UNIVERSITÉ DE SHERBROOKE

IFT585 - en guise de revue

UNIVERSITÉ DE SHERBROOKE

Couche réseau
Présentation

- *Comment parvenir à destination ?*
  - *sans « route » pré-établie*
  - *avec « route » pré-établie*
- *Une route est-elle un chemin ?*
- *... et autres questions existentielles*

UNIVERSITÉ DE SHERBROOKE

2007-09-12

Couche réseau
Les fonctions

- Relier plusieurs réseaux
- Acheminer les données entre les équipements de différents réseaux
- Contrôler l'état des aiguilleurs et des autres équipements de communication
- Harmoniser certaines caractéristiques d'acheminement telles que
  - schémas d'adressage
  - limites de longueur des éléments de réseau
  - mécanismes d'accès aux réseaux
  - délais d'attente permis
  - mécanismes de reprise d'erreur
  - rapports d'état du réseau
  - techniques d'aiguillage
  - méthodes de contrôle d'accès du réseau
  - modes d'acheminement de la communication

3

UNIVERSITÉ DE SHERBROOKE

2007-09-12

Couche réseau
Aiguillage

Un système d'aiguillage est

- un sous-ensemble d'équipements d'un réseau
- dont la fonction principale est de déterminer le chemin emprunté
- par les éléments de réseau (paquets)
- émis par d'autres équipements

4

UNIVERSITÉ DE SHERBROOKE

2007-09-12

Couche réseau
Connexion (rappel)

- Les services *avec connexion* négocient une entente (la connexion) entre la source et la destination avant de transférer les données. Il y a donc une première étape où la source communique avec la destination pour établir la connexion, une étape intermédiaire où la connexion est utilisée pour le transfert puis une dernière étape où la connexion est rompue.
- Les services *sans connexion* ne négocient aucune entente préalable. La source transmet un élément de réseau qui contient en entête l'adresse de la destination. Il n'y a donc qu'une étape : le transfert.

5

UNIVERSITÉ DE SHERBROOKE

2007-09-12

Couche réseau
Circuits virtuels et datagrammes

- Le *circuit virtuel* réserve un ensemble de liaisons formant un chemin entre la source et la destination. Le chemin entre la source et la destination est en premier lieu fixé puis c'est ce chemin qui sera utilisé pour la transmission des éléments de réseau pendant la durée de la communication.
- Le *datagramme* n'utilise aucune procédure d'établissement préalable de chemin. Les éléments de réseau sont transmis successivement d'aiguilleur en aiguilleur selon la disponibilité des liaisons entre la source et la destination.

6

UNIVERSITÉ DE SHERBROOKE

IPv4
La couche réseau de l'IETF

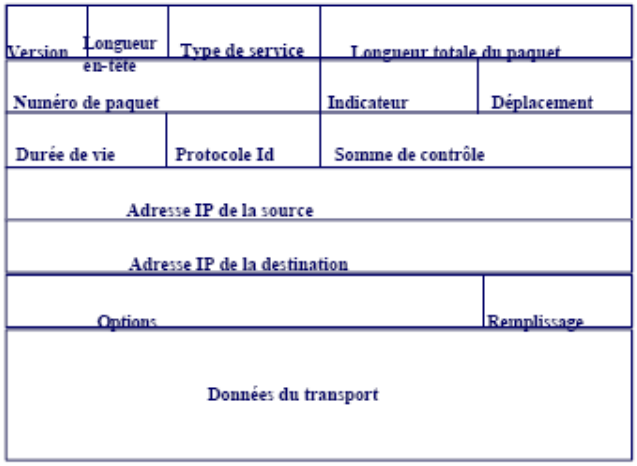
- Définir un schéma d'adressage en deux parties
  - adresse de réseau;
  - adresse d'équipement (au sein d'un réseau).
- Aiguiller le paquet vers une interface en fonction de son adresse de réseau (de destination)
  - Pour chaque paquet,
    - déterminer l'interface en fonction de l'adresse de réseau;
    - en cas d'échec, utiliser l'interface « par défaut ».
- Pour ce faire, pour chaque aiguilleur, définir
  - une liste d'aiguillage (« tableau de routage ») associant une adresse de réseau à une interface privilégiée
  - une interface « par défaut »

