réception d'un segment
 - SND.WND reçoit SEG.WND



I.4 – LA GESTION DE LA FENÊTRE TCP

LE TIMER DE RETRANSMISSION

- Problème
 - Différence avec un niveau liaison
 - Gigue non bornée
 - Chemins multiples
 - Aucune connaissance du réseau
 - Unique information = ACK
- Mesure expérimentale du RTT
 - Utilisation d'une moyenne glissante
 - SRTT reçoit $\alpha * \text{SRTT} + (1-\alpha) * \text{RTT}$
- Timer de réémission calculé en fonction de SRTT
 - RTO reçoit $\text{Béta} * \text{SRTT}$
 - Coefficient calculé en fonction de la variance du RTT
 - Une valeur communément utilisée est 2
 - Mais trop petite en cas d'instabilité

I.5 – EXERCICE TCP

ILLUSTRATION DE L'INSUFFISANCE DU CONTRÔLE DE FLUX

- Objectifs
 - Fenêtres
 - Fenêtre courante d'émission
 - Fenêtre de réception (awnd)
 - Accusés de réception cumulatif
 - Timer de retransmission
 - Retransmission Time Out
 - Calcul du RTO
- Questions
 - Donner la valeur d'awnd ?
 - Décrire le contenu de la fenêtre en A, B, C, D et E et expliquer son évolution.
 - D'où vient le problème?

PARTIE II – LE CONTRÔLE DE CONGESTION

PLAN (I)

II – 1 Contrôle de congestion dans TCP

- 2.1.1 – Contrôle de congestion et niveau du transport – le dilemme
- 2.1.2 – Une nouvelle fenêtre – cwnd
 - Obj = borner l'wnd par une valeur représentative de l'état de congestion du système
- 2.1.3 – Le Slow Start
 - Obj = éviter les burts de segments émis au démarrage de la connexion
- 2.1.4 – Evolution de cwnd
 - Obj = réagir en fonction de la congestion en baissant le débit
 - Problèmes :
 - Comment détecter la congestion?
 - Comment réagir?
- 2.1.5 – Retransmission Time Out et cwnd
 - Obj = prendre en compte la retransmission comme un problème de congestion
 - Comment = Introduction de la phase de Contrôle de Congestion

PARTIE II – LE CONTRÔLE DE CONGESTION

PLAN (I)

- 2.1.6 – Le Fast Retransmit
 - Obj = détecter plus rapidement un problème sur le réseau (et donc réagir plus rapidement)
- Conclusion TCP Tahoe

II – 2 Evolutions basiques de TCP

- 2.2.1 – L'impact du Slow Start sur les performances de TCP
- 2.2.2 – TCP RENO
 - Obj : Ne pas considérer trop pénalisé le débit TCP suite à une perte détectée par ndup
 - Comment:
 - Introduction du Fast Recovery pendant la récupération d'une perte
 - Abandon du Slow Start si on arrive à récupérer de la perte
- 2.2.3 – TCP New RENO
 - Pb : Mauvais comportement de TCP RENO lors de pertes multiples
 - Obj : Amélioration du comportement de TCP lors de pertes multiples

II – 3 D'autres évolutions...

PARTIE II – LE CONTRÔLE DE CONGESTION

AU NIVEAU RÉSEAU

- Paradoxe du contrôle de congestion dans Internet
 - La congestion est un problème réseau
 - Détection = routeur
 - Routeur = entité clef de la congestion
 - Gestion de la congestion?
 - Saturation du buffer du routeur
 - Suppression de paquet
 - Lesquels?
 - Dépendance de la file d'attente et de sa gestion
 - Nature Best Effort d'IP
 - Pas gestion de congestion
 - Pas d'information

PARTIE II – LE CONTRÔLE DE CONGESTION

AU NIVEAU RÉSEAU

- Un premier niveau = routeur
 - Pas de gestion
 - Files FIFO
 - Injustice
 - Utilisation de files spécifiques
 - Round Robin
 - Mais comment distinguer les paquets?
 - Adresse IP => table de mémorisation
 - Tags?
 - Ajout de tags
 - Utilisation du champ ToS
 - Diffserv
 - Intserv
 - MPLS
 - Interne à un FAI
 - Mais gérer la congestion ce n'est pas la prévenir...
 - Prévenir
 - Explicit Congestion Notification

PARTIE II – LE CONTRÔLE DE CONGESTION

AU NIVEAU RÉSEAU

- ECN [RFC 3168]
 - Principe
 - Avertir les entités de bout en bout d'une congestion pour leur communication
 - Besoin
 - Le protocole de bout en bout doit être capable de gérer la congestion
 - TCP, application spécifique
 - Négocier l'utilisation d'ECN
 - Avoir un retour!
 - L'émetteur doit recevoir une information de la congestion
 - Avoir un retour!
 - Comment
 - Champ TOS
 - Négociation de l'option ECN de bout en bout
 - Marquage aller/retour (OI et IO)
 - Marquage des routeurs « ECN capable » des paquets par CE (II) (Congestion Experienced)
 - Emission d'une information Backward à la source à la réception de II
 - Champ TCP reserved utilisé

CONCLUSION

○ TCP

- A la base
 - Contrôle de flux
 - Reprise d'erreur
 - Reséquencement
 - Multiplexage applicatif ...
- Mais...
 - Contrôle de flux peut s'avérer un handicap
 - Prise en compte de la congestion
 - Slow Start
 - Fast Retransmit
 - Fast Recovery
 - Congestion Avoidance
- Multiples versions de TCP
 - Différence principale = comportement face à la détection d'une perte
 - A la base une perte = une erreur du support
 - Evolution vers une perte = une congestion
 - Mais pas que...
- TCP est un protocole empirique
 - Observation du réseau
 - pas d'information réseau au niveau TCP
 - Fondé sur l'expérimentation
 - Quid de l'évolution?
 - La congestion reste un problème de niveau 3!



INTERNET AVANCÉ- IV

UN PETIT TOUR SUR LES APPLICATIONS

127

2A Apprentissage Info&Réseaux

Julien Fasson – julien.fasson@enseeiht.fr

PLAN

1 – Rouages applicatifs

Le modèle de communication
Domain Name Server
File Transfer Protocol
HyperText Transfer Protocol

2 – Un brin d'administration

Simple Network Management Protocol
Dynamic Host Configuration Protocol

3 – Pair à Pair ou la révolution Internet ?

4 – De la sécurité sinon rien !

1 – ROUAGES APPLICATIFS

OBJECTIFS ET PLAN

- « Fondamentaux » applicatifs d'Internet
 - Le Dialogue Client / Serveur
- Pour communiquer
 - Connaître l'adresse IP du serveur ?
 - Connaître le nom du serveur ?
 - DNS
- Télécharger des données
 - Ex : FTP
- Naviguer sur le Web
 - Récupérer et Restituer des informations de navigation
 - Pages Web
 - Informations visibles
 - Méta-informations
 - Naviguer => HTTP

1.1 – LE MODÈLE DE COMMUNICATION

○ Client / Serveur

- Largement inspiré du modèle TCP
- Client
 - Origine de la communication
 - Emet la requête
- Serveur
 - A l'écoute des clients
 - Traitement de demandes qui peuvent être nombreuses

○ Modèle de trafic lié

- Asymétrie
 - Client requête (signalisation) (-)
 - Serveur rend un service (données) (+)
- On parle d'un modèle commercial
 - Justification du modèle des accès pour les particuliers
 - Justification technique = partage de la ressource en upload plus délicate

