INFO-F303 - Réseaux
Guy Leduc
Résumé du cours

Rodrigue Van Brande

Julien Vanbergen

4 janvier 2017

Table des matières

1 Abréviations **6**

2 Questions et réponses **10**

2.1 Théorie . . . 10

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 ? . . . 10

2.1.2 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 ? . . . 10

2.1.3 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). . . . 11

2.1.4 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

2.1.5 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. . . . 11

2.1.6 Le protocole de routage inter-domaine BGP est plus apparenté à la famille des protocoles de routage intra-domaine 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. . . . 11

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 ? . . . 12

2.1.8 Le protocole de routage inter-domaine BGP est plus apparenté à la famille des protocoles de routage intra-domaine 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. . . . 12

2.1.9 Nommez et expliquez succinctement les 2 grandes familles de protocoles de routage intra-domaine (IGP) en insistant sur leurs différences. Expliquez en quoi et pourquoi le protocole de routage inter-domaine de l'Internet (BGP) est différent des protocoles de routage intra-domaine (IGP) déployés dans les divers systèmes autonomes (AS) qui composent l'Internet. . . . 12

2.1.10 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. . . . 12

2.1.11 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. . . . 12

2.1.12 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. . . . 13

2.1.13 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 ? . . . 13

2.1.14 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 ? 13
2.1.15 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 ? 14
2.1.16 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 inter-connectés. 14
2.1.17 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. 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. 14
2.1.18 Expliquez la dispersion de délai dans une fibre optique. Quelle en est la conséquence ? Dans quel type de fibre la rencontre-t-on ? 14
2.1.19 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 www.company.com, *en indiquant les RR présents dans ces messages.* On supposera que les caches DNS sont vides. 15
2.1.20 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. 15
2.1.21 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 ? 16
2.1.22 Enoncez 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. 16
2.1.23 Expliquez le principe du « Longest Prefix Match » lors de l'acheminement de paquets IP. Quel est son intérêt ? 17
2.1.24 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. 17
2.1.25 Expliquez le principe du multiplexage en longueur d'onde (WDM). Quel est son intérêt ? Comparez WDM aux techniques classiques de multiplexage TDM et FDM. 17
2.1.26 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). 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. 18
2.1.27 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 ? 18
2.1.28 Expliquez le principe de NAT et la structure d'une table NAT. 18

2.1.29 Quand des flux TCP et UDP partagent un même lien congestionné, comment réagissent ces deux types de flux et quelles en sont les conséquences ? 18
2.1.30 Expliquez comment un routeur construit les entrées de sa table d'acheminement pour les préfixes IP extérieurs à son domaine. 19
2.1.31 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. 19
2.1.32 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. 19
2.1.33 Citez une fonction majeure de chacune des 5 couches de la pile de protocoles Internet. . 19
2.1.34 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 ? 19
2.1.35 Expliquez la raison d'être des protocoles DHCP et NAT, et expliquez leur fonctionnement à l'aide de scénarios typiques. 19
2.1.36 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 ? . 20
2.1.37 Citez et définissez les différentes sources de délai que subit un paquet dans un réseau datagramme. 20
2.1.38 Décrivez sommairement le fonctionnement du système DNS. Comparez les deux modes de fonctionnement du protocole (avantages et inconvénients). 20
2.1.39 Expliquer 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 ? 20
2.1.40 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. 20
2.1.41 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. 21
2.1.42 Expliquez le principe général du contrôle de *flux* 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. 21
2.1.43 Combien d'adresses IP doit-on attribuer à un routeur ? Pourquoi ? 21
2.1.44 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 ? 21

2.1.45 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. 21
2.1.46 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 ? 21
2.1.47 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 ? 22
2.1.48 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. 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. 22
2.1.49 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. 22
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 ? 22
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 ? 23
2.1.52 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 ? 23
2.2 Pratique 23