UNIVERSITÉ DE SHERBROOKE

IPv4
Les adresses

- Adressage original
  - Système de classes fixes (A..E)
  - Possibilité de diffusion (classe D)
- Adressage sans classes (CIDR)
  - Le sous-réseau
  - Le masque
  - Les bénéfices
    - Diminuer le nombre d'unités par sous-réseau
    - Réduire la taille des domaines de diffusion
    - Mieux structurer l'adressage IP
    - Réduire les tables d'aiguillage

IPv4
L'en-tête du paquet



IPv4
Les champs (1/3)

- Version (4 bits)
  - identification de la version du protocole IP (4, 5 ou 6)
- Longueur (4 bits)
  - longueur de l'en-tête en mots (32 bits)
- Type de service (8 bits)
  - Priorité sur 3 bits (0 la plus faible, 7 la plus forte)
  - Qualité de service sur 3 bits
    - D (1 bit) : faible attente
    - T (1 bit) : flux important
    - R (1 bit) : fiable
  - RUF : 2 bits inutilisés
- Longueur totale du paquet (16 bits)
  - exprimée en octets
- Identificateur (16 bits)
  - numéro permettant d'associer les fragments d'un même datagramme en cas de fragmentation

IPv4
Les champs (2/3)

- Indicateurs (3 bits) :
  - DF : indique si le paquet peut être fragmenté
  - NU : non-utilisé
  - MF : indique si le fragment est le dernier du paquet
- Déplacement (13 bits)
  - indique le décalage du fragment de donnée en multiple de 8 octets par rapport au données transportées dans le datagramme originel. 0 pour un datagramme en 1 seul fragment, ou pour le premier fragment.
- Durée de vie (8 bits)
  - durée maximum de vie du paquet dans le réseau (en seconde)
- Protocole (8 bits)
  - identification du protocole de transport responsable de la charge utile du paquet
- Somme de contrôle (16 bits)
  - code détecteur d'erreur, doit être recalculé à chaque aiguillage

IPv4
Les champs (3/3)

- Adresse IP de la source (32 bits)
  - ...
- Adresse IP de la destination (32 bits)
  - ...
- Options (taille variable entre 0 et 40 octets, en multiples de 4)
  - Chaque option est codée comme suit
    - Code (1 octet) : indique le type de traitement à appliquer aux options
    - Copy (1 bit) : indique si les options doivent être recopiées dans les fragments
    - Classe (2 bits) :
      - 0 : datagramme ou contrôle
      - 1 et 3 réservé
      - 2 mise au point
    - Numéro (5 bits) : nom de l'option dans la classe
    - Longueur (1 octet) : longueur en octets des données de l'option
    - Données de l'option (0 à 37 octets)
    - Remplissage (0 à 3 octets) : pour aligner sur une frontière de 4 octets

IPv4
Les options (1/3)

- Sécurité
- Aiguillage strict
- Aiguillage partiel
- Enregistrement du chemin
- Horodatage

- voir
  - http://www.iana.org/assignments/ip-parameters
  - RFC 2780

IPv4
Les options (2/3)

Copy	Class	Number	Value	Name		Reference
0	0	0	0	EOOL	- End of Options List	[RFC791,JBP]
0	0	1	1	NOP	- No Operation	[RFC791,JBP]
1	0	2	130	SEC	- Security	[RFC1108]
1	0	3	131	LSR	- Loose Source Route	[RFC791,JBP]
0	2	4	68	TS	- Time Stamp	[RFC791,JBP]
1	0	5	133	E-SEC	- Extended Security	[RFC1108]
1	0	6	134	CIPSO	- Commercial Security	[???]
0	0	7	7	RR	- Record Route	[RFC791,JBP]
1	0	8	136	SID	- Stream ID	[RFC791,JBP]
1	0	9	137	SSR	- Strict Source Route	[RFC791,JBP]
0	0	10	10	ZSU	- Experimental Measurement	[ZSu]
0	0	11	11	MTUP	- MTU Probe	[RFC1191]*
0	0	12	12	MTUR	- MTU Reply	[RFC1191]*
1	2	13	205	FINN	- Experimental Flow Control	[Finn]
1	2	30	222	EXP	- RFC3692-style Experiment (**)	[RFC4727]

IPv4
Les options (3/3)