1.2 – DOMAIN NAME SERVER

LE BESOIN

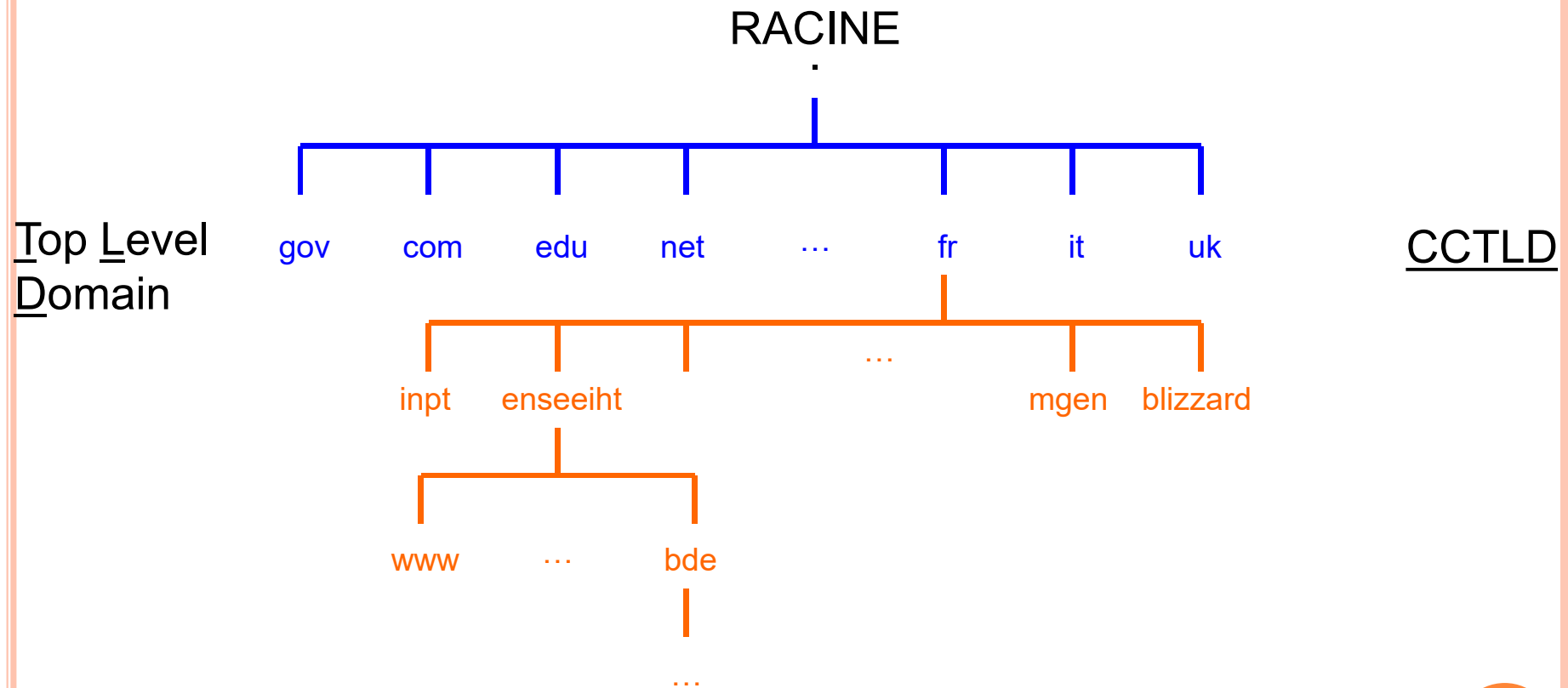
- Mémoriser des adresses IP
 - Analogie numéro de téléphone
 - Nom
- Correspondance?
 - Statique
 - Fichier host ou host.txt
 - Problème de la maintenance de la liste
 - Annuaire dynamique
 - Centralisé ou distribué?
- DNS

1.2 – DOMAIN NAME SERVER *GÉNÉRALITÉS*

- Annuaire distribué
 - nom symbolique <-> adresse IP
 - chaque domaine gère sa partie
- Définition
 - d'un protocole de communication [RFC 1034] [RFC 1035]
 - d'une politique de délégation [RFC 1591]
- Fondé sur
 - Une organisation de l'espace
 - Un système de serveurs hiérarchisés
 - De nombreux clients appelés resolver
- Deux parties
 - Un protocole de communication
 - Une politique de répartition des noms de domaines

1.2 – DOMAIN NAME SERVER

ORGANISATION DE L'ESPACE DES NOMS (I)



1.2 – DOMAIN NAME SERVER

ORGANISATION DE L'ESPACE DES NOMS (II)

- Fully Qualified Domain Name
 - www.enseeiht.fr. = Nom absolu
 - www = hôte (serveur web)
 - Profondeur maximale = 127 niveaux
 - 255 caractères max

- Notion de zone
 - Ex: enseeiht.fr
 - Peut être subdivisée (bde.enseeiht.fr)
 - Deux ou plus serveurs de noms DNS par zone
 - Primaire
 - Secondaire(s)

1.2 – DOMAIN NAME SERVER

SERVEURS DE NOMS DNS

- Serveurs DNS
 - Serveurs Racines
 - 13 serveurs au monde
 - Serveurs de domaine
 - Autorité sur une zone
 - Déclaré au serveur de domaine directement supérieur
- Dialogue
 - Resolver et DNS primaire
 - DNS zone avec DNS zone parente
- Logiciel
 - Plus commun = BIND
(Berkeley Internet Name Domain)

1.2 – DOMAIN NAME SERVER

RESOLVERS

○ Définition

- Processus client qui contacte les serveurs de noms

○ Rôles

- Dialogue avec le serveur de nom
- Interprétation des réponses
- Restituer l'information au logiciel appelant
- Mise en place d'un système de cache local

1.2 – DOMAIN NAME SERVER

LE PROTOCOLE (I)

- Messages
 - Questions
 - Réponses
 - Utilisation d'UDP
- Principe
 - Renvoyer le message au serveur DNS le plus apte à répondre
- Deux modes d'interrogation des serveurs
 - Itératif
 - Envoie de l'info la plus détaillée dont le serveur dispose
 - Récursif
 - Serveur prend en charge la suite des requêtes
 - Dépendant du serveur interrogé
 - Notion de serveur maître
 - Couplage des modes

1.2 – DOMAIN NAME SERVER

LE PROTOCOLE (II)

Illustration en cours

1.2 – DOMAIN NAME SERVER

DNS ET SÉCURITÉ

- Point critique d'Internet
 - DNS permet de faire association
 - nom symbolique
 - Adresse IP
 - Faux DNS = Fausse réponse
- Points faibles
 - Aucune préoccupation de sécurité
 - Interception et forge
 - Dénî de service
- Solutions
 - DNSSEC
 - Ne pas se référer à n'importe quel DNS!

1.3 – FILE TRANSFER PROTOCOL

GÉNÉRALITÉS

- Transfert (explicite) de fichier
 - Modèle Client/Serveur
 - Serveur FTP
 - Arborescence de fichiers
 - Commandes FTP pour lister, ajouter, télécharger...
- Supporte l'hétérogénéité
 - OS
- Fiable : basé sur TCP
- [RFC 114] [RFC 765] [RFC 959]

1.3 – FILE TRANSFER PROTOCOL

PRINCIPE

- Trois « Interfaces »
 - Interface utilisateur (dépendant du logiciel)
 - Cyberduck, gftp, CuteFTP...
 - Plan commandes
 - Plan de données

- Deux modes
 - Mode actif
 - Mode passif

1.3 – FILE TRANSFER PROTOCOL

CONNEXION DE CONTRÔLE

- Ouverture de connexion TCP
 - Du Client
 - Vers le port 21 serveur

- Commandes
 - En texte (telnet)
 - Contrôle d'accès
 - USER, PASS, CWD, QUIT, ...
 - Paramétrage du transfert
 - PORT, TYPE, ...
 - Service
 - RETR, STOR, ABOR, ...

