

INFO-F303 - Réseaux

Guy LEDUC

Résumé du cours

Rodrigue VAN BRANDE

Antoine DEWILDE (résumé original)

Julien VANBERGEN (réponses théorie)

19 janvier 2015

Table des matières

1	Résumé	3
1.1	Introduction	3
1.1.1	Qu'est-ce qu'Internet ?	3
1.1.2	Périphérie du réseau	3
1.1.3	Aspects physiques	3
1.1.3.1	Limites de débit	3
1.1.3.2	Réseau DSL	3
1.1.3.3	Réseau câblé et fibre optique	4
1.1.3.4	Types de câbles	4
1.2	Couche applicative	4
1.3	Couche de transport	4
1.4	Couche réseau	4
1.5	Couche de liaison	4
2	Questions et réponses	4
2.1	Théorie	4
2.1.1	Expliquez la différence entre une paire de cuivre torsadée de catégorie 3 et une paire de catégorie 5. Laquelle permet un débit plus élevé et pourquoi ? Expliquez la différence entre une fibre optique monomode et une fibre multimode. Laquelle permet un débit plus élevé et pourquoi ? Pourquoi utilise-t-on un modem pour transmettre de l'information numérique sur une ligne téléphonique ? Comment module-t-on le signal dans les modems « dial-up » les plus courants ?	4
2.1.2	Définissez les différents types de « Resource Records » utilisés par le protocole DNS et expliquez leur rôle.	5
2.1.3	10 processus clients communiquent simultanément avec un processus serveur attaché au port 8000. Combien de sockets vont être ouverts par le serveur si les processus communiquent par UDP ? Pourquoi ? Même question s'ils communiquent par TCP.	5
2.1.4	Expliquez le principe d'un protocole à fenêtre glissante SR (Selective Repeat). Quelle est la taille maximale de la fenêtre, si les trames sont numérotées modulo k ? Pourquoi ?	5
2.1.5	En première approximation, quels sont les 3 paramètres qui influencent le débit d'une connexion TCP ? Expliquez. TCP garantit-il un partage équitable des ressources du réseau par les différentes connexions ? Pourquoi ?	5
2.1.6	Décrivez l'architecture générique d'un routeur et le rôle de chaque composant. Comment peut-on perdre des paquets dans les ports d'entrée ? Comment peut-on perdre des paquets dans les ports de sortie ? Qu'est-ce que le blocage HOL ?	5
2.1.7	Décrivez le contenu des paquets de routage et leur méthode de diffusion dans le cas des protocoles à état de lien. En quelques mots, en quoi est-ce fondamentalement différent des protocoles à vecteur de distances ?	6
2.1.8	Le protocole de routage interdomaine BGP est plus apparenté à la famille des protocoles de routage intradomaine à vecteur de distances (DV) qu'à celle des protocoles à état de lien (LS). Expliquez deux ressemblances importantes entre BGP et un protocole DV. Expliquez deux différences importantes entre BGP et un protocole DV, et leur raison d'être.	6
2.1.9	Qu'est-ce que le CSMA/CD ? En quoi améliore-t-il le CSMA ? Quelle contrainte le CSMA/CD introduit-il par rapport au CSMA ? Pourquoi ? IEEE 802.3 (plus communément appelé Ethernet) est un protocole de type CSMA/CD dont la méthode d'accès a été améliorée. Quelle est cette amélioration ? IEEE 802.3 (plus communément appelé Ethernet) est un protocole de type CSMA/CD dont la méthode d'accès a été améliorée. Quelle est cette amélioration ?	6
2.1.10	On ne peut pas dire que les commutateurs Ethernet exécutent un protocole de routage (au sens de la couche 3), mais ils construisent toutefois des tables d'acheminement comme si un protocole de routage était à l'oeuvre. Expliquez comment ces tables sont construites, y compris quand plusieurs commutateurs sont interconnectés.	6

2.1.11	Un chercheur connecte son ordinateur portable à un commutateur Ethernet de son département. Il démarre son browser pour afficher la page web de <code>www.google.com</code> . Identifiez les protocoles mis en oeuvre, et dans l'ordre chronologique, entre le moment où l'ordinateur se connecte et le moment où la page d'accueil de Google s'affiche. Précisez au passage le rôle de chaque protocole et décrivez-les succinctement.	7
2.1.12	Expliquez la dispersion de délai dans une fibre optique. Quelle en est la conséquence ? Dans quel type de fibre la rencontre-t-on ?	7
2.1.13	Définissez les différents types de « Resource Records (RR) » utilisés par le protocole DNS et expliquez leur rôle. Donnez le scénario d'échange de messages DNS, par la méthode itérative, permettant à un client de trouver l'adresse IP d'un serveur web dont l'URL est <code>www.company.com</code> , <i>en indiquant les RR présents dans ces messages</i> . On supposera que les caches DNS sont vides.	7
2.1.14	Expliquez le principe d'un protocole à fenêtre glissante GBN (Go-back N). Quelle est la taille maximale de la fenêtre de l'émetteur, si les trames sont numérotées modulo k ? Pourquoi ? Citez et expliquez 4 différences apportées par le protocole SR (Selective Repeat).	8
2.1.15	Expliquez l'établissement de connexion « 3-way handshake » utilisé dans le protocole de transport TCP, en indiquant les paramètres importants présents dans les échanges et leurs rôles. Expliquez avec l'aide d'un exemple pourquoi un « 2-way handshake » ne serait pas suffisant.	8
2.1.16	Comment l'émetteur TCP détecte-t-il une congestion ? Décrivez le mécanisme de contrôle de congestion de TCP. Quelle distinction TCP fait-il entre congestion légère et congestion sévère ? Comment réagit-il dans chaque cas ? Quelle distinction TCP fait-il entre congestion légère et congestion sévère ? Comment réagit-il dans chaque cas ?	8
2.1.17	Énoncez les différents types de matrice de commutation (« switch fabric ») rencontrées dans les routeurs, ainsi que leurs avantages/inconvénients respectifs. Expliquez la raison d'être et l'inconvénient potentiel d'une bufferisation au niveau des ports d'entrées. Expliquez la raison d'être d'une bufferisation au niveau des ports de sortie.	9
2.1.18	Expliquez le principe du « Longest Prefix Match » lors de l'acheminement de paquets IP. Quel est son intérêt ?	10
2.1.19	Le protocole de routage interdomaine BGP est plus apparenté à la famille des protocoles de routage intradomaine à vecteur de distances (DV) qu'à celle des protocoles à état de lien (LS). Expliquez deux ressemblances importantes entre BGP et un protocole DV. Expliquez deux différences importantes entre BGP et un protocole DV, et leur raison d'être.	10
2.1.20	Expliquez le rôle et le principe général des codes détecteurs d'erreur. Pourquoi ne peuvent-ils être efficaces à 100% ? Donnez un exemple de code détecteur d'erreur plus élaboré que le bit de parité, et expliquez son principe.	10
2.1.21	Expliquez le principe du multiplexage en longueur d'onde (WDM). Quel est son intérêt ? Comparez WDM aux techniques classiques de multiplexage TDM et FDM.	10
2.1.22	Vous créez votre entreprise « MeMyself&I » et vous obtenez le nom de domaine « <code>memyselfandi.com</code> ». Vous souhaitez déployer votre propre serveur DNS pour ce domaine (<code>dns.memyselfandi.com</code> , <code>111.111.111.111</code>), ainsi qu'un serveur Web <code>www.memyselfandi.com</code> , <code>111.111.111.112</code>). Quelles informations doivent être ajoutées dans la hiérarchie DNS et à quel niveau ? Soyez précis. Donnez un scénario typique d'échange de messages DNS permettant à un client de trouver l'adresse IP de votre serveur web, en précisant bien les éléments importants des messages DNS. On supposera que les caches DNS sont vides.	11
2.1.23	Pourquoi la couche de transport (UDP et TCP) comporte-t-elle une fonction de démultiplexage ? Décrivez les techniques de démultiplexage effectuées par UDP et TCP en mettant bien en évidence leurs différences ?	11
2.1.24	Donnez 4 éléments majeurs des protocoles « Go-Back-N » et « Selective Repeat » qui permettent de les différencier. Pour chacun de ces éléments pris indépendamment, indiquez si TCP s'apparente davantage à l'un d'eux. Expliquez. Quelle optimisation supplémentaire, liée au contrôle d'erreur, TCP y apporte-t-il ?	11
2.1.25	Expliquez le principe de NAT et la structure d'une table NAT.	12

