Reseaux

Fiche

Introduction

- "ensemble de lignes entrelacées" (au propre)
- "ensemble de relations" (au figuré)

Modèles et couches

Le modèle OSI
SCHEMA

À quoi sert ce modèle ?
1. Il aide à la compréhension des problèmes et des solutions ;
2. A l'origine, devait servir de structure pour le développement d'une suite de protocoles... mais ils ont "perdu" contre TCP/IP.
Mais le modèle est très bien. Du coup on s'en sert pour comprendre les protocoles existants
Pourquoi un modèle sert au développement de protocoles ?
Structuration de la problématique.
Structuration = découpage en sous-problèmes = découplage
Découplage ⇒ construction plus rapide (réutilisation...)
Découplage ⇒ flexibilité et performance possibles
Flexibilité et performance ⇒ standardisation

0.1 couche physique

Couche physique : conversion de bits en signal sur médium physique
Le bit est le PDU (Protocol data unit) de la couche physique. C'est-à-dire l'unité dans laquelle on mesure ce qui est transmis par cette couche.
Les bits sont convertis en symbole pour la transmission ! Le baud mesure le nombre de symboles / s. Parfois, un symbole exprime un bit, parfois plus. Jamais moins. Pourquoi ?
Le médium physique peut être :
I Câble électrique (série ou parallèle..) ;
I Fibre optique ;
I Ondes radio ; I
Saint-bernards ;
I etc.

...

Quelles contraintes sur la couche physique ?
Taille du réseau : PAN ? LAN ? MAN ? WAN ?
Quelle topologie ?
I Point-à-point ;
I Bus ;
I Étoile ;
I Anneau ;
I Cube;
I HyperCube;
I Etc.

TOUS LES SCHEMA

Quel médium : câble électrique ? fibre ? radio ? saint-bernards ?
Câbles : Coaxial ? "Étanche" aux perturbations extérieures et hautes fréquences mais cher, rigide, pas facile à sertir... Ethernet 10BASE2, 10BASE5 utilisaient du coaxial.
Câbles : Câble parallèle ? Crosstalk / diaphonie Pas utilisé à ma connaissance si ! PLIP
Câbles : Câbles série ? Paire(s) torsadée(s) !
Différents standards physiques de paires torsadées :
I U/UTP : pas blindé ;
I U/FTP : blindé (feuille) sur les paires ;
I F/UTP : blindage (feuille) sur le câble ;
I ...
I SF/FTP (!!) : blindage (feuille + tresse) sur le câble + blindage (feuille) sur les paires !
À quoi sert le blindage ?

Par exemple : Figure 20: câbles avec paires torsadées

Plus de blindage Plus + de torsade Plus + de qualité dans les connecteurs (Plus probablement d'autres contraintes) Implique qu'on peut passer de plus hautes fréquences dans le câble. Implique qu'on peut passer plus de données (on verra pourquoi plus loin).

Figure 21: standards de câbles

On veut passer des fréquences plus grandes, pour faire transiter plus de données. Pourquoi on peut faire passer plus de données si on a de plus hautes fréquences disponibles ? On verra ça plus loin. Déjà, comment faire passer les données ?

Courant continu, courant alternatif. Signal.
Rappel : on veut coder des bits en signal électrique. Comment faire ?
Code NRZ (utilisé p.ex dans RS-232) :

Figure

Code Manchester (utilisé p.ex dans le vieil Ethernet 10BASE5) :

Figure
MLT-3 (utilisé p.ex dans 100BASE-TX)

Figure

Symboles. Si on a n symboles distincts, combien de bits un symbole peut-il représenter ? Et donc, quelle relation entre débit en baud et débit en bit/s ?
Pourquoi on peut faire passer plus de données si on a de plus hautes fréquences disponibles ? Eh bien c'est très simple...

Dessins.
1. Sinusoïde. Fourier. Résultat.
2. Carré. Fourier. Sinus cardinal.
3. Signal un peu carré et un peu aléatoire (on verra ça plus tard). Fourier.
4. Atténuation, décibel (20*log_10(sortie/entrée), 6 dB → /2, 20 dB → /10, 60 dB → /1000).
5. Bruit. Quelle conséquence ?

