

Résumé : Réseau et télécommunication

Introduction

- Réseau :
- moyen matériel et logiciels
 - offrir un service
 - = finalité → technique
→ qualité de service

Classification : fonctionnelle (téléphone, ...)

- type de transmission (Pbt / WiFi)
- mode de diffusion (1:1 1:n n:1)
- échelle (PAN, LAN, MAN, WAN)
- accès (public / privé)
- temporelle

[slide 1 Architecture de QoS]

applications, organisation, technologie

architecture : client - serveur

- Peer to Peer
- Multi-Tiers (couches client, service, données)

Si connection tous à tous : $\frac{N(N-1)}{2}$ → boson de commutateur.

Communauté → Circuits : Pas de stockage, ressource dédiées, coûts distance + durée

→ messages : asynchrone, de nœud en nœuds, transfert asynchrone

Paquets : Messages coupé en paquet

Pas de stockage intermédiaire

Pas d'ordre

Protocole : défini

format et ordre des messages échangés + actions qui en résultent

Interface / Implementation

→ couches : ensemble hiérarchique destiné à accompagner une tâche ou rendre un service

communications avec couches adjacentes

(encapsulation) (adjacence via header)

une en tête

[slide Modèle OSI] 7

[Modèle TCP] 5

La Transmission de données

court distance signal court
longue distance module + signal signalé

Représentation: analogique: continues, constante
digitale: numérique, binaires, binaire/gramme
discrettes.

Codage: 1 octets = 8 bits

ASCII = 7 bits

Coder P en $n = \log_2 P$ bits

UNICOM = 16 bits

Entropie: quantité moyenne d'information apportée par la connaissance d'un état

Compression:

$$Q = \text{quotient de compression} = \frac{\text{taille avant}}{\text{taille après}}$$

$$T = \text{taux} = \frac{1}{Q}$$

$$G = \text{gain} = (1 - T) \cdot \% \quad \text{ou} \quad G = \frac{T}{1-T} \cdot \%$$

Detection d'erreur: \rightarrow facteur physique

Méthode: \rightarrow facteur humain
par écho
par répétition
par code
par calcul

Type: parallèle / série

Temps: horloges / asynchrone / synchrone

Bande passante: Ondes / basse bande / haute bande

Support: (optique)
fibre, cuivre, ondes

Traffic: taux d'activité: transmission \uparrow vs réflexion (caissie)
Activité / appropriation du support

Intensité: Appropriation du support / temps

Concentration: $n \rightarrow 1$

multiplexeur: $n:1 \leftrightarrow 1:n$

Multiplexage \rightarrow spatial (canaux) fréquences
 \rightarrow temporel (chacun son tour)

Réseau local et télécommunication

①

Réseau local (LAN)

Paquets: TCP: Segment

IP: Datagramme

Ethernet: Frame (frame)

↓ encapsulation
entête + suffixe

LAN: géographiquement proche
chacun connaît son chemin
optimiser efficacité

Topologie → logique : flux des frames
→ physique

étoile: connect/déconnect mais single point of failure

ring: déconnecté

bus: possibilité de fragmentation du réseau

adresse physique: MAC

unicast: 1:1

broadcast: tous (utilise "PQ" de tous)

multicast: tous qui sont dans un groupe

frame Ethernet (technologie bus) → étoile (switched Ethernet)

Preamble	adresse destination	adresse source	type de frame	Donnees	CRC
(synchronisation)				~1500 bytes max	even

CSMA/CD détecter si le support est libre avant de transmettre

Collision Performance ↳ si gare → si collision

↑ si collision attendre 2x plus

Token Ring

message spécial - jeton/token

On ne peut émettre que si on a le jeton

Debit nominal:

si cher → débit utile ↓ car plus de collisions

Débit limite filiale
du CAN

possible de
calculer temps
maximum de délais

LAN étendue

- Segments :
 - o distance min et max (100m 10baseT)
 - o nombres de noeuds limité

osi 1 Repeater : pour allonger la distance (renforce signal atteint)

Ethernet Max 5 segment, 4 repeaters, 3 segments par défaut

- o crée des délais
- o même domaine de collision

osi 1 hub : plusieurs noeud joind (partage)

(extension fibre optique)

osi 2 point (bridge) :