Copy	Class	Number	Value	Name	Reference
1	0	14	142	VISA - Expermental Access Control	[Estrin]
0	0	15	15	ENCODE - ???	[VerSteeg]
1	0	16	144	IMITD - IMI Traffic Descriptor	[Lee]
1	0	17	145	EIP - Extended Internet Protocol	[RFC1385]
0	2	18	82	TR - Traceroute	[RFC1393]
1	0	19	147	ADDEXT - Address Extension	[Ullmann IPv7]
1	0	20	148	RTRALT - Router Alert	[RFC2113]
1	0	21	149	SDB - Selective Directed Broadcast	[Graff]
1	0	22	150	- Unassigned (Released 18 October 2005)	
1	0	23	151	DPS - Dynamic Packet State	[Malis]
1	0	24	152	UMP - Upstream Multicast Pkt.	[Farinacci]
0	0	25	25	QS - Quick-Start	[RFC4782]
0	0	30	30	EXP - RFC3692-style Experiment (**)	[RFC4727]
0	2	30	94	EXP - RFC3692-style Experiment (**)	[RFC4727]
1	0	30	158	EXP - RFC3692-style Experiment (**)	[RFC4727]

IPv4
Les protocoles auxiliaires

- ARP - Address Resolution Protocol
  - Résolution d'adresse IP en adresse MAC
- ICMP - Internet Control Message Protocol
  - Gestion des messages du protocole IP
- IGMP - Internet Group Management Protocol
  - Protocole de gestion de groupes (de diffusion)
- RARP - Reverse Address Resolution Protocol
  - Résolution d'adresse MAC en adresse IP (v0)
- BOOTP – Boot Protocol
  - Configuration dynamiques des adresses (v1)
- DHCP – Dynamic Host Control Protocol
  - Configuration dynamiques des adresses (v2)

UNIVERSITÉ DE SHERBROOKE

IPv4
NAT

- La planche de salut...
- et la condamnation à mort!
- Principes
  - utilisation des numéros de port de transport (TCP,UDP) pour étendre l'adressage IP
  - traduction à l'aller et au retour
  - problèmes
    - point de défaillance unique
    - éclatement des couches (y compris application!)
    - alouette!
    - voir Tanenbaum ou Kurose

UNIVERSITÉ DE SHERBROOKE

2009-04-18

La mise à jour des tables d'aiguillage
Catégories

- Classe
  - inondation
  - statique
  - dynamique
    - vecteur de distance (VC)
    - état de lien (EL)
    - distance et chemins (DC
- Algorithme
  - Bellman-Ford (n^3)
  - Ford-Fulkerson $O(n^3)$
  - Dijkstra $O(a \cdot n)$
- Déclenchement
  - Temporisation
  - Événementiel
    - topologie
    - mesure
- Support
  - IP, TCP
  - Universel
- Mesure
  - unique vs multiple
  - statique vs dynamique
  - homogène vs hétérogène
- Structure
  - aucune
  - hiérarchique OSI (IS)
  - hiérarchique IETF (AS)
- Portée
  - Interne
  - Externe
  - Hiérarchique

18

UNIVERSITÉ DE SHERBROOKE

La mise à jour des tables d'aiguillage Histoire

Protocole	Org	Type	Portée	Algo	Support	Déclenchement	Mesure	Particularités
RIP	*	VD	Interne	Ford	Rés-U	Tempo(30*[1..3])	USH	Split Horizon (SH)
RIP-2	IETF	VD	Interne	Ford	Rés-U	idem+Évé(mesure)	USH	SH+Poison
IRGP	Cisco	VD	Interne	Ford	Rés-U	Tempo(90*[1..4])	MDH	SH+Poison
EIRGP	Cisco	VD	Interne	Ford	Rés-U	idem+Évé(mesure)	MDH	idem+DUAL
IS-IS	ISO	EL	Hiérarchique	Dijkstra	Rés-U	Évé(topo,mesure)	MDH	m-niveau
OSPF	IETF	EL	Interne	Dijkstra	IP	Évé(topo,mesure)	MDH	3-niveaux
IDRP	ISO	DC	Externe	Libre	Rés-U	Évé(topo,mesure)	MDH	m-niveau(V+ag)
BGP-4	IETF	DC	Hiérarchique	Libre	TCP	Évé(topo,mesure)	USH	m-niveau(16)