2.1.26	Quand des flux TCP et UDP partagent un même lien congestionné, comment réagissent ces deux types de flux et quelles en sont les conséquences?	12
2.1.27	Nommez et expliquez succinctement les 2 grandes familles de protocoles de routage intradomaine (IGP) en insistant sur leurs différences. Expliquez en quoi et pourquoi le protocole de routage interdomaine de l'Internet (BGP) est différent des protocoles de routage intradomaine (IGP) déployés dans les divers systèmes autonomes (AS) qui composent l'Internet.	12
2.1.28	Expliquez comment un routeur construit les entrées de sa table d'acheminement pour les préfixes IP extérieurs à son domaine.	12
2.1.29	Décrivez le protocole CSMA. Pourquoi et comment a-t-il été amélioré? Citez les paramètres qui caractérisent un réseau CSMA. Quelle relation entre ces paramètres faut-il viser pour que le réseau CSMA ait des performances acceptables? Expliquez.	12
2.1.30	Considérez 3 réseaux Ethernet (N_1 , N_2 et N_3), un commutateur Ethernet (C) et un routeur (R) interconnectés selon une topologie en ligne $N_1-C-N_2-R-N_3$. Une station H_A (d'adresse IP_A) est attachée au réseau N_1 (par l'adresse MAC_A) et une station H_B (d'adresse IP_B) est attachée au réseau N_3 (par l'adresse MAC_B). C a deux adresses MAC : MAC_{11} sur N_1 et MAC_{12} sur N_2 . R a deux adresses MAC et deux adresses IP : MAC_{22} et IP_2 sur N_2 et MAC_{23} et IP_3 sur N_3 . Dessinez la configuration. H_A envoie un paquet IP à H_B . Si l'on suppose que les correspondances entre adresses IP et MAC sont connues de tous, décrivez les trois trames qui circulent respectivement sur les réseaux N_1 , N_2 et N_3 en vous limitant aux champs d'adresses des trames et aux champs d'adresses et de TTL (Time To Live) du paquet IP contenu dans la trame. Justifiez. Par quel protocole les correspondances entre adresses IP et MAC ont-elles été découvertes? Décrivez les échanges de ce protocole qui réalisent les mises en correspondance nécessaires lorsque H_A envoie son paquet IP à H_B . Mentionnez toutes les adresses présentes dans les messages échangés.	13
2.1.31	Citez une fonction majeure de chacune des 5 couches de la pile de protocoles Internet.	13
2.1.32	Pourquoi est-il plus difficile de fixer la durée du timer de retransmission de TCP que celle du timer de retransmission d'un protocole de liaison de donnée? Comment fixe-t-on la durée du timer de retransmission de TCP?	13
2.1.33	Expliquez la raison d'être des protocoles DHCP et NAT, et expliquez leur fonctionnement à l'aide de scénarios typiques.	13
2.1.34	Expliquez comment les commutateurs Ethernet apprennent où se trouvent les stations et par quel type d'adresse ils les identifient. Comment les pannes de stations ou leur mobilité sont-elles prises en compte? En quelques mots, quelle contrainte topologique doit être respectée pour que cet apprentissage fonctionne, et comment la réalise-t-on?	13
2.1.35	Citez et définissez les différentes sources de délai que subit un paquet dans un réseau datagramme.	13
2.1.36	Décrivez sommairement le fonctionnement du système DNS. Comparez les deux modes de fonctionnement du protocole (avantages et inconvénients).	13
2.1.37	Expliquez les principes de la programmation socket donnant accès aux services TCP et UDP. Quelles sont les différences importantes entre ces deux API? Dans une entité de transport, comment les sockets TCP et UDP sont-ils identifiés? Pourquoi?	14
2.1.38	Dans un protocole de transport, si l'on numérote les segments modulo 2, montrez par un contreexemple qu'il est également nécessaire de numéroter les acquits pour assurer la fiabilité du transfert. Dans quelle(s) situation(s) le protocole à bit alterné est-il quasiment aussi efficace qu'un protocole à grande fenêtre glissante? Expliquez.	14
2.1.39	Expliquez les circonstances dans lesquelles l'émetteur TCP peut recevoir trois doublons d'acquits venant du récepteur TCP. Décrivez deux actions importantes de l'émetteur TCP lorsque cela se produit et expliquez-en les raisons.	14
2.1.40	Expliquez le principe général du contrôle de <i>flux</i> de TCP. Expliquez deux mécanismes associés ayant pour but de permettre à TCP de s'adapter aux spécificités des applications ou de se protéger vis-à-vis de celles-ci.	14
2.1.41	Combien d'adresses IP doit-on attribuer à un routeur? Pourquoi?	14

