

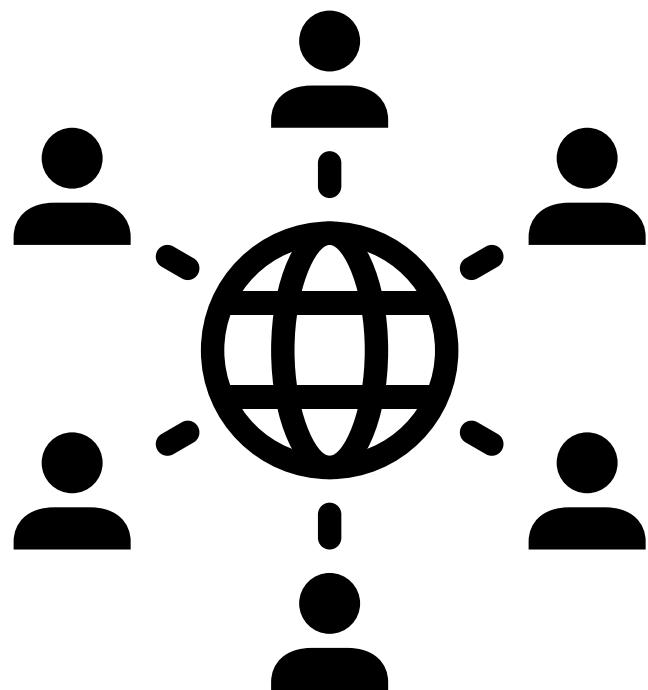
ARCHITECTURE DES RESEAUX

TCP IP

SEMESTRE 7

2020 - 2021

Fiches de révisions



TCP/IP - Interaction entre la partie de protocoles des 4 couches et les supports de transmission

Modèle OSI / TCP

Rappel

Modèle TCP/IP Modèle OSI

Application

7 Application

Transport

6 Présentation

Internet

5 Session

Accès

4 Transport

réseau

3 Réseau

2 Liaison de données

1 Physique

application réseaux

formatage et cryptage

établissement et maintien

transport de bout en bout

envoi et routage des paquets

délimitation des infos

transmission binaire

Modèle TCP/IP

Intercommunication des réseaux

L'intercommunication permet de gérer plusieurs réseaux présentant des différences physiques ou protocolaires afin de permettre la communication entre leurs entités.

Intercommunication de niveau 3 (couche réseau du modèle OSI)

+ masquer l'hétérogénéité des supports en les gérant

+ permettre un service de communication unique

⇒ IP fournit aux supports variés et offre des services à la couche 4.

Communication paquets vs communication circuits

PAQUETS

+ un message à transmettre est découpé en paquets composant la portion du message découpé, des informations d'adresses et autres informations de contrôle

- + Chaque paquet est ensuite envoyé vers sa destination en utilisant une route d'acheminement

CIRCUITS

- + négociation et construction d'un chemin unique exclusif d'une machine A à une machine B
- + le chemin ainsi créé perdure jusqu'à la clôture du dialogue
- + établissement physique des connexions lors de la construction des circuits

Mode connecté vs mode non connecté

connecté : la transmission s'effectue en mode connecté, tous les paquets du message vont suivre le même chemin

non connecté : aussi appelé mode datagravimme dans lequel les paquets ne vont pas tous suivre le même chemin, et la station réceptrice devra permettre les paquets dans le bon ordre pour reconstituer le message

Structure d'un paquet ethernet 802.3

0x0800 - IPv4					
Préambule	S F	Adresse destination	Adresse source	Longueur données	F C
	D	destination	source	Type	S
7 oct	1 oct	6 oct	6 oct	2 oct	46 à 1500 oct 4 oct

Classes d'adresse

- Classe A de 1.x.x.x à 127.x.x.x
- Classe B de 128.0.x.x à 191.255.x.x
- Classe C de 192.0.0.x à 223.255.255.x

TCP - IP

Notes 2

- Classe D de 224.0.0.0 à 239.255.255.255
- Classe E de 240.0.0.0 à 255.255.255.255

Résolution d'adresse

Les entités réseau sont désignées par leur adresse de niveau 3, utilisant d'un réseau physique pour l'acheminement d'un datagramme, identification des entités sur le réseau physique par leur adresse de niveau 2.

⇒ Objectif : obtenir l'adresse de niveau 2 d'une entité à partir de son adresse de niveau 3.