Example atténuation : Cat5e (Ethernet Gigabit), 32 dB / 100m (câble trouvé là : http://www.farnell.com/datasheets1311844.pdf)

Taux de transfert binaire maximal ?
Nyquist : s'il n'y avait pas de bruit.
C_Nyquist = 2 * Fmax * log_2(n_symboles) (en bps) (quelle implication de l'absence de bruit sur le nombre de symboles ?)

Shannon : il y a du bruit. Logiquement, devrait être... inférieur ?
Supérieur ? Au Nyquist. C_Shannon = Fmax * log2 (1 + signal / bruit) (en bps)

Modulation analogique. Utilisations : radios en tout genre.
I AM : Amplitude modulation
I FM : Frequency modulation
I PM : Phase modulation

Figure 25: AM/FM

On module pour nettoyer le signal... (carré → largeur infinie !) On module pour mettre le signal à la bonne fréquence (par exemple, dimension d'antenne) Et, sans aucun doute, pour d'autres raisons.

RTC (modem 56k...) : on module ; le signal reste dans la bande "voix" 300 → 3400 Hz... voix téléphonique

ADSL (modem ADSL...) : on module ; on étend le signal ailleurs que dans les fréquences vocales I ADSL : 0→ 1,1 MHz ; I ADSL2+ : 0 → 2,2 MHz.

Fibre optique !

À peu près comme les cables en cuivre, mais un peu différent :
I Atténuation beaucoup plus faible grâce à la réflexion totale (+ distance et/ou + débit);
I Insensibilité aux interférences (électromagnétiques) et pas de risques "électriques" ;
I Le verre se plie moins bien que le cuivre ;
I Fibre monomode / fibre multimode (voire diapositives suivantes)

Distances différentes selon les couleurs (= fréquences) différentes !
SCHEMA

Radio ! WiFi a/b/g/n/ac/ad/... 5G 4G 3,9G 3,75G 3,5G HSUPA HSDPA W-CDMA GPRS ZigBee 802.15.4 Wave LoRa LoRaWAN Bluetooth BLE WiMAX IrDA SigFox... On verra ça une prochaine fois

Quelques mesures
Délai/temps de transmission d'un message entre le début et la fin de l'émission : T_t = N / V_t
I N taille du message ;
I V_t vitesse de transmission/émission (bits émis par seconde).

Délai/temps de propagation du signal : T_p = D / V_p
I D distance à parcourir ;
I V_p vitesse de circulation du signal (dépend du support).

Délai d'acheminement/transfert : T = T_t + T_p
C'est la durée entre le début de l'émission de bits et la réception du dernier bit par le destinataire. Après, tout traitement ajoute son délai supplémentaire...

- RECAPITULATIF...

(Informations complémentaires sur Ethernet.) (Attention : Ethernet couvre la couche lien de données aussi).
I Vieil Ethernet désignera Ethernet en bus ;
I Jeune Ethernet désignera Ethernet en étoile.
- 1983 : 10BASE5 (500m, "thick")
- 1985 : 10BASE2 (185m, "thin")
- 1985 : 10BROAD36 (1800m, coax 50 ohm)
- 1987 : 1BASE5 (250m, paire téléphonique)
- 1990 : 10BASE-T (100m, 2 paires CAT3) - 1993 : 10BASE-FL (2000m, 2 multimodes)
- 2004 : 100BASE-BX10 (10km, 2 monomodes)
- 2006 : 10GBASE-T (100m, 4 paires CAT6a ; 55m, CAT6)
- 2016 : 40GBASE-T (30m, 4 paires CAT8

0.2 Liaison de données

Transfert des données (X) sur un même Y
Transfert des données (assez fiable) sur un même segment
PDU = trame/frame

Deux couches secondaires forment la couche 2 :
I Sous-couche Medium Access Control (MAC / "Contrôle d'accès au support")
I Sous-couche Logical Link Control (LLC / "Contrôle de la liaison logique")
Enfin, dans les protocoles usuels...
Couche 2 : liaison de données : Protocoles usuels : IEEE 802 (LAN et MAN)
802.2 LLC 802.3 Ethernet 802.4 Token Bus 802.5 Token Ring 802.6 DQDB (pour MAN) 802.11 Wi-Fi 802.15.1 Bluetooth 802.15.4 Zigbee and Cie 802.16 WiMAX

MAC

À votre avis, à quoi sert la couche Medium Access Control ? Pourquoi faut-il contrôler l'accès au support ?