1.3 – FILE TRANSFER PROTOCOL

CONNEXION DE DONNÉES

- Mode Actif
 - Ouverture d'une connexion
 - Du serveur
 - Vers le port 20 du client
 - Problèmes
 - Firewall
 - NAT
- Mode Passif
 - Choix d'un port par le serveur
 - Envoie du port au client
 - Ouverture de la connexion par le client

1.4 – HYPERTEXT TRANSFER PROTOCOL

- Protocole
 - Client/serveur
 - TCP
 - Ouverture de connexion par le client vers le port 80 du serveur
- Client HTTP
 - Navigateur web
 - Grande concurrence
 - IE, Mozilla-Firefox, Chrome, Opera...
 - Interprétation HTML
 - Aspirateur de sites
 - Robots d'indexation
 - Moteur de recherche
- Serveur HTTP
 - Apache
 - Internet Information Services
 - Web Zeus
- Exercice :
 - Différents Messages et Encapsulation pour envoyer le premier GET de la page d'accueil à un serveur WEB

2 – UN BRIN D'ADMINISTRATION

PLAN

2 – Un brin d'administration

2.1 – Simple Network Management Protocol

- a) Besoin
- b) Généralités
- c) Protocole

2.2 – Dynamic Host Configuration Protocol

- a) Besoin
- b) Généralités
- c) Principe

2.1 – SIMPLE NETWORK MANAGEMENT PROTOCOL

UN BESOIN

- Supervisor
 - Détections pannes matériel
 - Mauvaise configuration
 - Mauvais comportement
 - Performances
- Administration et configuration
 - Du réseau
 - Des différents équipements
 - Serveurs
 - Routeurs
 - ...
 - Des différentes configurations
- Gestion de la sécurité
- A distance

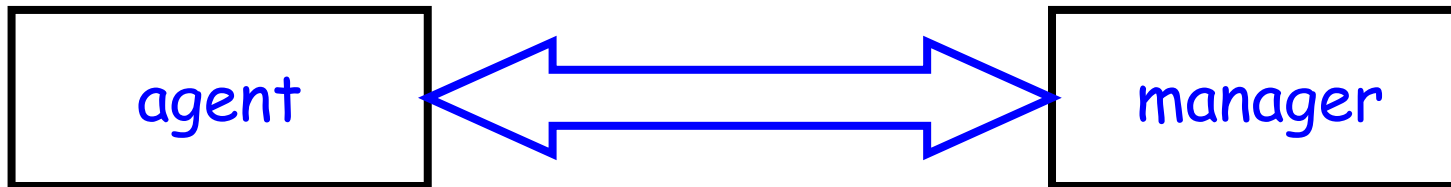
2.1 – SIMPLE NETWORK MANAGEMENT PROTOCOL

GÉNÉRALITÉS

- Un protocole
 - Trois versions
 - v1 [RFC 1157] (en 87-89)
 - v2 [RFC 1441]
 - V3 [RFC 2571] (plus de sécurité)
 - Sur UDP – à destination du port 161 pour les requêtes
 - Récolte d'informations pour le superviseur
 - Standard pour TCP/IP
- Trois éléments
 - Superviseur
 - Nœuds = équipement supervisé
 - Agents = interface de communication sur noeud
- Base de données arborescente
 - Management Information Base
 - Base de donnée d'un équipement
 - Consultation/modification
 - Structure hiérarchique
 - MIB II [RFC 1213] (TCP/IP)

2.1 – SIMPLE NETWORK MANAGEMENT PROTOCOL

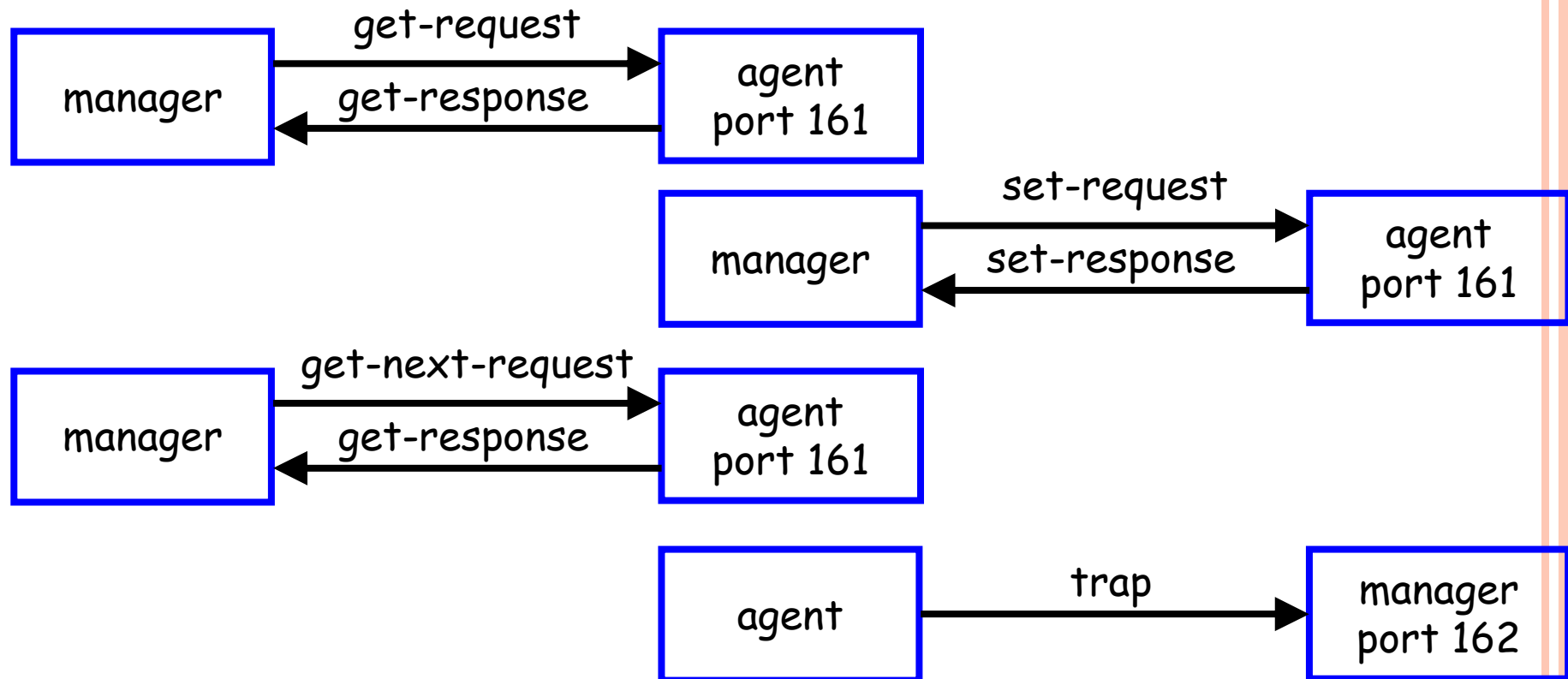
LE PROTOCOLE – RÔLE DE L'AGENT ET DU SUPERVISEUR



- Agent
 - élément d'administration local
 - émet des alertes (trap)
- Superviseur
 - interface utilisateur
 - envoie des ordres aux agents (get, get_next, set)

2.1 – SIMPLE NETWORK MANAGEMENT PROTOCOL

LE PROTOCOLE – LES ÉCHANGES



2.2 – DYNAMIC HOST CONFIGURATION PROTOCOL

UN BESOIN

- Configurer
 - Un profil réseau
 - Interface IP
 - Route par défaut
 - DNS
 - ...
 - Machines utilisateurs
 - Nombre
 - Similitudes et différences
- Configuration manuelle
 - Adressage statique
 - Maintenance
 - Prise en otage d'adresses
- Configuration automatisée
 - DHCP

2.2 – DYNAMIC HOST CONFIGURATION PROTOCOL

GÉNÉRALITÉS

- Dynamic Host Configuration Protocol
 - Protocole Client/Serveur
 - Fondé sur UDP
 - Port 67 (requête à destination du serveur)
 - Port 68 (réponse à destination du client)
- Configuration au démarrage
 - Adresse IP d'une machine et masque du réseau
 - Route par défaut
 - Adresse du DNS
 - Adresse du serveur TFTP pour OS
- Allocation dynamique/temporaire d'adresses
- [RFC 2131], [RFC 1533]

2.2 – DYNAMIC HOST CONFIGURATION PROTOCOL

PRINCIPE

- Requête du client
 - Diffusion sur le réseau
 - DHCP DISCOVER
- Offre du serveur (ou des serveurs)
 - Unicast au client
 - DHCP OFFER
- Choix de l'offre
- Demande au serveur
 - Diffusion sur le réseau
 - DHCP REQUEST
- Confirmation et informations du serveur
 - DHCP ACK

3 – PAIR À PAIR OU LA RÉVOLUTION D' INTERNET?