2.1.42	Considérez un protocole de routage à états de liens (link state). Décrivez le contenu des paquets de routage, expliquez le rôle de chaque champ, et décrivez la méthode de diffusion des paquets. En quelques mots, en quoi est-ce fondamentalement différent des protocoles à vecteur de distances ?	15
2.1.43	Décrivez les principes du protocole de routage inter-domaine BGP. Expliquez comment BGP permet à un réseau périphérique (« stub ») multi-connecté (« multihomed ») de ne pas accepter du trafic de transit.	15
2.1.44	Sachant que la couche de transport est équipée de mécanismes (Cf. TCP) pour récupérer les erreurs de bout-en-bout, pourquoi la couche de liaison de données implémente-t-elle aussi toute une série de fonctions de ce type, comme la détection d'erreurs, voire même la retransmission de trames erronées dans certains cas.	15
2.1.45	Dans un réseau local composé de plusieurs segments Ethernet interconnectés par des commutateurs Ethernet, un ordinateur peut-il conserver son adresse IP si on le change de segment ? Pourquoi ? En est-il de même si les segments sont interconnectés par des routeurs ? Pourquoi ? Pourquoi est-il plus intéressant d'interconnecter des segments Ethernet par des commutateurs Ethernet plutôt que par des hubs ?	15
2.1.46	Expliquez la différence entre une fibre optique multimode et une fibre monomode. Laquelle permet un débit plus élevé ? Pourquoi ? Expliquez le multiplexage en longueur d'onde (WDM). Quel est son intérêt ? Expliquez le multiplexage en longueur d'onde (WDM). Quel est son intérêt ?	15
2.1.47	Quel mécanisme est utilisé par un serveur Web pour conserver de l'état relatif aux usagers ? Expliquez le principe en l'illustrant sur un scénario. Expliquez le fonctionnement de HTTP avec proxy-cache à partir d'un scénario impliquant le client, le serveur et le proxy. Expliquez le gain d'efficacité lorsque l'objet est en cache.	16
2.1.48	Dans un protocole de transport, si l'on numérote les segments modulo 2, montrez par un contreexemple qu'il est également nécessaire de numéroter les acquits pour assurer la fiabilité du transfert. Dans quelle(s) situation(s) le protocole à bit alterné est-il quasiment aussi efficace qu'un protocole à grande fenêtre glissante ? Expliquez.	16
2.1.49	Dans les protocoles à fenêtre glissante de type « selective repeat », quelles sont les relations qui sont satisfaites à tout instant entre les quatre valeurs suivantes : les bords inférieurs et supérieurs des fenêtres de l'émetteur et du récepteur ? Justifiez.	16
2.1.50	Dans TCP, comment fixe-t-on les numéros des premiers segments transmis dans chaque sens d'une connexion ? Si l'on attribuait systématiquement la valeur 0 (par exemple) à ces premiers numéros, quel serait le risque et comment pourrait-on l'éviter en conservant toutefois cette numérotation ? Quel serait l'inconvénient ?	16
2.1.51	Dans quelle(s) situation(s) le protocole de routage à vecteur de distances (DV) risque-t-il de ne pas converger ? Décrivez un comportement pathologique possible à l'aide d'un exemple simple. Comment peut-on atténuer ce phénomène ?	16
2.1.52	Décrivez les principes du protocole de routage inter-domaine BGP. Expliquez comment BGP permet à un réseau périphérique (« stub ») multi-connecté (« multihomed ») de ne pas accepter du trafic de transit.	17
2.1.53	Déterminez analytiquement l'expression de l'efficacité du protocole ALOHA discrétisé (slotted ALOHA) en fonction de la charge du réseau pour un grand nombre de stations actives. On supposera que chaque station émet dans un slot avec une probabilité p . Représentez l'efficacité graphiquement (avec définition des axes), et expliquez la forme de la courbe. La suppression des slots (Cf. ALOHA pur) améliore-t-elle les performances ? Pourquoi ?	17
2.2	Pratique	17

1 Résumé

1.1 Introduction

1.1.1 Qu'est-ce qu'Internet ?

Le réseau est composé de

- **Système d'extrémité (end systems)** est un hôte, qui utilise des applications réseaux.
- **Liens de communication (communication links)** sont des point d'accès WiFi, câbles, ...

Pour communiquer entre eux, les systèmes périphériques utilisent différents *protocoles*. Un protocole est un algorithme décrivant la méthode utilisée pour l'envoi de données à travers le réseau. Ils définissent plusieurs choses, comme le type de routage et de gestion des congestions, c'est-à-dire qu'ils définissent par où acheminer les paquets pour limiter la charge, éviter les obstacles, etc. Certains protocoles garantissent la fiabilité des transferts (tous les paquets arrivent, et dans le bon ordre), d'autres font moins de vérifications mais sont plus rapides, etc.

1.1.2 Périphérie du réseau

La périphérie du réseau (ou network edge) est l'ensemble des applications et systèmes qui utilisent le réseau (par opposition aux liens et routeurs qui forment le cœur du réseau). Elle est généralement organisée selon un de ces deux modèles : Modèle client/serveur Une machine (le serveur) contient les informations et est toujours présente sur le réseau. D'autres machines (les clients) se connectent à celle-ci pour communiquer ; ils peuvent se connecter et se déconnecter à tout moment ; les communications ne se font qu'entre clients et serveur. Modèle peer-to-peer Chaque système est à la fois client et serveur. L'information est décentralisée, et les différents systèmes communiquent entre eux directement.

1.1.3 Aspects physiques

Pour transmettre des données, on peut utiliser le réseau téléphonique classique. Pour cela, on utilise un modem qui permet de (dé)coder l'information. Il existe plusieurs types de modulation : Modulation d'amplitude (AM) Pour coder un signal binaire, on change l'amplitude de l'onde selon que le bit soit à 1 ou à 0 Modulation de fréquence (FM) Pour coder un signal binaire, on change la fréquence de l'onde selon que le bit soit à 1 ou à 0 De plus, pour augmenter le débit, on essaye de coder plusieurs bits d'un coup en combinant ces techniques (on peut par exemple utiliser la phase et la fréquence pour coder plusieurs bits d'un coup). On mesure alors le débit en baud, 1 baud étant 1 symbole/seconde (c'est-à-dire 1 ensemble de bits par seconde)

1.1.3.1 Limites de débit

Avec le réseau téléphonique classique, le baud-rate (quantité de bauds par seconde) est limitée à 4KHz, car c'est la fréquence prévue pour le téléphone (fréquence de la voix humaine). On ne peut donc coder qu'un nombre limité de bits par bauds. De plus, il y a une limite au maintien du signal : au minimum 1/2 période (sous ce seuil, on ne sait plus interpréter le signal de manière univoque car on ne connaît p.e. pas l'amplitude). Enfin, il y a une limitation quand à la quantité de bits codés par baud : on ne peut pas prendre une amplitude trop grande pour coder les différents ensembles de bits, sans quoi on risque de griller le fil de cuivre. De plus, le data-rate (nombre de bits par seconde) est limité aussi, mais par la loi de Shannon. En effet, moins le signal est maintenu longtemps, plus le bruit est important, ce qui limite donc le débit.