Le médium (segment) est partagé entre plusieurs noeuds. S'ils injectent leurs symboles en même temps au même endroit... tout s'additionne : brouillage.

Selon les topologies... 1. Sur le vieil Ethernet : bus. 2. Jeune-vieux Ethernet "point à point"/étoile : deux paire torsadée. 3. Jeune Ethernet : quatre paires torsadées. 4. Token Ring ..? Dans quelle situation le problème est le pire, à votre avis?

Quelles solutions ?
Multiplexage Temporel, spatial, fréquentiel, codage...
Multiplexage temporel : 1. Ordonnancement : chacun son tour ; 2. Aléatoire (avec quelques règles, quand même) ; Couche 2 : liaison de données : MAC
Multiplexage temporel ordonnancé TDMA (Time Division Multiple Access) Intérêt : délai maximum garanti. Rarement utilisé en filaire, souvent en radio.
Multiplexage temporel aléatoire : I Soit on "écoute" pas et on communique (CSMA); I Soit on "écoute" si un autre "hôte" est en train de communiquer avant de commencer ; Dans les deux cas, il peut y avoir des collisions...

Premier protocole: ALOHA (Hawaii, sans fil) 1. On envoie (sans "écouter") ; 2. Si collision, on réenvoie après temps aléatoire. Version sans time slots (créneaux horaires ?) : 18% d'effcacité Version avec time slots : 36% d'effcacité

Amélioration : CSMA On écoute avant de communiquer. Mais deux stations peuvent commencer au même moment.

Amélioration : CSMA/CD (Collision Detection) On arrête la transmission dès qu'on détecte une collision. On gagne du temps. Vieil Ethernet
CSMA/CD Délai garanti ? Qualité de service ?

Il y a aussi le CSMA/CA (Collision Avoidance) Attente aléatoire avant nouvelle tentative. Wi-Fi

Revenons au CSMA/CD (Vieil Ethernet). La "détection de collision" impose une taille minimale de trame : 64 o. Basé sur le délai de propagation : Station distante détecte la collision et doit prévenir avant la fin. Il faut temps_de_transmission ¿ 2 x délai_de_propagation. Ethernet : 64 o.

Note : le jeune Ethernet est 1. Commuté/switché ; 2. full-duplex = chacun sa ligne ; Plus de collisions.

Rappel : on était dans la problématique "Comment éviter les collisions ?"

Là où il y a le plus de collisions, c'est dans les communications sans fil. On verra ça plus tard...

Qu'y a-t-il d'autre dans la sous-couche MAC ? I Adresses (48 bits) I Détection/correction d'erreurs (CRC)

Le Cyclic Redundancy Check est un code de détection d'erreur. Vous pouvez chercher si vous voulez savoir comment ça fonctionne.

Le CRC est calculé à partir des données. Il permet de détecter les erreurs sur 1, 2 ou nombre impair de bits.

Si la couche MAC d'en face détecte une erreur (en comparant CRC et données), elle demande le renvoi de la trame.

Le CRC n'est pas un code correcteur d'erreur. Exemple code correcteur : code de Hamming.

Code correcteur utilisé quand (pas dans les LAN normaux):
I Taux d'erreur très élevé ;
I Délai très important ;
I Communication unidirectionnelle (exemple ?);

LLC

IEEE 802.2 formalise cette couche. Logical link control n'est pas un nom très clair (je trouve). Elle est généralisée dans les protocoles de la famille 802 (Ethernet, token ring, 802.11...).

LLC fournit (si on lui demande, voir plus loin):
I Trames (pour multiplexage des protocoles supérieurs
I Fiabilité : contrôle de flux, acquittements

Trois types de service (selon les protocoles autour) :
1. Pas d'acquittement, pas de connexion ;
2. Connexion avec acquittments ;
3. Acquittements sans connexion. Selon le type de service, différents types de trames utilisés.

1. Pas d'acquittement, pas de connexion. Mode le plus basique. (Ethernet avec IPv4 par dessus – qui gère la délivrance des messages ?)

2. Connexion avec acquittements I Connaissance de la taille de la fenêtre du récepteur : rafales sans acquittement I Numéros de séquence

SCHEMA

Couche 2,5 ARP

Address Resolution Protocol On a une adresse... MAC ? IP ? On cherche une adresse... MAC ? IP ?