PLAN

3 – Pair à Pair

3.1 – Principe

- a) Réseau d'Overlay
- b) Aux Origines du pair à pair
- c) Générations de pair à pair

3.2 – Une révolution d'Internet

3.1 – PRINCIPE

RÉSEAU D'OVERLAY

- Pair à pair c'est quoi?
 - Communication d'égal à égal
 - Opposition au modèle client/serveur
 - « Client et serveur à la fois »
- Réseau d'overlay
 - Réseau de recouvrement
 - « Réseau au dessus du réseau »
 - Mise en œuvre
 - Tunnel
 - Routage applicatif
 - Utilité
 - Test de protocole
 - Gestion et maintenance
 - Partage de ressources
 - Nœud du réseau = processus applicatif sur une machine

3.1 – PRINCIPE *AUX ORIGINES*

- Né en 1995 aux Etats-Unis
 - Besoin de partage de données
 - Universités
- Napster
 - 1999 – création par Shawn Fanning
 - 2000 – 23 millions d'utilisateurs
 - 2002 – Napster fermé
- Mais d'autres ont déjà pris la relève
 - KaZaA, Morpheus...

3.1 – PRINCIPE

PREMIÈRE GÉNÉRATION DE PAIR À PAIR

- Index central
 - Permet de trouver les machines associés à un fichier
- Principe
 - Client connaissent différentes adresses de serveur
 - Client indexe auprès du serveur leurs fichiers partagés
 - Interrogation des serveurs
 - Dialogue entre client
- Problèmes
 - Légaux
 - Vulnérabilité des serveurs centraux
 - Responsabilité direct du fournisseur de service
- Logiciels
 - Napster
 - Audiogalaxy
 - Accords très rigoureux bloquant la quasi-totalité des fichiers à partir de 2002

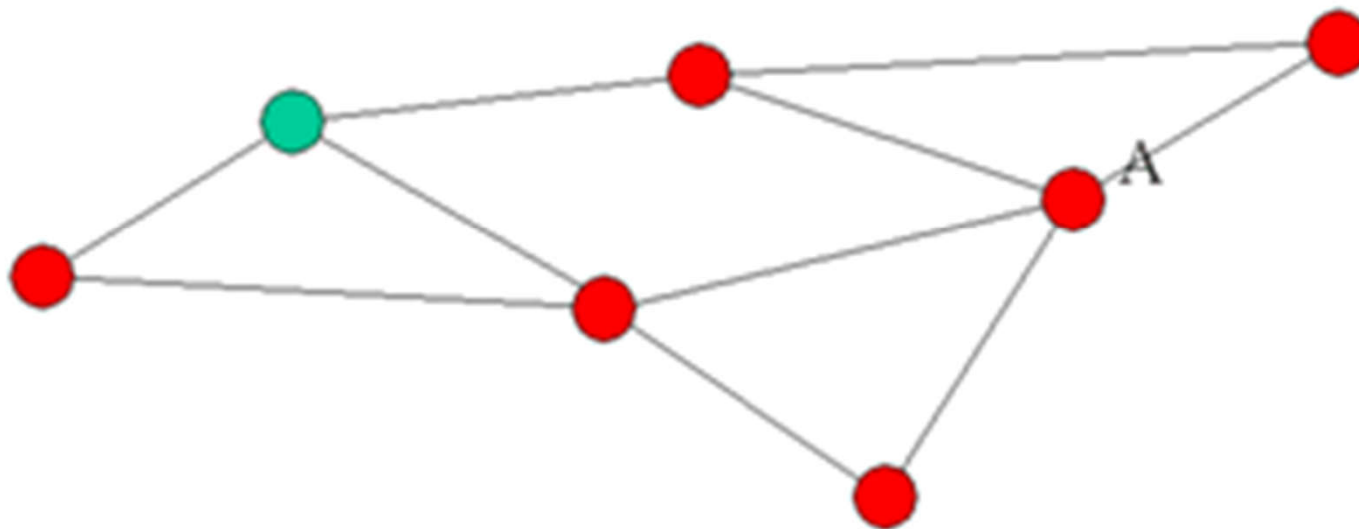
3.1 – PRINCIPE

DEUXIÈME GÉNÉRATION DE PAIR À PAIR (I)

- Index par machine du réseau
 - Interrogation de proche en proche
 - Utilisation d'un cache pour les connaître les machines (Gwebcache)
- Principe
 - Client indexe leurs fichiers partagés
 - Client contacte un voisin (grâce à un cache pour trouver le premier)
 - Voisin renvoie ses voisins connus et ainsi de suite
 - Dialogue entre client en passant par les pairs
- Problèmes
 - Différences de capacités des noeuds
- Logiciels
 - Gnutella v0.4

3.1 – PRINCIPE

DEUXIÈME GÉNÉRATION DE PAIR À PAIR (II)



3.1 – PRINCIPE

TROISIÈME GÉNÉRATION DE PAIR À PAIR

- Distinction entre pair
 - Pair = connexion bas débit
 - Superpair = connexion haut débit
- Principe
 - Client indexe leurs fichiers partagés auprès des superpair
 - Fonctionnement basé sur un réseau de superpair
- Logiciels
 - Gnutella v0.6
 - Kazaa sur FasTrack (réseau)

3.1 – PRINCIPE

LES NIÈMES GÉNÉRATIONS

- Prise en compte de l'asymétrie
 - Utilisation d'ADSL
 - Téléchargement multiple
- Coopération
 - Fragments téléchargés directement disponibles au partage
 - Point de téléchargement par fichier échangés
 - Donneurs multiples
- Indexation par hachage
 - Overnet
- Logiciels
 - eDonkey, eMule et mlDonkey sur réseau eDonkey
 - BitTorrent

3.2 – UNE RÉVOLUTION D'INTERNET

QUELQUES RÉFLEXIONS

- Ouverture vers le monde
 - Rapide diffusion
 - Démocratisation de la musique
 - Naissance de nouveaux artistes et nouvelles vagues musicales
- Ouverture des réseaux
 - Multiplication du principe pair à pair pour
 - Distribution OS (Redhat)
 - Jeux en réseau
 - Voix sur IP (skype)
- Mais
 - Enjeux « Ethiques »
 - Enjeux Economique

3.2 – UNE RÉVOLUTION D'INTERNET

QUELQUES CHIFFRES

- Déformation du trafic Internet en 2005-2006
 - Plus de 80% de la masse du trafic mondial?
 - Sur certains réseaux d'accès
 - Poids de la signalisation
 - Déforme le modèle classique et asymétrique du client serveur
 - Peur = la fin d'Internet
- La quasi-totalité des Internautes ont un logiciel de P2P (2006)
 - 40% des internautes français téléchargent de la musique illicitement
 - amalgame

4 – DE LA SÉCURITÉ SINON RIEN!

- Ben rien alors!
- La sécurité
 - loin de la préoccupation de l'internaute lambda
 - infection par des logiciels communs
- Buts de l'infection
 - Évolution du « tour de force »
 - Destruction de fichier
 - Mise à mal d'un système d'exploitation
 - Destruction du système (BIOS, périphérique, ...)
 - A l'arnaque, la fraude et le crime organisé



INTERNET AVANCÉ V

AUTOUR D'IP

164

2A Apprentissage Info&Réseaux

Julien Fasson – julien.fasson@enseeiht.fr

PRÉSENTATION DU SUJET

○ Précédemment

- Internet = IP
 - Simple
 - Limites
 - Congestion => TRANSPORT
 - Adressage => réseau privé & NAT
 - ...