- o contrôle la trame avant de l'envoyer

- o segmentation du LAN en plusieurs domaines de collisions
⇒ optimise performance sans filouter broadcast
- o risque de cycles.

osi 2 commutateur (switch) : trame

- o un switch simule un réseau de pont avec un seul noeud sur chaque segment

osi 3 Routeur (router) o manipule des paquet

- o pas de broadcast partagé ⇒ plus de scalabil

(WAN / MAN)

- Bande locale: infrastructure déployée par un opérateur pour connecter les abonnés à son réseau.
 - « dégroupage »
 - grand investissement
 - métallique: DSL, modem
 - électrique: Powerline communication
 - optique: Fiber To The Curb, Node, Home, Terminal
 - CATV: Multiplexage spatial + problème de fréquence / bande passante partagée

Connexions point à point:

- ligne fondées
- Trunk: Circuits grande capacité OC-X STS-X
 - X.25 OSI 1-3 \Rightarrow Relais de trame OSI 1-2
Permanent Virtual Circuit
- ATM: Asynchronous Transfer Mode:
cellules: paquets petit de même taille
- PPP: OSI 2: compatible avec différents protocoles
paramètre défini par un protocole de contrôle IPCP

WAN: réseau avec une grande couverture géographique et capable de supporter un grand nombre d'abonnés

routeage: acheminement est réalisé sur la base d'adresse de destination

commutation: circuit virtuel ^{acheminement et routeage}, étiquette de ce circuit

table de routage: niveau hiérarchique, besoin de connaître uniquement ses proches!

TCP/IP: Conception Application

suite de protocoles utilisés pour Internet:

TCP:	transport
IP	réseau
(UDP, ICMP, ARP)	

motivation application distribuée,
protocoles → types messages échangés
client/server

Interface *couche réseautique

- Couches: application
HTTP, FTP, PUP3 ...
- transport
TCP / UDP
- réseau
IP, DHCP, ICMP
- réseau physique
(Transport Control Protocol)

TCP: orienté connexion, négociation initial, garantie l'arrivée, limite congestion

UDP: broadcast, rapide, pas de garantie
(User Datagram Protocol)

o Processus (programme) [f:n] threads



o POP vs IMAP
210 143 : SMTP
443 25

o HTTP Hypertext Transfer Protocol

adresse
headers
contenu

statique vs dynamique
lien vers Common Gateway Interface (CGI)

o Domain Name System (DNS)

base de données décentralisée

caché et réPLICATION pour scalabilité et performance et résilience du système

Top/Ip: couche transport

- services de communication de bout en bout au processus de la couche application
 - abstraction du réseau
 - multiplexage/démultiplexage pour partager l'interface réseau entre processus.
 - Tcp/Udp implementés uniquement dans les nœuds terminaux, (pas au sein)
 - - gestion de l'association processus \leftrightarrow socket.

multiplexage : - encapsulation du message dans des segments \rightarrow IP \rightarrow paquet (francopost) src + dest

demultiplexing: - $M^P \rightarrow$ appelle des primitives TCP UDP

- décapitation du paquet pour obtenir le segment (minérite part)
- transfère à travers le sacut → processus

Association de socket

UDP:

{adresse IP destination, numéro de port destination}

Numeros port sonne du segment indigne
return;

- sans connexion

- Best-effort \Rightarrow pas de garantie arrivé

- 1-1, in

rapide, pas de contraste. Plus, congénital

\langle IP source, port source
IP dest, port dest \rangle

socket "server" < #, #, IPdest, portdest >
attend connection

Observe connection hasard
→ SYN 1, sans données, nb séquence (random)

→ nomen socket < IP source, port src, IP destination buffer nennebaie de SYN 1

→ client initializes seq buffer, sends ack 1

- Connexion bidirectionnelle

intégrale dans le bon ordre

- tout avant l'entretien

- 1 -

- Contrôle de flux / congestion
adapter vitesse à l'émission
réception

TCP! renvoie de données si pas reçus fin d'un accroissement dans les délais temps par varian:

crop lang : pas efficace

trop count: congestion

RTT: Round Trip Time → estime ERTT future et choisit un fin de virage plus grand

stop-and-wait: attendre acknowledgement

pipeling : envoie en bloc

Go-Back-N: acquitté en bloc jusqu'à un numéro de séquence

TCP: segment contient données, acquittement, numéro de séquences, longueur
· piggybacking.
 ↳ premier
 système mangnant

fermeture connexion

- envoie de FIN=1
- ↔ ACK=1, FIN=1
- ACK=1 + TIME_WAIT ↳ fin normale
- CLOSED

buffer = fenêtre (window) restante
indique l'état des réceptions en fonction
de ce qu'il doit attendre