⇒ Solutions:

- + fonction de traduction simple, sur un réseau physique donné
- + table de traduction statique (volumineuse, difficile à maintenir)
- + mécanisme de découverte à l'aide d'un protocole réseau
- + solutions hybrides (ARP)

Protocole ARP

Adresse Resolution Protocol

PRINCIPE:

- + vérification de l'existence de la correspondance entre adresse IP et adresse physique dans la table dynamique
- + En cas d'absence:
 1. envoie d'une requête ARP Request (who has) en diffusion générale (broadcast) sur le réseau physique
 2. réception et traitement de la réponse par toutes les entités du réseau, l'unité cible répond (is-at)

GESTION DE LA TABLE DYNAMIQUE DE RÉSOLUTION

- + collecter des informations sur le réseau pour éviter les requêtes inutiles
- + conserver les correspondances acquises suffisamment longtemps pour éviter de synchroniser le réseau
- + ne pas les conserver trop longtemps pour limiter la taille des tables et éviter les entrées obsolètes

STRUCTURE DU PAQUET

- 2 Hardware type
- 2 Protocole type
- 2 Hardware Length m Protocole Length m
- 2 Operation code
- m Sender Hardware Address
- m Sender Protocol Address
- m Target Hardware Address
- m Target Protocol Address

TCP/IP - Protocole de la couche réseau (IP/ICMP) Réseau 3

PRINCIPE DE FONCTIONNEMENT DU PROTOCOLE IP

- + Acheminement "au mieux"
- + Pas de protection contre perte de paquet IP, duplication de paquets, changement de séquence
- + Possibilité de destruction des datagrammes (nourrir, défaillances, congestion)
- + Envoyé au max d'un rapport d'erreur (ICMP). Pas de la destruction d'un datagramme IP.

FONCTIONNALITÉS NÉCESSAIRES

1. Limiction de la durée de vie des datagrammes
 - ↳ duplication possible des datagrammes et acheminement max garantie
 - ↳ temps de transit à priori inconnu dans le réseau
 - ↳ accessibilité de la destination d'un datagramme inconnu à cause du max nom commun.
 - ⇒ existence potentielle de datagrammes "envois" pouvant conduire à l'empruntage du réseau
2. Qualité de service (QoS)
 - ↳ qualité de service possible, mais non obligatoire, en fonction des réseaux empruntés.
 - ↳ indication de la priorité des informations transportées ou de la nature du service souhaité
3. Fragmentation des datagrammes et reassembly
 - ↳ adaptation de la taille des datagrammes MTU des

supports empêtrés : fragmentation par la source et pas
nouvelles intérmédiaires

↳ reconstitution du datagramme d'origine : nécessité d'un
réassemblage réservé au destinataire final du datagramme

4. Routage

- ↳ principalement par la destination : choix de la
direction d'un datagramme à l'aide de son
adresse de destination et de la table de routage
- ↳ occasionnellement par la source : utilisation des
options permettant de fixer, de manière plus
ou moins rigide, la route d'un datagramme

Protocole IP:

Versoem : versoem du protocole utilisé (IPv4)

Internet header length : longueur de l'en-tête

Total Length : longueur totale du datagramme

Time to live : durée de vie restante du datagramme

Protocol : numéro du protocole auxquelles appartiennent les
données

Header checksum : total de contrôle de l'en-tête

Source address : adresse IP de l'entité source

Destination address : adresse IP de l'entité destination

Identification : permet de créer un unique identifiant
pour un datagramme

Flags : fragmentation

o DF MF



Offset : position, en multiples de 8 octets, du
premier octet de données de ce fragment parmi
l'ensemble des octets du datagramme complet.

Differentiated Service (DS) [RFC2474]

réseaux

- Support pour la politique de qualité de service
- Differentiation
- Champ commun à IPv6.

128

Routage pour la destination

- en fonction du réseau de destination du destinataire et à l'aide de tables de routage
- compatibilité entre le numéro du réseau de l'émetteur et le numéro de réseau de destination grâce à l'utilisation des classes d'adresses
- choix entre l'échelonnement direct et l'échelonnement par nœud / choix du nœud suivant (fonction de routage élémentaire pour tout hôte d'un réseau TCP/IP)

Les réseaux tout à "0" ou tout à "1" dans le sous-réseau sont possibles mais peuvent créer des ambiguïtés. Les bits du masque identifiant un sous-réseau et machine doivent être préférablement contigus.

VLSM (variable Length subnet masks)

- Évite la rigidité du masque fixe qui impose le nombre de sous-réseaux et le nombre de machines pour sous-réseau.
- Division d'un espace IP en sous-réseaux successifs.
- Permet de masquer les informations de routage entre groupes de sous-réseaux.