UNIVERSITÉ DE SHERBROOKE

La mise à jour des tables d'aiguillage Version limitée à l'IETF

	RIP	RIP-2	IRGP	EIRGP	OSPF
adressage	par classe	CIDR	CIDR	CIDR	CIDR
infini	16	16	16..255	16..255	2^{32}-1
mesure (métrique)	unique, statique, homogène	unique, statique, homogène	multiple, dynamique, homogène	multiple, dynamique, homogène	multiple, dynamique, homogène
identification du suivant	non	oui	oui	oui	oui
authentification	aucune	très faible	aucune	aucune	faible
multicasting	non	oui	oui	oui	oui
bande passante	très grande	grande	moyenne	faible	faible
convergence	très lente	lente	moyenne	rapide	rapide
répartition de charge	absente	absente	partielle	complète	partielle

UNIVERSITÉ DE SHERBROOKE

2009-04-18

IPv4
Une synthèse

- L'épuisement des adresses
- La fragmentation
- La qualité de service
- L'amélioration de la diffusion (broadcast et multicast)
- La performance
  - simplification du protocole
  - simplification de l'entête
- La mobilité
- L'interopérabilité
  - présente
  - future

21

UNIVERSITÉ DE SHERBROOKE

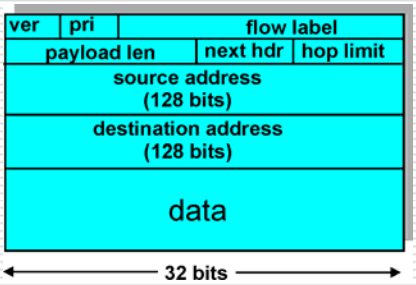
IPv6
La tentative de sauvetage

- *Objectifs pris en compte*
  - *adresses hybrides de 128 bits*
  - *simplification de l'en-tête*
  - *mécanisme extensif d'options*
  - *sécurisation*
  - *qualité de service*
  - *compatibilité*
- Objectifs déclassés
  - réduction de la taille des tables d'adressage
  - mobilité

UNIVERSITÉ DE SHERBROOKE

IPv6
Nouvel en-tête

- Mot 1
  - version (4)
  - classe (8)
  - étiquette (20)
- Mot 2
  - longueur (16)
  - prochain entête (8)
  - limite de sauts (8)
- Source (4 mots)
- Destination (4 mots)
- Options chaînées (presque 64 Ko)



UNIVERSITÉ DE SHERBROOKE

Couche de transport
Rappels

- APDU
  - Message (message)
- TPDU
  - Segment (segment)
- NPDU
  - Paquet (packet)
- LPDU
  - Trame (frame)
- Échange (dialogue)
- Communication
- Connexion
- Circuit
- Lien
- Canal
- Voie de transmission

UNIVERSITÉ DE SHERBROOKE

Couche de transport
Services

- Acheminement de messages point à point
- Transmission avec ou sans connexion
- Livraison fiable ou non
- Contrôle de débit
- Qualité de service
- Traitement des erreurs

UNIVERSITÉ DE SHERBROOKE

Couche de transport
Différentiation Réseau - Transport

- Hébergement
  - Réseau -> sous-réseau
  - Transport -> équipement
- Indépendance des applications p/r aux réseaux
- Capacité de traitement des erreurs

UNIVERSITÉ DE SHERBROOKE

Couche de transport
Interface minimale

- listen
- connect
- disconnect
- send
- receive

UNIVERSITÉ DE SHERBROOKE

TCP – une couche de transport de l'IETF
Interface typique (Berkeley)

- socket
- bind
- listen
- accept
- connect
- close
- send
- recv (receive)

UNIVERSITÉ DE SHERBROOKE

TCP
État d'une connexion

- états.com = (inoccupé, établi)
- actions = (établissement, déconnexion)
- états.serv = actions x (passif)
- états.client = actions x (actif)

- au total au moins 6 états, TCP en modélisera 11 dont 6 pour la seule déconnexion!