Réseau et Télécommunications

(5)

+ TCP/IP Architecture Réseau

- o ~~best effort~~
- o service de communication de "point à point"
- o protocole IP est implementé sur tous les nœuds du réseau (confirme hôte)
- o Segment TCP ou UDP encapsulé dans un datagramme IP
- o Headers (IP source + destination)
- o gestion des routes des datagrammes (algorithmes de routage) en fonction de l'adresse de destination

IPv4: 32 bits : 255.255.255.255 → prefixe: ~~sous-réseau~~ ~~global~~

2~~bits~~ ip/contes réseau: redondance
 ↗ identifie une interface connectée à un réseau

client+admin (backbone)
 sécurité
 ↗ suffixe: ~~local~~ interface
 gestion global du réseau

classes d'adressage: 4 premiers bits

Internet (pour ISP)	A: 0 - 127	entité limitée
autre (central IANA)	B: 128 - 191	
	C: 192 - 223	
	D: 224 - 239	
	E: 240 - 255	

adressage sans classe: avec masque de sous-réseau:

Classless Interdomain Routing (CIDR) indique le nombre de bit alloués au préfixe

IP / 32	
all-0	all-0
network 0	this computer bootstrap
network 1	network
1	broadcast on network
127	1 broadcast local
	any loopback (hosting)

Datagramme IP:

- o longueur variable ~~>~7500 bytes~~
- o transporté sur différent réseau physique (Ethernet, X25)
- o taille de l'entête max = MTU

✓ Fragmentation: plusieurs datagramme avec indication de position
 → reconstruction pour l'hôte final

Internet Control Message Protocol : ICMP

protocole IP = best effort → aucune garantie

mais ICMP dans le datagramme IP fournit des informations sur le réseau
→ ping, traceroute

état du réseau

Forwarding / Routing

Forwarding: Utilisation des tables de routage pour trouver la bonne interface

Routing: Construction des tables de routage (de terminer chemins entre source et destination)

→ statique: définit au démarrage

→ dynamique: mise à jour automatique

→ par inondation: messages sur toutes les interfaces

(lent)

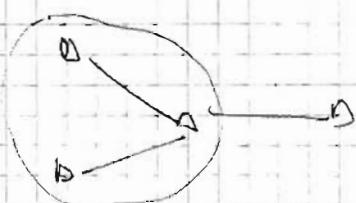
algorithmes (moyens court): "vecteur distance": échange des tables optimisé RIP
BGP

grants "à état de liens" - tous connaissent la topologie OSPF

Pour limiter le traffic

systèmes autonomes AS

⇒ l'intérieur des AS



entre AS

↔ External gateway protocol (EGP)

synthesise

Border Gateway Protocol (BGP)

Interior Gateway protocol (IGP)

Routing Information Protocol (RIP)

Open Shortest Path First (OSPF)

IPv6

128 bits

structure plus simple

pas de fragmentation → taille plus petite MTU

→ si réponse ICMP "Packet too Big"

→ meilleures performances car hôte fait la fragmentation

- 6
- TCP/IP: couche d'accès réseau - link layer
- datagrammes encapsulés dans des trames
- adresse physique: MAC : Medium Access Control fix au matériel
(vs adresse logique (couche réseau) IP qui est hiérarchique)
- résolution de l'adresse Mac par l'adresse IP.
- table (mapping manuelle)
 - calcul
 - échange de messages → serveur (risque de surcharge, pas de tolérance aux pannes)
(ARP) → décentralisé (broadcast) (Chacun sa liste)
 - Address Resolution Protocol
 - que même sans réseau