1.1.3.2 Réseau DSL

Le réseau DSL utilise la même technique que la connexion dial-up, à la différence qu'on utilise d'autres bandes de fréquences. Cela permet de pouvoir téléphoner et utiliser le réseau simultanément, mais cela nécessite un équipement un peu plus important. On sépare aussi le trafic "upstream" (vers le réseau) du trafic "downstream" (venant du réseau), en donnant au premier une bande de fréquences moins importante, car on suppose qu'on recevra plus de données qu'on en enverra la plupart du temps.

1.1.3.3 Réseau câblé et fibre optique

Cette fois, on n'utilise plus les fils de cuivre du réseau téléphonique comme support, mais le câble TV et de la fibre optique (généralement un mélange des deux). A la différence de l'ADSL, l'accès au réseau par câble est partagé, c'est-à-dire que les différents utilisateurs partagent la même connexion, et donc les données et le débit. C'est fort pratique pour la télévision (usage prévu de la fibre optique/coaxial), mais ça peut poser des problèmes pour Internet (en termes de débit ou de protection des données).

1.1.3.4 Types de câbles

Historiquement, on utilise des câbles composés de deux fils de cuivre torsadés. Ils sont torsadés pour limiter le courant induit (le passage de courant dans le fil crée un champ magnétique, et le passage de ce champ dans la boucle crée un autre courant, plus faible, en sens inverse), et au plus ils sont torsadés, au plus cela a de l'incidence sur le débit offert (on réduit le bruit, donc par la loi de Shannon on peut augmenter le signal). Le câble coaxial fonctionne sur le même principe, à la différence que les conducteurs sont concentriques (il y a un fil de cuivre à l'intérieur, puis une couche d'isolant, un autre fil de cuivre et le plastique qui entoure le câble). Enfin, il y a la fibre optique, qui transporte l'information sous forme d'impulsions lumineuses. Elles permettent le transfert de données à grande vitesse (vitesse de la lumière dans le verre) et sont insensibles aux perturbations électromagnétiques (contrairement aux fils de cuivre), mais il y a un problème lié à la réfraction de la lumière. En effet, si on envoie une série de photons au même instant au départ, ils auront tous un angle de départ différent, donc un angle d'incidence différent aux bords de la fibre. Du coup, ils ne seront pas réfléchis avec le même angle, ce qui signifie que certains feront plus de "rebonds" que d'autres, donc parcourront plus de distance, donc arriveront plus tard. Au final, une impulsion lumineuse arrive dispersée, ce qui ralentit le débit puisqu'il faut attendre l'arrivée de tous les photons avant d'envoyer l'impulsion suivante. Pour régler ce problème, plusieurs types de fibre ont été inventés : Fibre multimode Il s'agit du type de fibre qui ne résout pas le problème décrit : les photons sont dispersés et arrivent avec un certain décalage ; tant pis, on fait avec Fibre monomode Ce type de fibre résout le problème en laissant une zone de propagation extrêmement étroite ($2.4 \mu m$). De cette manière, les photons seront presque parallèles à la fibre ; ils se réfléchissent donc très peu sur les parois et seront peu dispersés Fibre multimode à coefficient variable Ce type de fibre ressemble à la fibre multimode, à la différence que le coefficient de réfraction est différent en tout point de la fibre. De cette manière, on s'arrange pour que les photons qui s'approchent du bord de la fibre soient accélérés par rapport à ceux allant "tout droit". Au final, certains photons auront donc fait plus de chemins que d'autres, mais ils arriveront en même temps puisque leur vitesse varie.

1.2 Couche applicative

1.3 Couche de transport

1.4 Couche réseau

1.5 Couche de liaison

2 Questions et réponses

2.1 Théorie

2.1.1

- Expliquez la différence entre une paire de cuivre torsadée de catégorie 3 et une paire de catégorie 5. Laquelle permet un débit plus élevé et pourquoi ?
- Expliquez la différence entre une fibre optique monomode et une fibre multimode. Laquelle permet un débit plus élevé et pourquoi ?
- Pourquoi utilise-t-on un modem pour transmettre de l'information numérique sur une ligne téléphonique ? Comment module-t-on le signal dans les modems « dial-up » les plus courants ?

(a) ?

(b) ?

(c) ?

2.1.2 Définissez les différents types de « Resource Records » utilisés par le protocole DNS et expliquez leur rôle.

?

2.1.3 10 processus clients communiquent simultanément avec un processus serveur attaché au port 8000.

(a) Combien de sockets vont être ouverts par le serveur si les processus communiquent par UDP ? Pourquoi ?

(b) Même question s'ils communiquent par TCP.

(a) ?

(b) ?

2.1.4

(a) Expliquez le principe d'un protocole à fenêtre glissante SR (Selective Repeat).

(b) Quelle est la taille maximale de la fenêtre, si les trames sont numérotées modulo k ? Pourquoi ?

(a) ?

(b) ?

2.1.5

(a) En première approximation, quels sont les 3 paramètres qui influencent le débit d'une connexion TCP ? Expliquez.

(b) TCP garantit-il un partage équitable des ressources du réseau par les différentes connexions ? Pourquoi ?

(a) ?

(b) ?

2.1.6

(a) Décrivez l'architecture générique d'un routeur et le rôle de chaque composant.

(b) Comment peut-on perdre des paquets dans les ports d'entrée ?

(c) Comment peut-on perdre des paquets dans les ports de sortie ?

(d) Qu'est-ce que le blocage HOL ?

(a) ?

(b) ?

(c) ?

(d) ?

2.1.7 Décrivez le contenu des paquets de routage et leur méthode de diffusion dans le cas des protocoles à état de lien. En quelques mots, en quoi est-ce fondamentalement différent des protocoles à vecteur de distances ?

?

2.1.8 Le protocole de routage interdomaine BGP est plus apparenté à la famille des protocoles de routage intradomaine à vecteur de distances (DV) qu'à celle des protocoles à état de lien (LS).

- (a) Expliquez deux ressemblances importantes entre BGP et un protocole DV.
- (b) Expliquez deux différences importantes entre BGP et un protocole DV, et leur raison d'être.

(a) ?

(b) ?

2.1.9

- (a) Qu'est-ce que le CSMA/CD ? En quoi améliore-t-il le CSMA ?
- (b) Quelle contrainte le CSMA/CD introduit-il par rapport au CSMA ? Pourquoi ?
- (c) IEEE 802.3 (plus communément appelé Ethernet) est un protocole de type CSMA/CD dont la méthode d'accès a été améliorée. Quelle est cette amélioration ?
- (d) Expliquez pourquoi, si l'on veut garder le même format de trame, la méthode CSMA/CD exige de raccourcir le réseau pour atteindre des débits plus élevés. Il est toutefois possible de ne pas respecter cette longueur maximale du réseau, qui devient très contraignante à haut débit. Dans quelles conditions ?