UNIVERSITÉ DE SHERBROOKE

TCP
Adressage

- adresse réseau (NSAP) = adresse IP
- adresse transport (TSAP) = adresse IP + port
- stratégies
  - directe
  - préconnexion (serveur de processus)
  - annuaire (serveur de noms)

UNIVERSITÉ DE SHERBROOKE

TCP
Connexion

- problème des doublons
- stratégies
  - limiter la taille du sous-réseau
  - séquencement (panne)
  - TTL (bon premier effort)
  - estampille (synchro)
  - Tomlinson

UNIVERSITÉ DE SHERBROOKE

TCP
Déconnexion

- problème de terminaison

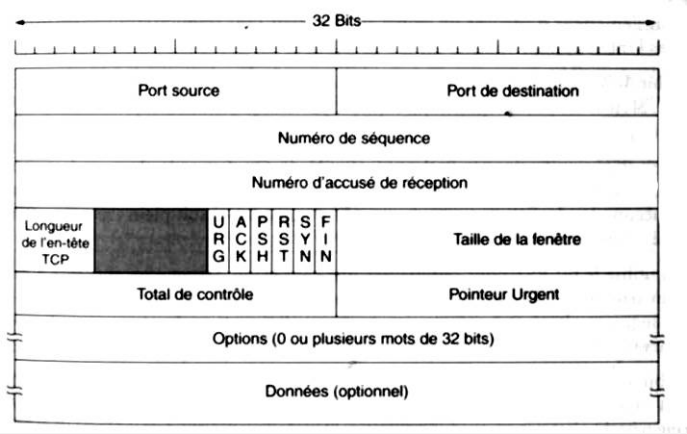
UNIVERSITÉ DE SHERBROOKE

TCP
Contrôle de débit

- Tampons
  - chaînés fixes
  - chaînés variables
  - circulaires
  - ... la sécurité sans la performance
- Références
  - directe
  - indirecte
  - ... la performance sans la sécurité

UNIVERSITÉ DE SHERBROOKE

TCP
Format de l'en-tête



UNIVERSITÉ DE SHERBROOKE

TCP
Champs de l'en-tête

- source (16)
- destination (16)
- no séquence (isn) (32)
- no accusé de réception (32)
- taille en-tête TCP (4)
- indicateurs (6+6)
- taille de fenêtre (16)
- somme de contrôle (16)
- pointeur urgent (16)

- FIN :
  terminer la connexion
- SYN (synchronisation) :
  établir la connexion
- RST (reset) :
  réinitialiser la connexion
- PSH (push) :
  pousser les données dans le « pipe » de l'application.
- ACK (acknowledge) :
  prendre en compte le champ numéro d'accusé de réception
- URG (urgent) :
  prendre en compte le pointeur urgent

UNIVERSITÉ DE SHERBROOKE

TCP – précisions [0]

- isn (4 ms)
- option « MSS »
- URG vs PSH
- taille de la fenêtre (16 bits)

- fin de liste (0)
- noop (1)
- max segment size (2)
- window scale factor (3)
- timestamp (8)

UNIVERSITÉ DE SHERBROOKE

TCP – précisions [1]

- segmentation
  - théorique : 64 Ko
  - pratique : MTU, donc moins de 1,5 Ko
  - problématique de consolidation
- séquencement des octets sur 32 bits
  - 10 Mbps -> 3600 s >> 2MSL
  - 100 Mbps -> 360 s > 2MSL
  - 1 Gbps -> 36 s < 2MSL
  - 10 Gbps -> 3,6 s << 2MSL

UNIVERSITÉ DE SHERBROOKE

TCP – précisions [2]

- (window size = 0) => arrêt de transmission
- 2 exceptions
  - URG
  - réannoncer window size

UNIVERSITÉ DE SHERBROOKE

TCP – précisions [3]

- Congestion : transmission vs réception
- Loi de conservation des paquets
- Double fenêtrage
  - slow start (exp)
  - threshold (seuil)
- Envoi d'un octet à la fois : Naggle
  - exemple : saisie
  - premier (temporisation, 50% segment)
  - désactivation (socket) [X Window, ESC]
- Consommation d'un octet à la fois : Clark
  - exemple : oscillation des fenêtres
  - min libre (50%, taille d'un segment)
  - désactivation (socket)

UNIVERSITÉ DE SHERBROOKE

TCP – précisions [4]

- réinitialisation
  - port inexistant
  - demande explicite (fin)
- détection des connexion mi-ouverte
- connexion simultanée
- déconnexion simultanée

UNIVERSITÉ DE SHERBROOKE

TCP - protocole

- 3WHS
- 2WC
- 30 s < MSL < 120 s
- MSL : maximum segment lifetime
- 2MSL : temps d'aller-retour le plus long

- closed
- listen
- syn rcvd
- syn sent
- established
- fin wait 1
- fin wait 2
- timed wait
- closing
- close wait
- last ack

UNIVERSITÉ DE SHERBROOKE

TCP – diagramme d'états