○ Une autre version d'IP?

- Plusieurs solutions
 - Que doit-on intégrer?
 - Que doit-on changer?

=> IPv6
- Hétérogénéité?
 - Les tunnels

PARTIE I – IPv6

HISTORIQUE

○ Besoins

- Augmentation rapide du nombre d'utilisateurs d'Internet
 - En 1990 – moins d'un million d'utilisateurs d'Internet
 - En 2000 – 250 millions d'utilisateurs d'Internet
 - En 2010 – plus de 2 milliards d'utilisateurs d'Internet
- Impact sur
 - L'espace d'adressage
 - 2^{32} adresses = 4.29 milliards d'adresses
 - Mais problème de l'attribution
 - Pénurie d'adresses?
 - La taille des tables de routage
 - Explosion des tables de routages?
 - La sécurité devient préoccupante dans Internet
 - Utilisation commerciale grandissante
 - La mobilité

PLAN

- Partie 1 – IP version 6
 - Historique
 - Principe et Fonctionnement
 - En-tête IPv6
 - L'adressage IPv6
 - Auto-configuration
 - « Nouveaux » Protocoles
- Partie 2 – IP et tunnel
 - Principe
 - Generic Routing Encapsulation
 - IPsec
- Partie 3 – Multicast IP
 - Principe
 - Listing de protocoles

PARTIE I – IPv6

HISTORIQUE

- Appel à un nouveau protocole dans le début des années 90
 - Plusieurs Propositions
 - Dont l'utilisation d'adresses au niveau Transport
 - Et Simple Internet Protocol Plus, le futur IPv6
 - Elaboration des différents critères techniques
 - Décembre 1994 – RFC 1726 Critères
 - Janvier 1995 – RFC 1752 Recommandations
 - Elaboration du protocole
 - Décembre 1995 – RFC 1883 spécifications d'IPv6
 - Décembre 1998 – RFC 2460 finalisations d'IPv6

PARTIE I – IPv6

PRINCIPE ET FONCTIONNEMENT

- Fonctionnement équivalent à IPv4
- Mais
 - Augmentation de la taille des adresses
 - x4 bits = 128 bits (notation en hexa)
 - Structuration augmentée de l'adresse
 - En-tête restructurée
 - Simplification pour le routage
 - Ajout d'options via les extensions d'en-tête
 - Multicast natif
 - Sécurité
 - Auto-configuration
 - ...

PARTIE I – IPv6

EN-TÊTE IPv6



PARTIE I – IPv6

EN-TÊTE IPv6 (II)

- Version d'IP => 6
- Traffic Class => priorité ou CoS
- Flow Label => label du flux
- Payload Length => taille de la charge utile (avec les en-têtes optionnelles – pas certain –)
- Next Header => Indique quel type d'en-tête suit dans la charge utile
 - Classiquement c'est un protocole au dessus d'IP (TCP, UDP, OSPF, ICMP,...)
 - Ou un en-tête optionnel
- Hop Limit \Leftrightarrow TTL

PARTIE I – IPv6

EN-TÊTE IPv6 (III)

○ Quelques options

- Fragmentation (Fragment Header) – à noter que la fragmentation n'est réalisable que par la source du datagramme
- Sécurité
 - Authentication Header
 - Privacy Header
- Lecture du contenu
 - End-to-End => lecture que par le destinataire final
 - Hop-by-hop => traitement par les nœuds intermédiaires
- Routage par la source (routing header)

PARTIE I – IPv6

L'ADRESSAGE IPV6 – NOTATION

○ La notation

- Notation en Hexadécimale
- 1 Octet = représentation sur deux chiffres
- Groupement deux octets par deux octets
- Séparation par ‘:’
- Exemple:

2011:adde:0000:05a0:0000:0000:bc2f:8101

○ Simplification de la notation

- Suppression des suites de zeros

2011:adde::05a0:0000:0000:bc2f:8101

2011:adde:0000:05a0::bc2f:8101

- Suppression des zeros non significatifs

2011:adde:0:5a0::bc2f:8101

PARTIE I – IPv6

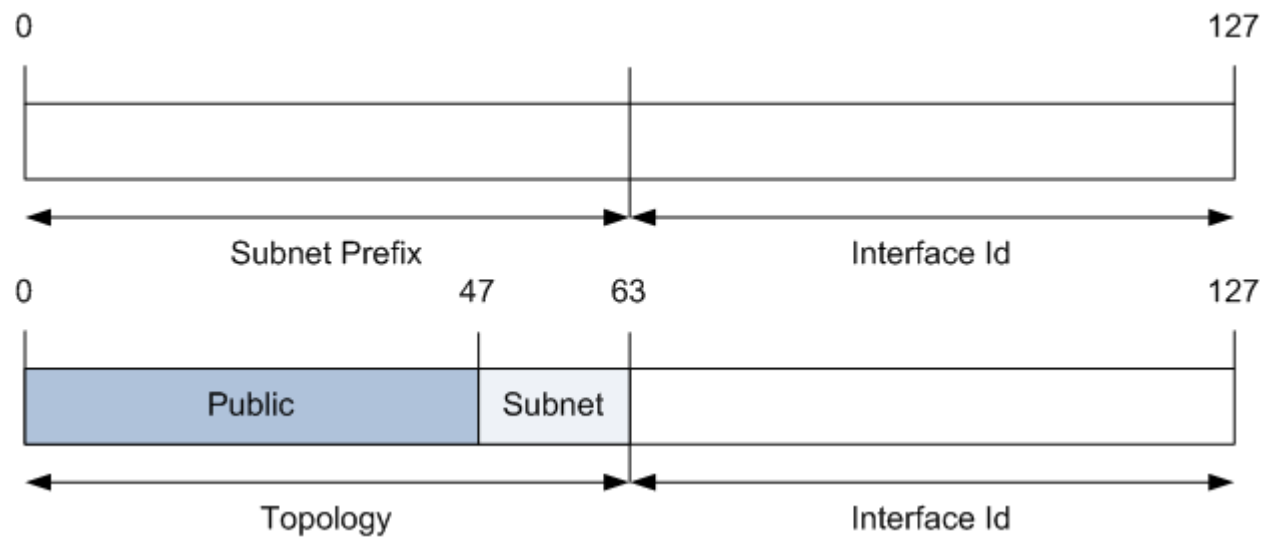
L'ADRESSAGE IPv6

- Des types différents d'adresses
 - Adresses Globales Unicast
 - Adresses Anycast
 - Adresse correspondant à « une machine parmi d'autres »
 - Adresses Site local
 - Adresses Link local
 - Adresses Multicast
 - Adresses spécifiques/réservées
 - Compatibles IPv4
 - Mapping d'une adresse IPv4
 - Adresses de rebouclage
 - ...
 - PAS d'adresses de diffusion