(a) La technologie **Carrier Sense Multiple Access** permet à plusieurs machines d'utiliser un même média de communication. En plus de l'équipement de transmission, une sonde mesure l'état du média. Dans la version simple de CDMA, une machine ne peut transmettre si elle détecte de l'activité sur le média. Cependant, en raison du temps de propagation, surtout sur des longues distances, deux machines pourraient considérer le bus comme libre et commencer à écrire en même temps, pour se retrouver en collision quelques instants après. Le CSMA/CD rajoute la **Collision Detection** : si lorsqu'un bit a été écrit, l'état mesuré est différent, la machine considère qu'il y a collision et arrête immédiatement d'écrire sur le bus. Elle attend ensuite pour un temps déterminé aléatoirement afin que deux machines en collision ne recommencent pas à émettre en même temps.

(b) ?

(c) ?

(d) ?

2.1.10 On ne peut pas dire que les commutateurs Ethernet exécutent un protocole de routage (au sens de la couche 3), mais ils construisent toutefois des tables d'acheminement comme si un protocole de routage était à l'oeuvre. Expliquez comment ces tables sont construites, y compris quand plusieurs commutateurs sont interconnectés.

?

2.1.11 Un chercheur connecte son ordinateur portable à un commutateur Ethernet de son département. Il démarre son browser pour afficher la page web de www.google.com.

- (a) Identifiez les protocoles mis en oeuvre, et dans l'ordre chronologique, entre le moment où l'ordinateur se connecte et le moment où la page d'accueil de Google s'affiche.
- (b) Précisez au passage le rôle de chaque protocole et décrivez-les succinctement.

- (a) ?
- (b) ?

2.1.12

- (a) Expliquez la dispersion de délai dans une fibre optique.
- (b) Quelle en est la conséquence ?
- (c) Dans quel type de fibre la rencontre-t-on ?

- (a) La dispersion du délai se produit lorsque les rayons lumineux sont réfractés ou réfléchis par la couche périphérique de l'âme de la fibre, et que ces rayons ont des trajectoires différentes. Ces trajectoires ayant des longueurs différentes, le temps que mettra la lumière à les parcourir différera, et une impulsion lumineuse très courte pourrait être reçue en plusieurs fragments de l'autre côté.
- (b) La détection des bits formés par ces impulsions lumineuses devient plus difficile, voire impossible, à moins d'espacer les impulsions lumineuses par un délai d'attente. Cependant, ce délai pénalise énormément le débit de la fibre puisque c'est du temps qui pourrait être utilisé pour transférer des données.
- (c) On rencontre ce phénomène dans les fibres multimodes.

2.1.13

- (a) Définissez les différents types de « Resource Records (RR) » utilisés par le protocole DNS et expliquez leur rôle.
- (b) Donnez le scénario d'échange de messages DNS, par la méthode itérative, permettant à un client de trouver l'adresse IP d'un serveur web dont l'URL est `www.company.com`, en indiquant les RR présents dans ces messages. On supposera que les caches DNS sont vides.

- (a) – A : Name est hostname et Value est l'IP de l'hostname. A fournit le mapping standard hostname-to-IP.
- NS : Name est un domaine et Value est le hostname d'un serveur DNS autoritaire qui connaît l'adresse IP du domaine. Il permet à un client de connaître le serveur à contacter pour ce domaine.
- CNAME : Name est un alias pour le hostname présent dans Value.
- MX : Value est le nom canonique d'un serveur mail qui a un hostname alias Name.
- (b) – Le client émet une requête `www.company.com in A` à son serveur DNS local.
- Le serveur local, n'ayant pas l'adresse requise en cache, contacte un des root servers (défini dans sa configuration), avec la même requête.
- Le serveur root contacté lui renvoie alors le nom et l'adresse autoritaire (champs NS et A du serveur principal pour le TLD `.com`)
- Le serveur local réémet à nouveau la même requête vers le serveur du TLD `.com`. Ce serveur TLD renvoie lui aussi les champs NS et A pour le serveur faisant autorité sur le domaine `www.company.com` (par exemple `ns110.ovh.net`).
- Le serveur local contacte alors le serveur autoritaire, qui lui renvoie la zone pour le domaine `company.com`, qui contient un champ CNAME pour `www.company.com`. Si cet champ pointe vers le domaine contenu dans l'enregistrement A de la zone, la recherche s'arrête, le client a obtenu l'ip désirée.
- Sinon, tant qu'un enregistrement A n'a pas été trouvé, le serveur recommence les mêmes étapes à partir du domaine obtenu dans le champ CNAME.

2.1.14

- (a) Expliquez le principe d'un protocole à fenêtre glissante GBN (Go-back N).
- (b) Quelle est la taille maximale de la fenêtre de l'émetteur, si les trames sont numérotées modulo k ? Pourquoi ?
- (c) Citez et expliquez 4 différences apportées par le protocole SR (Selective Repeat).

- (a) Le sender est autorisé à transmettre de multiples packets (si disponible) sans attendre d'ACKs, mais est contraint de ne pas avoir plus de N packets sans ACK dans le pipeline.
- (b) $\text{Window size}(N) \leq \text{seq\#size}(K) - 1$
- (c) – Le receveur de GBN a une fenêtre de 1.
 - Pas de buffer au receveur avec GBN mais bien dans SR pour mémoriser les packets qui ne sont pas dans l'ordre.
 - 1 timer dans GBN pour le plus ancien paquet envoyé mais pas reçu. Chaque packet a son propre timer dans SR.
 - Dans SR, on renvoie que les packets sans ACK alors que dans GBN, on renvoie tout les packets à partir de celui sans ACK.

2.1.15

- (a) Expliquez l'établissement de connexion « 3-way handshake » utilisé dans le protocole de transport TCP, en indiquant les paramètres importants présents dans les échanges et leurs rôles.
- (b) Expliquez avec l'aide d'un exemple pourquoi un « 2-way handshake » ne serait pas suffisant.

- (a) Comme son nom l'indique, le three-way handshake se déroule en trois étapes :
 - SYN : Le client qui désire établir une connexion avec un serveur va envoyer un premier paquet SYN (synchronized) au serveur. Le numéro de séquence de ce paquet est un nombre aléatoire A.
 - SYN-ACK : Le serveur va répondre au client à l'aide d'un paquet SYN-ACK (synchronize, acknowledge). Le numéro du ACK est égal au numéro de séquence du paquet précédent (SYN) incrémenté de un (A + 1) tandis que le numéro de séquence du paquet SYN-ACK est un nombre aléatoire B.
 - ACK : Pour terminer, le client va envoyer un paquet ACK au serveur qui va servir d'accusé de réception. Le numéro de séquence de ce paquet est défini selon la valeur de l'acquittement reçu précédemment p.e. A + 1 et le numéro du ACK est égal au numéro de séquence du paquet précédent (SYN-ACK) incrémenté de un (B + 1).