Address Resolution Protocol On a une adresse... IP On cherche une adresse... MAC

On envoie une requête ARP en broadcast MAC : "Je suis IP[x], quelle est l'adresse MAC de la machine qui a l'adresse IP [y] ?"

La machine concernée répond, "je suis IP [x], voilà mon adresse MAC" Les deux mettent leur cache ARP à jour (liste des IP -¿ MAC).

Simple, effcace.

Comment se faire passer pour une autre machine ?

Pris en charge par IPv6 directement... Neighbor Discovery Protocol/NDP

SLIP

SLIP : Serial Line Internet Protocol RFC 1055 : "A NONSTANDARD FOR TRANSMISSION OF IP DATAGRAMS OVER SERIAL LINES: SLIP"

Très simple : I 1 paragraphe d'introduction I 3 paragraphes d'historique I 2 paragraphes pour dire où trouver le pilote I 3 paragraphes de protocole I 6 paragraphes de limitations et une implémentation en 127 lignes de C

Utilité : encapsuler des paquets IP et les envoyer sur port série. Il faut : I Pouvoir reconnaître le début et la fin d'un paquet ; I C'est tout.

Comment reconnaître le début/la fin d'un paquet ?

On insère un marqueur. Dans SLIP, il s'appelle END : #define END 0300 /* indicates end of packet */ ...etilindiqueledébutaussi

Donc : 1. On envoie END 2. On envoie le message 3. On envoie END Problème ?

...Et si le message contient 0xC0 ? (0xC0 == 0300 == 192 == END)

Solution ? Transformer ?

Échappement ! Comme '/én C et dans à peu près tous les langages.

#define ESC 0333 /* indicates byte stuffing */ #define ESC_END 0334 /* ESC ESC_END means END data byte */ #define ESC_ESC 0335 /* ESC ESC_ESC means ESC data byte */

En hexadécimal... #define END 0300 /* 0xC0 */ #define ESC 0333 /* 0xDB */ #define ESC_END 0334 /* 0xDC */ #define ESC_ESC 0335 /* 0xDD */

Exemple : on veut envoyer le message : 0x63 0x65 0x63 0x69 0xc0 0x65 J'imagine que ça n'est pas un paquet IP valide mais oublions IP pour l'exemple. EXEMPLE MESSAGE Algorithme de lecture ?

Taille de trame SLIP : souvent, 1006 o, mais pas défini formellement.

Quelques problèmes de SLIP :
I Pas de mécanisme pour connaître l'adresse IP de l'autre (style ARP/RARP)
I Pas d'identificateur de protocole encapsulé – encapsulation d'un seul protocole (pas de multiplexage)
I Détection d'erreur ?
I Compression ? (il y a quand même une version compressée, CSLIP)

PPP

PPP = Point to Point Protocol Évolué !

Fonctionnalités : I Authentification I Chirement I Compression I Autres fonctionnalités

PPP est donc un protocole un peu complexe. Il est séparé en plusieurs parties/sous-protocoles (et plusieurs Requests For Comments/RFCs). Il est "extensible".

1. Encapsulation, multiplexages : trames (la base) ; 2. Link Control Protocol (LCP); 3. Des Network Control Protocols (NCPs); 4. Des protocoles de support de LCP ; 5. Des protocoles optionnels de LCP. Chaque partie a ses RFCs.

Commençons par LCP (on décrira les trames plus tard) : LCP gère le lien (merci captain obvious). SCHEMA1 SCHEMA2 Premier protocole : PAP : Password Authentication Protocol Simple... ...SCHEMA.... CHAP : Challenge-Handshake Authentication Protocol ...SCHEMA.... NCP = Network Control Protocol Configuration de paramètres spécifiques au(x) protocole(s) de couche 3 utilisés.

Cas le plus classique en couche 3 transporté par PPP : IP. =¿ NCP = IPCP (IP Control Protocol ...)

À quoi sert IPCP ? I Négociation de l'utilisation d'entêtes IP réduits ; I Obtention d'une adresse IP.

PPP a d'autres sous-protocoles : LQR : Link Quality Reporting.

PPP a d'autres sous-protocoles : CCP : Compression Control Protocol.

PPP a d'autres sous-protocoles : ECP : Encryption Control Protocol.

PPP a d'autres sous-protocoles : MP : Multilink Protocol.