PARTIE I – IPv6

L'ADRESSAGE IPv6

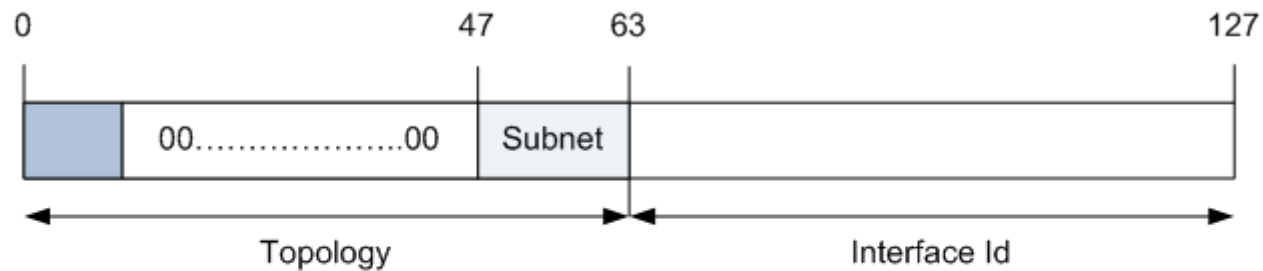
- Unicast et Anycast - unique




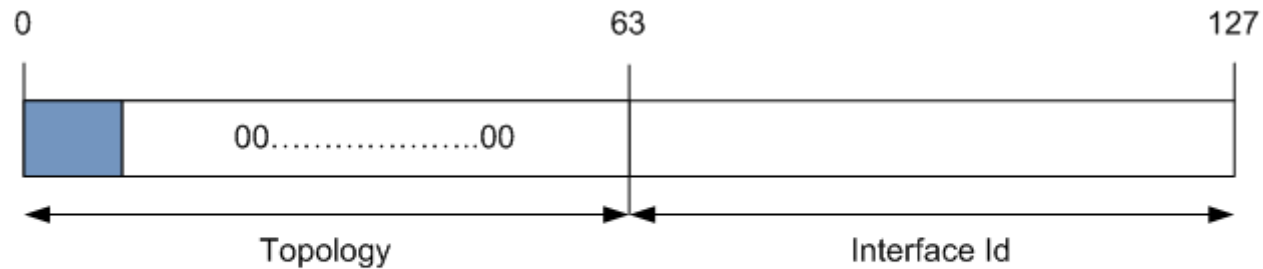
PARTIE I – IPv6


L'ADRESSAGE IPv6

- Site Local et Link Local



 = 111111011 = FEC0

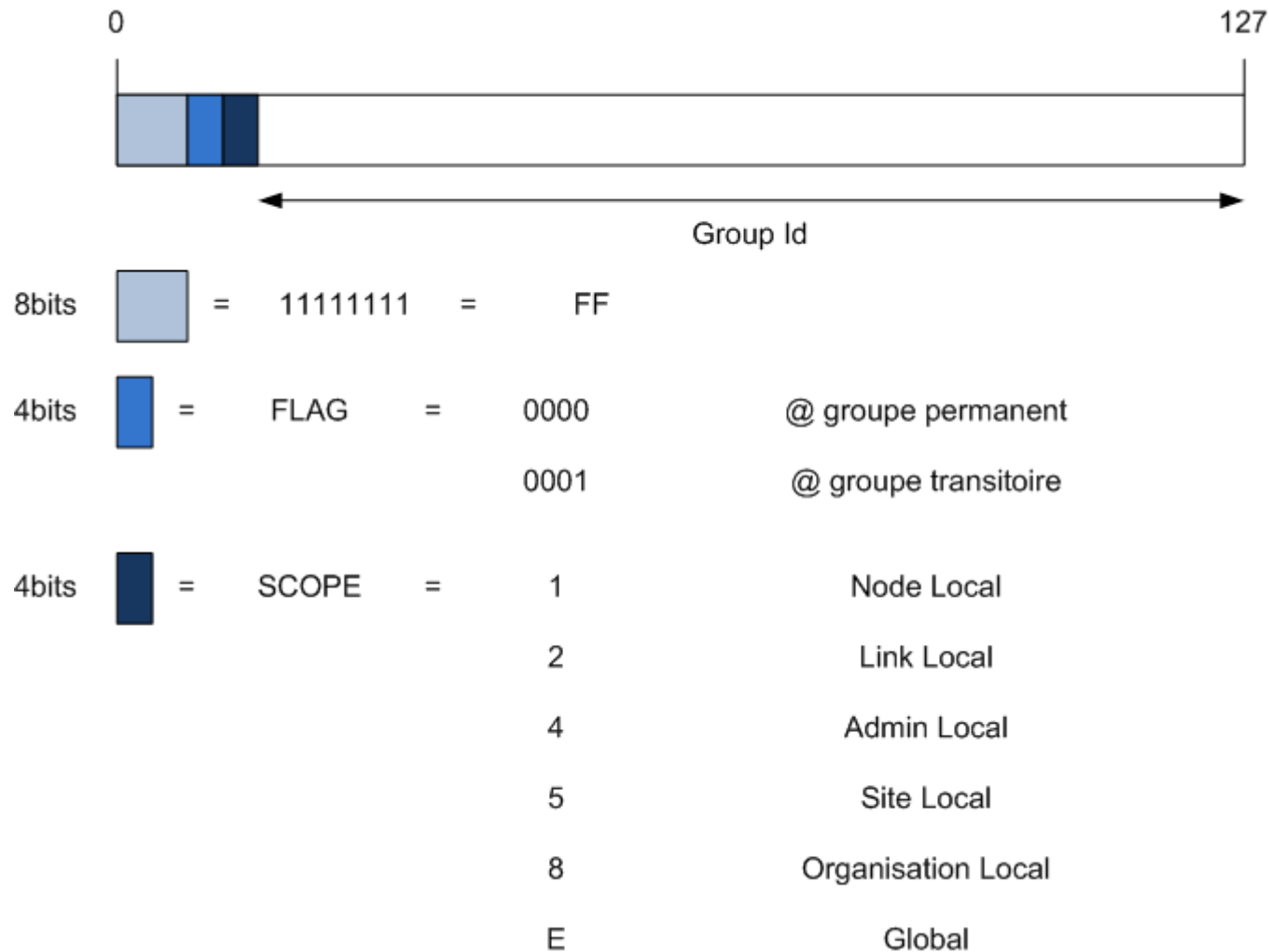


 = 11111010 = FE80

PARTIE I – IPv6

L'ADRESSAGE IPv6

○ Multicast

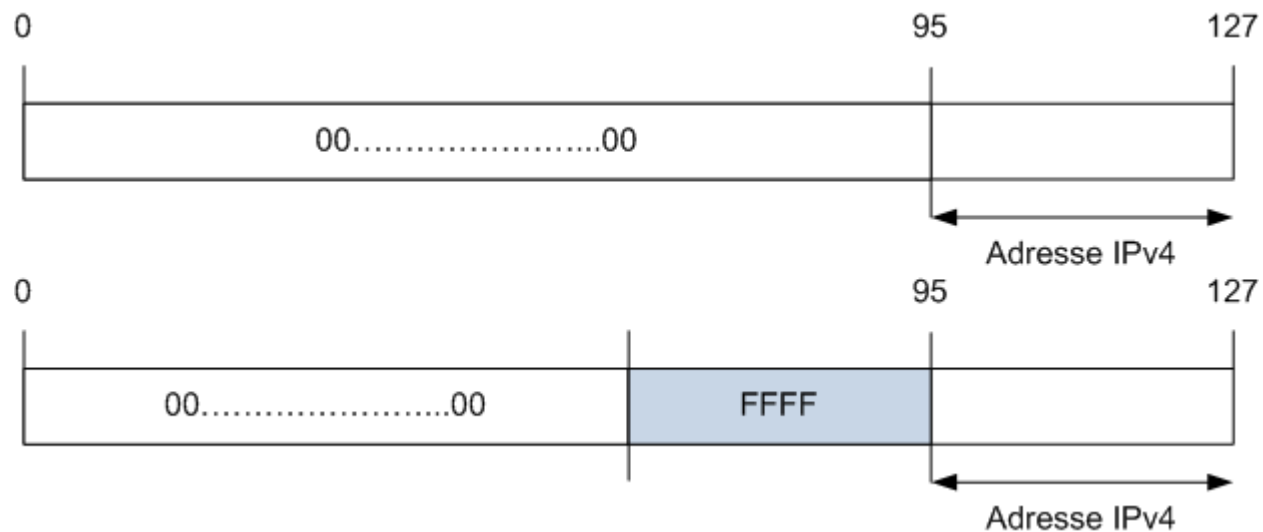


PARTIE I – IPv6

L'ADRESSAGE IPv6

○ Adressage spécifique

- Adresse Compatible => utilisation en mode tunnel
 - Le paquet IPv6 est encapsulé en IPv4 et l'adresse IPv4 destination est celle compatible
- Adresse « Mappée » => utilisation en mode dual stack