Une fois le three-way handshake effectué, le client et le serveur ont reçu un acquittement de la connexion. Les étapes 1 et 2 définissent le numéro de séquence pour la communication du client au serveur et les étapes 2 et 3 définissent le numéro de séquence pour la communication dans l'autre sens. Une communication full-duplex est maintenant établie entre le client et le serveur

- (b) Le 2 way handshake n'est pas suffisant car on saute l'étape 2 du 3 way handshake. Si par exemple, un Client A veut parler avec un serveur B, il faut que B sache que A peut entendre ce qu'il dit. Car dans le 2 way handshake, A envoie à B et B répond à A. Mais B ne sait pas si son message est reçu par A.

2.1.16

- (a) Comment l'émetteur TCP détecte-t-il une congestion ?
 - (b) Décrivez le mécanisme de contrôle de congestion de TCP.
 - (c) Quelle distinction TCP fait-il entre congestion légère et congestion sévère ? Comment réagit-il dans chaque cas ?
 - (d) Si on néglige les effets du contrôle de flux, ce contrôle de congestion détermine largement le débit moyen d'une connexion TCP. Quand plusieurs connexions TCP sont en compétition, se partagent-elles la bande passante disponible de façon équitable. Expliquez.
- (a) TCP peut distinguer 2 types de congestions : soit il reçoit 3 ACKs consécutifs pour le même numéro de séquence (donc un des paquets intermédiaire a été perdu, mais les suivants sont passés : **faible congestion**), soit un ACK n'arrive pas dans le temps imparti (timeout, beaucoup de paquets perdus : **congestion sévère**).

- (b) Au démarrage de la transmission, TCP envoie les données avec une fenêtre de taille $1MSS^1$, correspondant au nombre de paquets qui peuvent être "en vol" simultanément. La taille de la fenêtre est doublée à chaque itération (en incrémentant la taille à chaque ACK reçu), de sorte qu'elle a une **croissance exponentielle**. S'il détecte une faible congestion, il divise la taille de la fenêtre par deux et change de mode pour incrémenter la taille de la fenêtre à chaque itération (+1 pour chaque fenêtre totalement envoyée) pour adopter une **croissance linéaire**. Il approche ainsi dichotomiquement la taille moyenne de fenêtre optimale (càd le nombre de paquets "en vol", et donc la vitesse d'envoi). S'il détecte une congestion sévère, il réduit la taille de fenêtre à 1 et recommence en mode de croissance exponentiel. Il peut éventuellement repasser en mode de croissance linéaire lorsqu'il a atteint la moitié de la taille de fenêtre qui a provoqué un timeout (puisque doubler sa taille provoquera probablement de nouveau un timeout).
- (c) Voir (a) et (b).
- (d) Sachant que le timeout est calculé à partir du RTT, deux sessions TCP en compétition pour la même connexion approcheront toujours la vitesse optimale pour leurs RTT. TCP répartira la connexion de façon équitable en ce sens que chaque session utilisera une bande passante inversement proportionnelle à son RTT, évitant la retransmission en bloc de paquets inutiles sur des connexions trop lentes.

2.1.17

- (a) **Enoncez les différents types de matrice de commutation (« switch fabric ») rencontrées dans les routeurs, ainsi que leurs avantages/inconvénients respectifs.**
- (b) **Expliquez la raison d'être et l'inconvénient potentiel d'une bufferisation au niveau des ports d'entrées.**
- (c) **Expliquez la raison d'être d'une bufferisation au niveau des ports de sortie.**

- (a) – via Memory : Les plus simples, les premiers routeurs étaient de simples ordinateurs. Le switch entre les ports d'entrée et sortie étaient fait via le CPU. Lorsqu'un paquet arrive au port d'entrée, le processus de routing l'identifiera via une interruption. Il copiera ensuite les paquets arrivant du buffer d'entrée sur le processeur mémoire. Le processeur extrait ensuite l'adresse de destination, recherche la table appropriée et copie le paquet sur le buffer du port de sortie. Dans les routeurs modernes, la recherche de l'adresse de destination et le stockage du paquet dans la mémoire appropriée est exécuté par les cartes de ligne d'entrée des processeurs.

Avantages :

Inconvénients :

- via un bus : Le port d'entrée transfère les paquets directement sur le port de sortie via un bus partagé sans l'intervention d'un processus de routage. Comme le bus est partagé, seul un paquet est transféré à la fois via le bus. Si le bus est occupé, le paquet arrivant doit attendre dans une file. La bande passante du routeur est limitée par le bus comme chaque paquet doit traverser le bus seul. Exemple : Bus switching CISCO-1900, 3-COM's care builder5.

Avantages :

Inconvénients :

- via un réseau interconnecté : Pour surmonter le problème de la bande passante d'un bus partagé, les commutateurs réseaux en croix sont utilisés. Dans les commutateurs réseaux en croix, port entrées et sorties sont connectés par des bus horizontaux et verticaux. Si nous avons N ports d'entrées et N ports de sorties, on a besoin de 2N bus pour les connecter. Pour transférer un paquet du port d'entrée au port de sortie correspondant, le paquet traverse le bus horizontal jusqu'à une intersection avec un bus vertical qui le conduit à son port de destination. Si le vertical est libre, le paquet est transféré. Mais si le bus vertical est occupé à cause d'une autre entrée, la ligne doit transférer des paquets au même port de destination. Les paquets sont bloqués et font la file sur le même port d'entrée.

Avantages :

Inconvénients :

1. Maximum Segment Size

(b) ???

(c) ???

2.1.18

(a) Expliquez le principe du « Longest Prefix Match » lors de l'acheminement de paquets IP.

(b) Quel est son intérêt ?

(a) Quand on cherche à envoyer une table d'entrée pour une adresse de destination donnée, on utilise le préfixe de la plus longue adresse qui correspond à l'adresse de destination.

(b) Ca sert à détecter le cas où une table donne un sous-réseau.

2.1.19 Le protocole de routage interdomaine BGP est plus apparenté à la famille des protocoles de routage intradomaine à vecteur de distances (DV) qu'à celle des protocoles à état de lien (LS).

(a) Expliquez deux ressemblances importantes entre BGP et un protocole DV.

(b) Expliquez deux différences importantes entre BGP et un protocole DV, et leur raison d'être.

(a) ?

(b) – BGP mémorise toutes les routes vers toutes les destination : récupération rapide lorsqu'une destination devient inaccessible par la route initialement choisie.

– BGP construit des routes sans boucle :

– Le chemin suivi est décrit explicitement à l'aide des AS traversés.

– Les boucles sont facilement détectées.

2.1.20

(a) Expliquez le rôle et le principe général des codes détecteurs d'erreur.

(b) Pourquoi ne peuvent-ils être efficaces à 100% ?

(c) Donnez un exemple de code détecteur d'erreur plus élaboré que le bit de parité, et expliquez son principe.

(a) ?

(b) ?

(c) ?