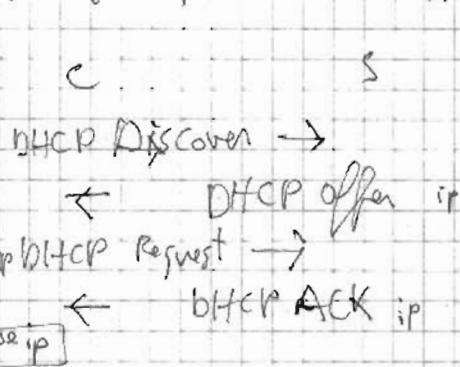
● Configuration manuelle

- coût
- changement difficile
- risque d'envers
- utilisation mobile difficile
- utilisation peu efficace des plages IP
- poste sans disque impossible

→ automatique mieux:

RARP: serveur gère le mapping → admin
↓
BOOTP + fichier boot

DHCP IP ~~MAC~~ + IP
permise lease
(ressources) times



Application classification → streaming → live
 → temps réel → IP phone
 → compensation interpolation → pas de délais → IP video sharing - App...
 → mais sensible aux variations

Cache entre variable → sortie constante

+ proxy cache → bande passante + cache serveur → graphique
 côté client → sécurité → limite CPU

Protocoles : SIP, ...

CDN: Content Distribution Networks

problème: Load balancing: énorme dans un data center ne suffit pas toujours.
 → pour plus de scalabilité / sécurité ... ; réduction des délais
 différents emplacements géographiques
 → serveurs DNS spécial redirige vers le serveur le plus proche
 (cataloguer)
 → surtout pour le multimédia le reste est hébergé chez Content Provider

P2P

vs client-server
 mixte → serveur pour connecter les clients

pure → bootstrap → clients populaires

Overlay network = réseau niveau application → réseau décentralisé

Problèmes

- Internet = Best Effort, mais multimédia besoin de garantie
- Status quo: cache, + de bandpassante
- Differentiated service: QoS supplémentaire (classes de paquets?)
- Integrated service: changer l'infrastructure

- Risques et menaces

- Accès illicite
- Interception des échanges
- Usurpation d'identité
- Usage illicite des ressources
- = Denial of Service
- Virus, spam \Rightarrow contenus

politique de sécurité

ouverture des SI

lois & régimes (log...)

contenu

- Identification / authentification : mots de passe, certificats

- - Autorisation: (après identification) liste de contrôle d'accès (ACL)
- Confidentialité: cryptage des messages \rightarrow interception vs compréhension
- Intégrité: empreinte (digest) prouver que le contenu n'a pas changé lors du transfert
mais c'est que cryptage
- Non-répudiation: preuve de réception: signature électronique

Cryptages: \rightarrow clés symétriques: \leftrightarrow besoin d'échanger la clé

\rightarrow clés asymétriques: clé publique et privée

\rightarrow besoin de CA pour que l'on ne peut pas se faire passer pour quelqu'un d'autre

Gestion des identités

besoin de centraliser \rightarrow + de contrôle qui à quel accès
1 seul mot de passe

o consolidation: rendrait à modifier les applications pour qu'elles y accèdent

o intégration: synchronisation des applications: Δ application sur des applications

o Single Sign-On: protégé par un agent non sécurisé.
qui laisse passer si l'utilisateur a un "jeton"

o autorisation basé sur les rôles + de flexibilité que droit sur un utilisateur.

Cours 12 : Mobilité

? RFID :

- technologie ancienne
- en mutation → standardisation, globalisation, cont'l, ...
- Localiser des objets avec des tags
lecteur mix (~~fixe~~ fix vs mobile) + intégration au SI
- exemple médical
- défis :
 - quantité de données (infrastructure)
 - intégration
 - contraintes physique

} Besoin de signaler
au niveau local

Cours 13: gestion du réseau

Réseau vital: application → grand impact

(bourse...) conséquences financière et non financière
merciel transport (physique)

proactif → prév, metric des composants
remplacement

Réduire les panne & détecter rapidement + réduire temps réparation

↓
prévention... surveillance procédures

Réseau complexe: · nombreux éléments qui interagissent } . besoin d'architecture
· nature différente | Parcimonie différent } . documenté
· évolution } . besoin de contrôle centralisé

indicateurs: · alive (répondant)

SNMP → agent ↔ Interface
(besoin standard) requête/réponse
· taux de charge ou notification

(besoin standard)

Best practices: ITIL

contrôle autoratique con trop complexe pour être manuel