PARTIE I – IPv6

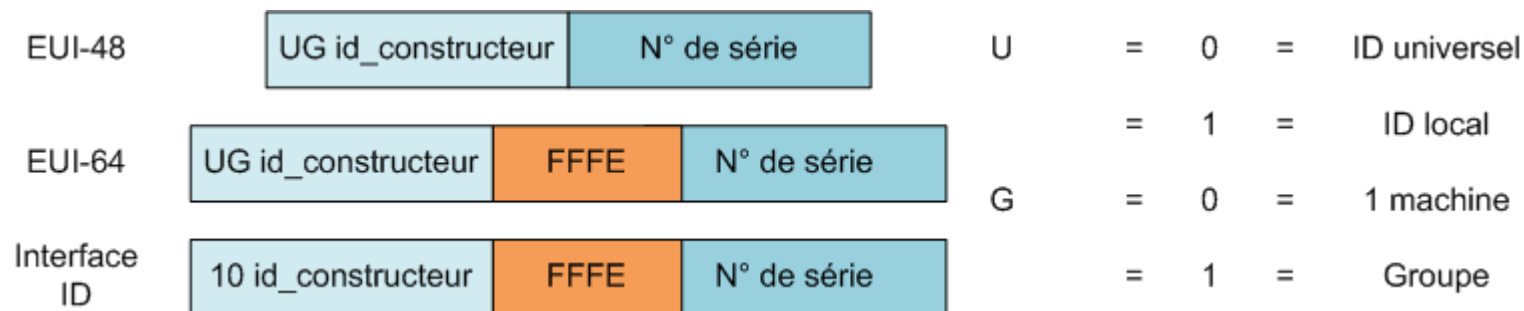
L'ADRESSAGE IPv6

- L'adresse de *loopback*
 - ::1
- L'adresse non déterminée
 - ::
- La notion de masque
 - Principe identique à IPv4
 - Notation abrégée /x

PARTIE I – IPv6

AUTO-CONFIGURATION

- Utilisation de l'identifiant d'interface
 - En fonction de l'adresse MAC de l'interface (Extended Unique Interface – 48)
 - Mais il faut « mapper » 48 bits dans 64 bits



PARTIE I – IPv6

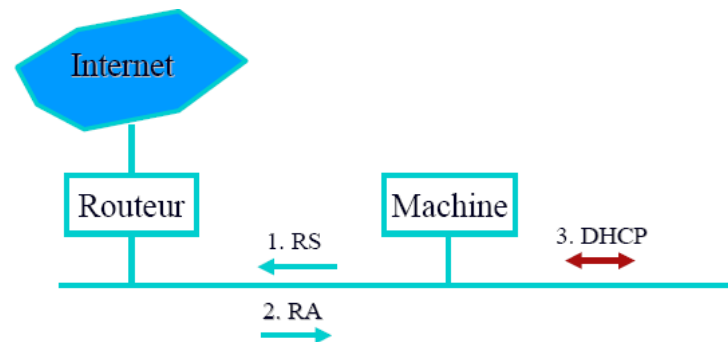
AUTO-CONFIGURATION

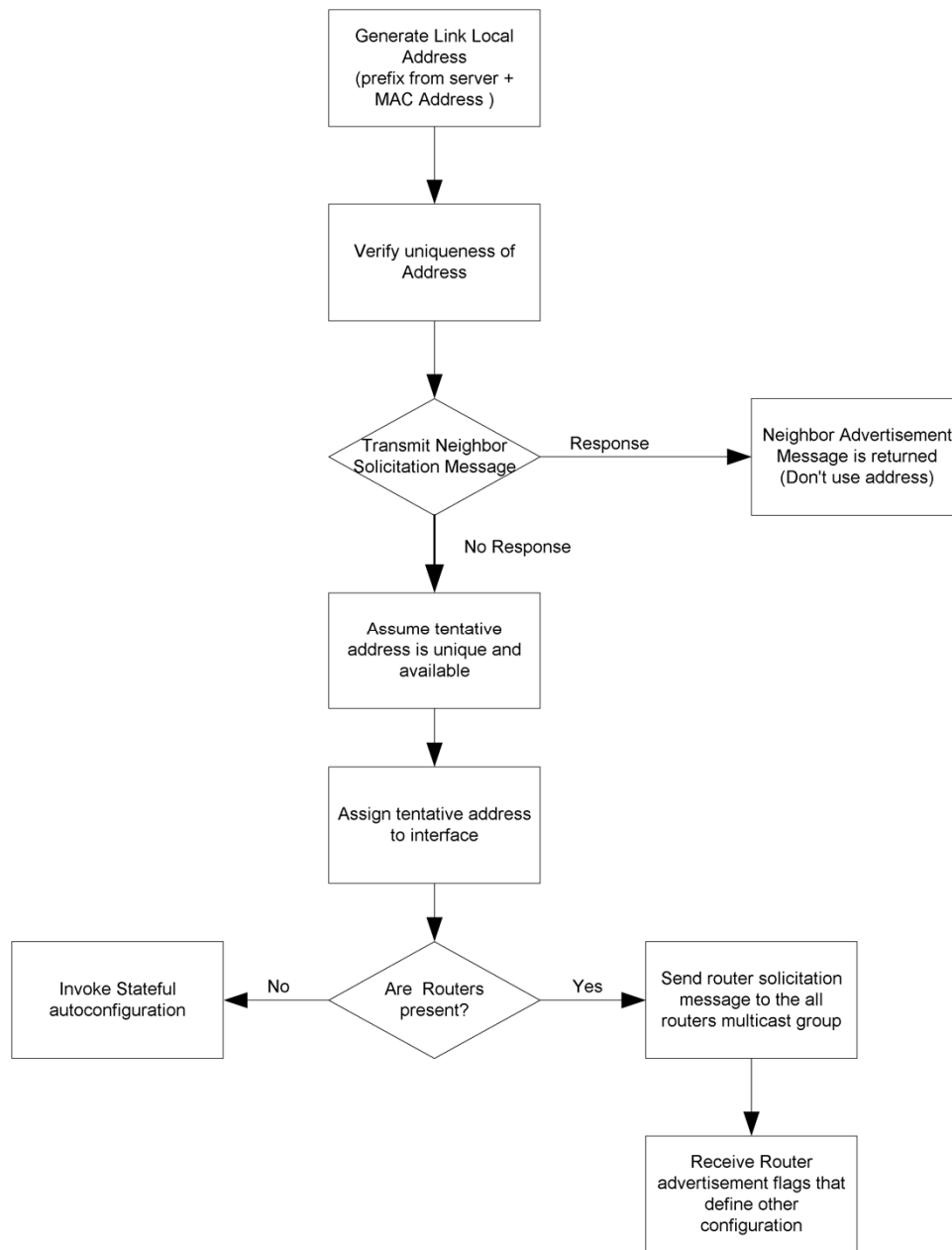
- Neighbor Discovery
 - Utilisation sur le même support physique
 - Principe:
 - découvrir les voisins
 - déterminer les adresses de niveau 2 des voisins (ARP)
 - localiser les routeurs (DHCP)
 - Information et avertissements (ICMP)
 - 5 types de paquets (ICMPv6?)
 - Neighbor Solicitation (NS)
 - Neighbor Advertisement (réponse à une NS)
 - Redirect Pas la bonne route
 - Router Solicitation (RS)
 - Router Advertisement (RA)

PARTIE I – IPv6

AUTO-CONFIGURATION

- Neighbor Discovery
 - Utilisation de messages ICMPv6
 - Router/Neighbor Solicitation
 - Router/Neighbor Advertisement
- Auto-configuration avec serveur
 - DHCPv6
 - Mix BOOTP et DHCP
- Auto-configuration sans serveur
 - Utilisation de la construction d'adresses