2.1.21

(a) Expliquez le principe du multiplexage en longueur d'onde (WDM). Quel est son intérêt ?

(b) Comparez WDM aux techniques classiques de multiplexage TDM et FDM.

(a) Dans WMD, chaque station reçoit deux canaux. Un canal de faible bande passante pour la signalisation de la station et un canal d'une bande passante plus large pour envoyer et recevoir des trames. Chaque canal est divisé en groupes de slots. Appelons m le nombre de slots du canal de signalisation. L'expression $n+1$ indique le nombre de slots du canal de données : n slots de données utiles et un slot supplémentaire pour que la station renseigne sur son état, principalement pour indiquer les slots libres sur chacun de ses deux canaux. Sur ces deux canaux, la séquence de slots se répète continuellement, avec un marquage particulier pour le slot 0, afin que les stations arrivant plus tard puissent le repérer. Toutes les stations sont synchronisées au moyen d'une seule horloge pilote. Le protocole gère 3 classes de trafic :

– Un trafic à débit constant en mode connecté, tel celui d'une vidéo compressée.

- Un trafic à débit variable en mode connecté, tel celui d'un transfert de fichier.
 - Un trafic constitué de datagrammes en mode non connecté, tels des paquets UDP.
- (b) Pour les deux protocoles orientés connexion, l'idée de base est qu'une station A souhaitant communiquer avec une station B doit au préalable insérer une trame de demande de connexion dans un slot libre sur le canal de signalisation de B. Si B accepte, la communication peut avoir lieu par l'intermédiaire du canal de données de A.

2.1.22 Vous créez votre entreprise « MeMyself&I » et vous obtenez le nom de domaine « memyselfandi.com ». Vous souhaitez déployer votre propre serveur DNS pour ce domaine (dns.memyselfandi.com, 111.111.111.111), ainsi qu'un serveur Web www.memyselfandi.com, 111.111.111.112).

- (a) Quelles informations doivent être ajoutées dans la hiérarchie DNS et à quel niveau ? Soyez précis.
- (b) Donnez un scénario typique d'échange de messages DNS permettant à un client de trouver l'adresse IP de votre serveur web, en précisant bien les éléments importants des messages DNS. On supposera que les caches DNS sont vides.

(a) ?

(b) ?

2.1.23

- (a) Pourquoi la couche de transport (UDP et TCP) comporte-t-elle une fonction de démultiplexage ?
- (b) Décrivez les techniques de démultiplexage effectuées par UDP et TCP en mettant bien en évidence leurs différences ?

- (a) Ports can provide multiple endpoints on a single node. For example, the name on a postal address is a kind of multiplexing, and distinguishes between different recipients of the same location. Computer applications will each listen for information on their own ports, which enables the use of more than one network service at the same time. It is part of the transport layer in the TCP/IP model, but of the session layer in the OSI model.
- (b) In TCP, the receiver host uses all of source IP, source port, destination IP and destination port to direct datagram to appropriate socket. While in UDP, the receiver only checks destination port number to direct the datagram.

2.1.24

- (a) Donnez 4 éléments majeurs des protocoles « Go-Back-N » et « Selective Repeat » qui permettent de les différencier.
- (b) Pour chacun de ces éléments pris indépendamment, indiquez si TCP s'apparente davantage à l'un d'eux. Expliquez.
- (c) Quelle optimisation supplémentaire, liée au contrôle d'erreur, TCP y apporte-t-il ?

(a) ?

(b) ?

(c) ?

2.1.25 Expliquez le principe de NAT et la structure d'une table NAT.

Lorsqu'un paquet est envoyé vers l'extérieur, il passe par un dispositif NAT qui convertit l'adresse IP interne en adresse IP officielle de l'entreprise. Le dispositif NAT et un pare-feu sont souvent combinés dans le même équipement, offrant ainsi une certaine sécurité en contrôlant précisément ce qui entre sur le réseau et en sort.

Structure d'une table NAT :

IP interne	IP externe	Durée (s)	Réutilisable ?
------------	------------	-----------	----------------

2.1.26 Quand des flux TCP et UDP partagent un même lien congestionné, comment réagissent ces deux types de flux et quelles en sont les conséquences ?

?

2.1.27

- (a) Nommez et expliquez succinctement les 2 grandes familles de protocoles de routage intradomaine (IGP) en insistant sur leurs différences.
- (b) Expliquez en quoi et pourquoi le protocole de routage interdomaine de l'Internet (BGP) est différent des protocoles de routage intradomaine (IGP) déployés dans les divers systèmes autonomes (AS) qui composent l'Internet.

(a) ?

(b) ?

2.1.28 Expliquez comment un routeur construit les entrées de sa table d'acheminement pour les préfixes IP extérieurs à son domaine.

?

2.1.29

- (a) Décrivez le protocole CSMA.
- (b) Pourquoi et comment a-t-il été amélioré ?
- (c) Citez les paramètres qui caractérisent un réseau CSMA. Quelle relation entre ces paramètres faut-il viser pour que le réseau CSMA ait des performances acceptables ? Expliquez.

(a) ?

(b) ?

(c) ?

2.1.30 Considérez 3 réseaux Ethernet (N_1 , N_2 et N_3), un commutateur Ethernet (C) et un routeur (R) interconnectés selon une topologie en ligne $N_1-C-N_2-R-N_3$. Une station H_A (d'adresse IP_A) est attachée au réseau N_1 (par l'adresse MAC_A) et une station H_B (d'adresse IP_B) est attachée au réseau N_3 (par l'adresse MAC_B). C a deux adresses MAC : MAC_{11} sur N_1 et MAC_{12} sur N_2 . R a deux adresses MAC et deux adresses IP : MAC_{22} et IP_2 sur N_2 et MAC_{23} et IP_3 sur N_3 .

- (a) Dessinez la configuration. H_A envoie un paquet IP à H_B . Si l'on suppose que les correspondances entre adresses IP et MAC sont connues de tous, décrivez les trois trames qui circulent respectivement sur les réseaux N_1 , N_2 et N_3 en vous limitant aux champs d'adresses des trames et aux champs d'adresses et de TTL (Time To Live) du paquet IP contenu dans la trame. Justifiez.

- (b) Par quel protocole les correspondances entre adresses *IP* et *MAC* ont-elles été découvertes ? Décrivez les échanges de ce protocole qui réalisent les mises en correspondance nécessaires lorsque H_A envoie son paquet *IP* à H_B . Mentionnez toutes les adresses présentes dans les messages échangés.

(a) ?

(b) ?

2.1.31 Citez une fonction majeure de chacune des 5 couches de la pile de protocoles Internet.

?

2.1.32

- (a) Pourquoi est-il plus difficile de fixer la durée du timer de retransmission de TCP que celle du timer de retransmission d'un protocole de liaison de donnée ?
- (b) Comment fixe-t-on la durée du timer de retransmission de TCP ?

(a) ?