PPP a d'autres sous-protocoles : BAP : Bandwidth Allocation Protocol. BACP : Bandwidth Allocation Control Protocol.

PPP fait vraiment beaucoup de choses.

Quel format ont les trames PPP ? Observons la RFC 1662...
FONCTIONNEMENT TRAME

0.3 Réseaux sans fil

Comment peuvent-elles communiquer ? I Ondes électromagnétiques ; I Ondes "sonores" ;
Mais généralement, ondes radio.
En bref : 1. Les ondes radio sont des ondes électromagnétiques 2. Plus la fréquence est haute, plus le signal est atténué (plus de "choses" deviennent des obstacles) ; 3. Fréquence (temporelle) et longueur d'onde (spatiale) sont liées ; 4. Diérentes bandes de fréquences ont diérents usages.
Pour transmettre le signal Antenne basique : antenne dipolaire. SCHEMA
Taille de l'antenne liée à la longueur d'onde qu'on veut transmettre. Bonne taille, souvent : L/2 .
Réseaux sans fil
La caractéristique essentielle d'une antenne est : Dans quelle direction rayonne-t-elle ?
Réseaux sans fil
Antenne isotropique. Théorique. Rayonne dans toutes les directions avec la même puissance.
Gain d'antenne = Le gain d'antenne est le pouvoir d'amplification passif d'une antenne. C'est le rapport entre la puissance rayonnée dans le lobe principal et la puissance rayonnée par une antenne de référence, isotrope ou dipolaire. Le gain d'une antenne dépend principalement de sa surface équivalente, de sa directivité et de la fréquence. I Donc plus une antenne est directive, plus son gain est élevé. I On mesure le gain en dBi (décibel isotrope, parce qu'on compare à une antenne isotrope)

Comment augmenter fortement le gain

Une plus grosse antenne maintenant : I 860-870 MHz (LoRa : 868 MHz) I 360 degrés à l'horizontale, 25 degrés à la verticale I 6 dBi I 50W

Attention : une antenne est influencée par ce qu'il y a autour. I cf. parabole... I cf. intérieur téléphone portable

0.4 Autre couche

couche liaison:

La trame/frame est le PDU (Protocol data unit) ; l'unité qui caractérise ce qui est transmis
Un segment, c'est un médium partagé par deux ou plus individus. I Câble ;
I Hub ethernet ;
I "Voisinage" radio ;

Fiabilité $\longrightarrow$ détection/correction d'erreur (CRC...)

couche réseau
Couche réseau : transmission de paquets jusqu'au(x) destinataire(s)
Le paquet est le PDU ici.
À noter que la base d'Internet, le protocole IP (v4 ou v6) correspond bien au modèle OSI.

couche transport
Couche transport : transmission de segments/datagrammes de service/processus à service/processus
segment/datagramme PDU de la couche. Curieusement, ça correspond exactement aux termes TCP et UDP. TCP, UDP $\longrightarrow$ numéros de ports = service (HTTP ? FTP ? SSH ?).

couche session
Couche session : guestion de sessions (séquences de dialogue entre applications) ; inclut suivi de l'état de la session avec rollback éventuel, authentification, autorisation Note : à partir d'ici, la suite de protocoles TCP/IP dit "c'est l'application qui gère". De manière générale, les choses deviennent un peu plus floues. RPC, SDP, RTCP, PPTP, AppleTalk

couche présentation
Couche présentation : encodage, chiffrement des données Encodage caractères (ASCII, UTF..) avec déclaration, XML, ASN.1, JSON (un peu ?)

0.5 Difference

En pratique, les protocoles les plus utilisés sont de la "suite" TCP/IP / Internet protocol suite.

OSI vs TCP/IP

Ça correspond ! À peu près. Il ne faut pas essayer de tout faire rentrer dans les cases du modèle OSI. La correspondance couche OSI $\leftrightarrow$ protocole est parfois floue. SSL/TLS (crée une session $\longrightarrow$ couche session ? ; chiffrement $\longrightarrow$ couche présentation ?) Couches "application"..
Encapsulation, décapsulation. Chaque couche rajoute ses informations. À l'envoi, chaque couche "emballe" ce qui vient "du dessus" avec ses paramètres. À la réception, chaque couche "déballe" ce qui vient du dessous.

tab titre

...	...	...