IPV6 NEIGHBOR DISCOVERY

- Protocole ND utilisé pour gérer les machines partageant un même support physique
- Regrouper plusieurs IPV4
- IP permet de :
 - localiser les voisins
 - découvrir le ou les prefixes du réseau
 - découvrir les paramètres du réseau
 - détecter la duplication d'adresse
 - déterminer si une machine est devenue inaccessibile
 - déterminer l'adresse réseau d'une machine à partir de son adresse IPV6
 - permet de configurer automatiquement une adresse IPV6
 - indiquer un meilleur chemin

OPTIONS DANS IPV4

Informations et commandes optionnelles concernant le protocole IP

Options en fin d'en-tête IP : 0 à 40 octets

- ↳ pas de séparation particulière
- ↳ possibilité d'ajouter le début de chaque option après un multiple de 4 octets en partant du début de l'en-tête
- ↳ bounage éventuel en fin de liste pour atteindre un nombre multiple de 4 dans l'en-tête

Fonction générique d'une option IP : TSV (TYPE-LENGTH-VALUE)

- ↳ TYPE : 1er octet indique de l'option
- ↳ Length : 2ème octet longueur totale de l'option, y compris option-type et option-length, exprimée en octets
- ↳ Value : autres octets : données proposées à l'option

Protocole ICMP (Internet Control and Error message protocol)

- But : supervision du fonctionnement IP (réponds d'erreurs, demandes d'informations)
- Éléments de protocole
 - ↳ utilisation des services IP
 - ↳ éléments de protocole spécifiques à chaque fonction
- Format
 - ↳ 1er octet : type
 - ↳ reste : dépend du type

TCP/IP : Les couches Transport UDP/TCP

La couche transport

Ces couches "l'issiom de données" et "transport" s'occupent tout particulièrement d'assurer le transport de la charge utile entre différents points d'un réseau de communications. L'objectif de la couche transport est la transmission de données de bout en bout, la vérification que les données arrivent dans l'ordre correct (TCP par exemple) et déterminer à quelle application chaque donnée est destinée.

UDP (un datagramme protocole)

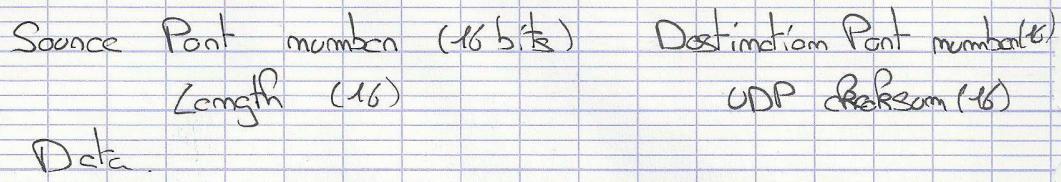
Protocole de transport sans connexion de service applicatif.

- émission de messages applicatifs : sans établissement de connexion ou préable.
- l'arrivée des messages ainsi que l'endommagement ne sont pas gérés.

Ces points permettent l'identification du service et la gestion du multiplexage.

Les adresses IP désignent les machines entre lesquelles les communications sont établies.

Structure d'un datagramme UDP



TCP Transmission control protocol

résumé

- Communication fiable en mode connecté
- Fiabilité : illustration assurée par le service
- Transport transparent : découpage en segments
- Connexions bidirectionnelles et simultanées

Génération de numéros de message ainsi que de l'ordonnancement

Connexion

Une connexion de type circuit virtuel est établie avant que les données ne soient chargées : appel + négociation + transferts

Une connexion = une paire d'extrémités de connexion

Une extrémité de connexion = couple (adresse IP, port)

La connexion se fait en deux étapes

1. une application effectue une ouverture passive
2. une autre application effectue une ouverture active.

Segmentation

Les données transmises à TCP constituent un flux d'octets de longueur variable. TCP divise ce flux de données en segments en utilisant un mécanisme de fragmentation.

Un segment est emballé dans un datagramme IP.

Contrôle d'accès à UDP, TCP garantit l'intégrité des messages, c'est à dire qu'en cas de perte les deux extrémités sont prévenues. Ce concept repose sur les techniques d'acquittement, S écrit M vers D et attend A qui ayant d'envoyer M+1

Ouverture d'une connexion

Ouverture en 3 phases permettant une synchronisation
fiable des numéros de séquence initiaux (pas de débris ouvertures)
et pas de confusion)

Fenêtre

La technique d'accrétion simple présente les performances,
on envoie donc T messages avant de recevoir l'accrétion.
La fenêtre glissante permet d'optimiser la bande
passante.

Congestion

TCP contrôle de bout en bout le flux et contrôle aussi
la congestion liée à l'internumérotation. La congestion correspond
à la saturation de murs dans le réseau provoquant
des défauts d'échappement de datagrammes jusqu'à
un point éventuel. \Rightarrow Algorithme de congestion