(b) ?

2.1.33 Expliquez la raison d'être des protocoles DHCP et NAT, et expliquez leur fonctionnement à l'aide de scénarios typiques.

?

2.1.34

- (a) Expliquez comment les commutateurs Ethernet apprennent où se trouvent les stations et par quel type d'adresse ils les identifient.
- (b) Comment les pannes de stations ou leur mobilité sont-elles prises en compte ?
- (c) En quelques mots, quelle contrainte topologique doit être respectée pour que cet apprentissage fonctionne, et comment la réalise-t-on ?

(a) ?

(b) ?

(c) ?

2.1.35 Citez et définissez les différentes sources de délai que subit un paquet dans un réseau datagramme.

?

2.1.36

- (a) Décrivez sommairement le fonctionnement du système DNS.
- (b) Comparez les deux modes de fonctionnement du protocole (avantages et inconvénients).

(a) ?

(b) ?

2.1.37

- (a) Expliquer les principes de la programmation socket donnant accès aux services TCP et UDP.
- (b) Quelles sont les différences importantes entre ces deux API ?
- (c) Dans une entité de transport, comment les sockets TCP et UDP sont-ils identifiés ? Pourquoi ?

(a) ?

(b) ?

(c) ?

2.1.38

- (a) Dans un protocole de transport, si l'on numérote les segments modulo 2, montrez par un contreexemple qu'il est également nécessaire de numérotter les acquits pour assurer la fiabilité du transfert.
- (b) Dans quelle(s) situation(s) le protocole à bit alterné est-il quasiment aussi efficace qu'un protocole à grande fenêtre glissante ? Expliquez.

(a) ?

(b) ?

2.1.39

- (a) Expliquez les circonstances dans lesquelles l'émetteur TCP peut recevoir trois doublons d'acquits venant du récepteur TCP.
- (b) Décrivez deux actions importantes de l'émetteur TCP lorsque cela se produit et expliquez-en les raisons.

(a) ?

(b) ?

2.1.40

- (a) Expliquez le principe général du contrôle de *flux* de TCP.
- (b) Expliquez deux mécanismes associés ayant pour but de permettre à TCP de s'adapter aux spécificités des applications ou de se protéger vis-à-vis de celles-ci.

(a) ?

(b) ?

2.1.41 Combien d'adresses IP doit-on attribuer à un routeur ? Pourquoi ?

?

2.1.42

- (a) Considérez un protocole de routage à états de liens (link state). Décrivez le contenu des paquets de routage, expliquez le rôle de chaque champ, et décrivez la méthode de diffusion des paquets.
- (b) En quelques mots, en quoi est-ce fondamentalement différent des protocoles à vecteur de distances ?

(a) ?

(b) ?

2.1.43

- (a) Décrivez les principes du protocole de routage inter-domaine BGP.
- (b) Expliquez comment BGP permet à un réseau périphérique (« stub ») multi-connecté (« multihomed ») de ne pas accepter du trafic de transit.

(a) ?

(b) ?

- 2.1.44** Sachant que la couche de transport est équipée de mécanismes (Cf. TCP) pour récupérer les erreurs de bout-en-bout, pourquoi la couche de liaison de données implémente-t-elle aussi toute une série de fonctions de ce type, comme la détection d'erreurs, voire même la retransmission de trames erronées dans certains cas.

?

2.1.45

- (a) Dans un réseau local composé de plusieurs segments Ethernet interconnectés par des commutateurs Ethernet, un ordinateur peut-il conserver son adresse IP si on le change de segment ? Pourquoi ?
- (b) En est-il de même si les segments sont interconnectés par des routeurs ? Pourquoi ?
- (c) Pourquoi est-il plus intéressant d'interconnecter des segments Ethernet par des commutateurs Ethernet plutôt que par des hubs ?

(a) ?

(b) ?

(c) ?

2.1.46

- (a) Expliquez la différence entre une fibre optique multimode et une fibre monomode.
- (b) Laquelle permet un débit plus élevé ? Pourquoi ?
- (c) Expliquez le multiplexage en longueur d'onde (WDM). Quel est son intérêt ?
- (d) Comparez TDM, FDM et WDM.

(a) ?

(b) ?

(c) ?

(d) ?

2.1.47

- (a) Quel mécanisme est utilisé par un serveur Web pour conserver de l'état relatif aux usagers ? Expliquez le principe en l'illustrant sur un scénario.
- (b) Expliquer le fonctionnement de HTTP avec proxy-cache à partir d'un scénario impliquant le client, le serveur et le proxy. Expliquez le gain d'efficacité lorsque l'objet est en cache.

(a) ?

(b) ?

2.1.48

- (a) Dans un protocole de transport, si l'on numérote les segments modulo 2, montrez par un contreexemple qu'il est également nécessaire de numérotter les acquits pour assurer la fiabilité du transfert.
- (b) Dans quelle(s) situation(s) le protocole à bit alterné est-il quasiment aussi efficace qu'un protocole à grande fenêtre glissante ? Expliquez.

(a) ?

(b) ?

- 2.1.49** Dans les protocoles à fenêtre glissante de type « selective repeat », quelles sont les relations qui sont satisfaites à tout instant entre les quatre valeurs suivantes : les bords inférieurs et supérieurs des fenêtres de l'émetteur et du récepteur ? Justifiez.

?

2.1.50

- (a) Dans TCP, comment fixe-t-on les numéros des premiers segments transmis dans chaque sens d'une connexion ?
- (b) Si l'on attribuait systématiquement la valeur 0 (par exemple) à ces premiers numéros, quel serait le risque et comment pourrait-on l'éviter en conservant toutefois cette numérotation ? Quel serait l'inconvénient ?

(a) ?

(b) ?

2.1.51

- (a) Dans quelle(s) situation(s) le protocole de routage à vecteur de distances (DV) risque-t-il de ne pas converger ?
- (b) Décrivez un comportement pathologique possible à l'aide d'un exemple simple.
- (c) Comment peut-on atténuer ce phénomène ?

(a) ?

(b) ?

(c) ?

2.1.52

- (a) Décrivez les principes du protocole de routage inter-domaine BGP.
- (b) Expliquez comment BGP permet à un réseau périphérique (« stub ») multi-connecté (« multihomed ») de ne pas accepter du trafic de transit.

(a) ?

(b) ?

2.1.53

- (a) Déterminez analytiquement l'expression de l'efficacité du protocole ALOHA discrétisé (slotted ALOHA) en fonction de la charge du réseau pour un grand nombre de stations actives. On supposera que chaque station émet dans un slot avec une probabilité p .
- (b) Représentez l'efficacité graphiquement (avec définition des axes), et expliquez la forme de la courbe.
- (c) La suppression des slots (Cf. ALOHA pur) améliore-t-elle les performances ? Pourquoi ?

(a) ?

(b) ?

(c) ?

2.2 Pratique