PARTIE I – IPv6

« NOUVEAUX » PROTOCOLES

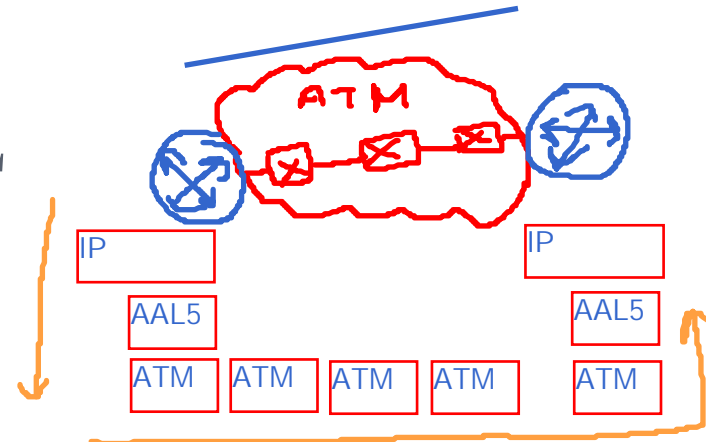
- IPv6 intègre directement certains ajouts à IPv4
 - Path MTU Discovery
 - QoS (mais problème similaire à IPv4)
 - Meilleure gestion de la mobilité (MIPv6 cf. 3eme année)
 - Sécurité
 - Authentification
 - Intégrité
 - Confidentialité

PARTIE II – IP ET TUNNEL

PRINCIPE

○ Tunnel

- Un principe très répandu dans l'interconnexion
 - Cf cours d'interconnexion
 - Exemple de l'ADSL
- Principe
 - Encapsuler un message protocolaire pour passer à travers une autre forme de technologie (ou pas)
 - Construction d'un sur-réseau
 - Invisible pour le protocole encapsulé
- Utilisations
 - Interconnexion de réseaux locaux/privés d'entreprises
 - De manière sécurisé
 - Masquage et inaccessibilité vis-à-vis de l'extérieur
 - Être sur le même réseau local à distance
 - Télétravail...



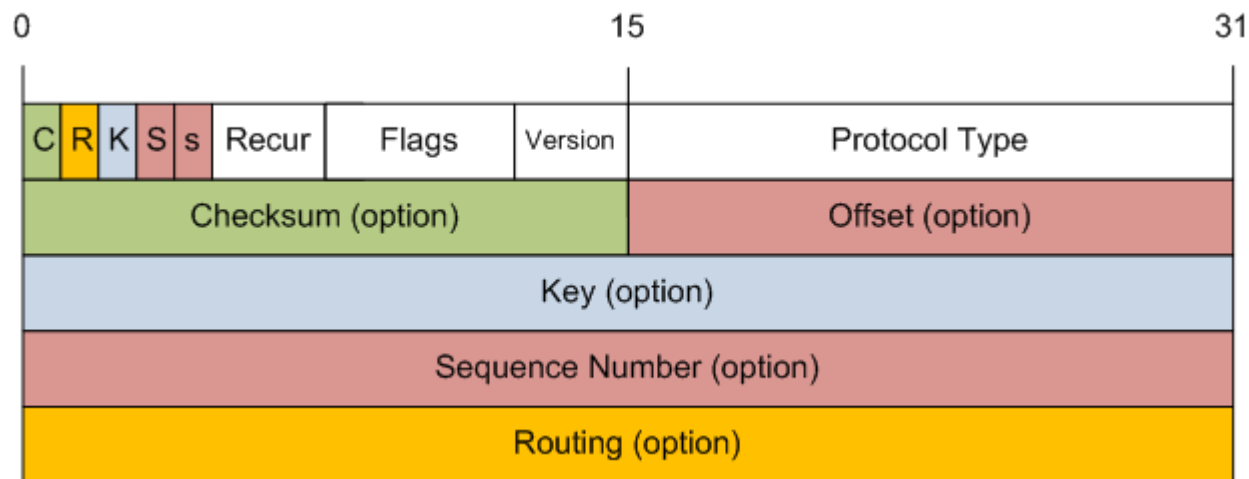
PARTIE II – IP ET TUNNEL

GENERIC ROUTING ENCAPSULATION

○ GRE

- Dernier RFC 2890 en 2000 par CISCO
- Objectif = encapsuler un protocole dans un autre
 - Aussi appelé IP Tunneling
- Un en-tête très simple

Tout ce qui est en couleur est une option,
sans option il y a 4 octets

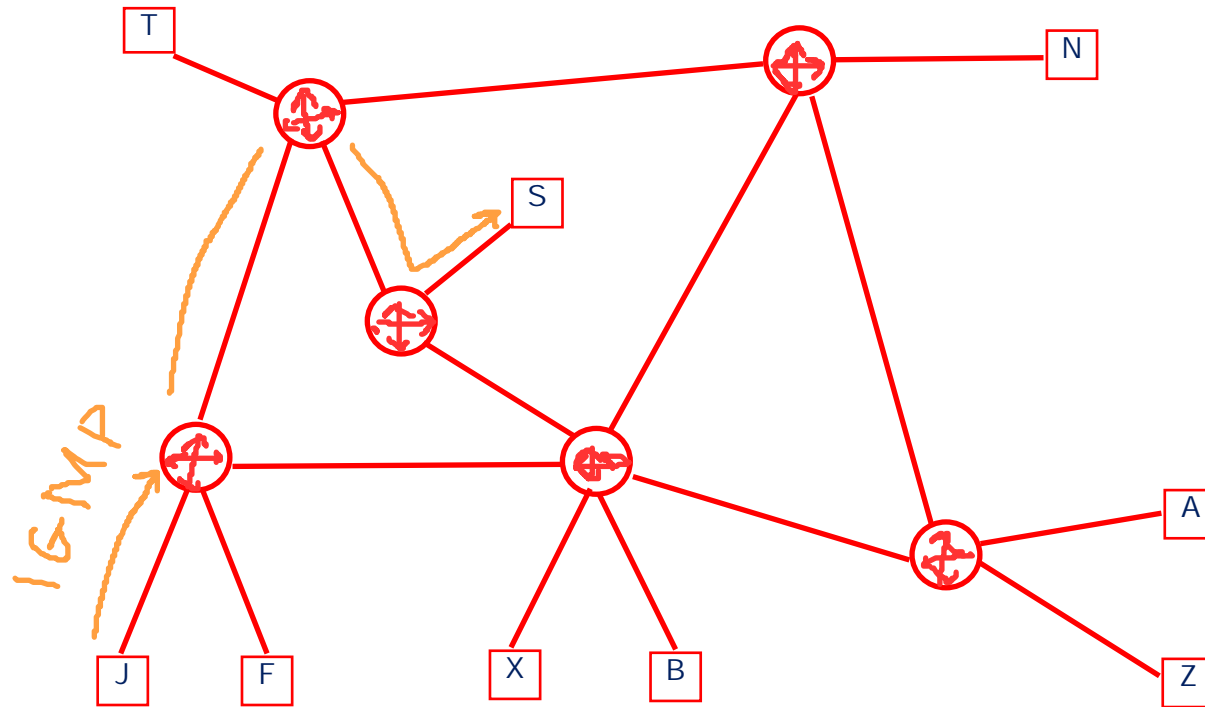


○ Illustration en TP

PARTIE III – MULTICAST

PRINCIPE

○ Illustration Tableau



PARTIE IV – REAL TIME PROTOCOL

PRINCIPE

- RFC 3550
 - Juillet 2003
 - Remplaçant le RFC 1889 de Janvier 1996
- Unidirectionnel
 - Construit pour un flux multimédia
 - Vidéo (Realplayer à la base?)
 - Comment faire pour la voix?
- Protocole de contrôle séparé
 - RTCP
 - Utilisation de Feedback
- Basé sur UDP
 - TCP peut adapté au multimedia

PARTIE IV – REAL TIME PROTOCOL

EN-TÊTE

- RFC 3550
 - Juillet 2003
 - Remplaçant le RFC 1889 de Janvier 1996
- Unidirectionnel
 - Construit pour un flux multimédia
 - Vidéo (Realplayer à la base?)
 - Comment faire pour la voix?
- Protocole de contrôle séparé
 - RTCP
 - Utilisation de Feedback
- Basé sur UDP
 - TCP peut adapté au multimedia