1 Abréviations

AIMD *Additive Increase, Multiplicative Decrease* Algorithme de contrôle de congestion de TCP. L'approche de TCP consiste à faire en sorte que chaque expéditeur régule sa vitesse d'envoi en fonction du niveau de congestion perçu au sein du réseau. Le phénomène de perte (qui est la principale conséquence d'une congestion sur le réseau) est identifié soit par l'expiration du temps imparti, soit par la réception de trois accusés de réception identiques de la part du destinataire. L'algorithme de contrôle de congestion de TCP présente trois composantes principales : Un accroissement additif et une décroissance multiplicative, un départ lent et une réaction au phénomène d'expiration du temps imparti. Avec le contrôle de congestion de TCP, chaque pôle maintient une variable dite fenêtre de congestion appelée CongWin, qui impose une limite au rythme auquel l'expé- diteur est autorisé à charger des données sur le réseau. TCP a recours à une approche décroissante multiplicative, c'est-à-dire que la valeur CongWin est diminuée de moitié après chaque phénomène de perte, avec une limite en la valeur de 1 MSS. Une fois le phénomène de congestion résorbé, TCP doit pouvoir agir pour augmenter le taux d'envoi. TCP procède donc à un agrandissement progressif linéaire de sa fenêtre de congestion. Cet algorithme est appelé algorithme AIMD (Additive Increase, Multiplicative Decrease). Au début d'une connexion, la variable CongWin a une valeur de un MSS, ce qui fait un taux d'envoi de MSS/RTT. Mais le réseau dispose peut-être d'un débit bien plus important, et il serait idiot de faire une progression linéaire jusqu'à cette valeur (ce qui peut prendre beaucoup de temps sur une connexion disposant d'un très bon débit). L'expéditeur aura donc recours à une accélération exponentielle en doublant la valeur de CongWin à chaque RTT, et ce jusqu'aux premiers phénomènes de perte, moment auquel il divise brusquement CongWin par deux et passe au mode de progression linéaire décrit ci-dessus. Cette phase initiale est appelée départ lent. Il reste un point important à détailler : TCP fait une distinction entre un phénomène de perte signalé par trois accusés identiques (ce qui indique une perte de seulement quelques paquets sur le réseau) et un phénomène de perte décelé par expiration du temps imparti (qui laisse plus croire à une grosse congestion du réseau qui aurait perdu tout ce qui a été envoyé). Dans le premier cas, il se contente de diviser la fenêtre de congestion par deux, et de continuer une progression linéaire, comme nous l'avons déjà précisé (on parle de récupération rapide). Dans le second cas, l'expéditeur revient au départ lent, ramenant la taille de la fenêtre de congestion à un seul MSS. De plus TCP garde le contrôle sur les processus au moyen d'une variable Seuil, qui détermine la taille que doit atteindre la fenêtre avant que ne cesse la phase de départ lent et ne commence la phase d'évitement de congestion. Cette variable prend initialement une valeur élevée (65 Ko en pratique), et se trouve divisée par deux lors des phénomènes de perte. L'algorithme de contrôle de congestion de TCP opère donc de la façon suivante :

- Tant que la taille de la fenêtre de congestion est inférieure à la valeur du seuil, l'expéditeur est en phase de départ lent et la fenêtre connaît une croissance exponentielle.
- Une fois la valeur du seuil dépassée, l'expéditeur entre dans la phase d'évitement de congestion durant laquelle la fenêtre s'accroît de manière linéaire.
- Lorsqu'il y a trois accusés de réception identiques, la valeur du seuil est réglée à la moitié de la taille de la fenêtre de congestion en cours et cette dernière est portée à la valeur du seuil.
- Lors de l'expiration du temps imparti, la valeur du seuil est réglée à la moitié de la fenêtre de congestion en cours et cette dernière est portée à 1 MSS.

Le débit à un instant donné sera CongWin/RTT, mais il est continuellement en dents de scie, il est donc naturel de se demander quel est le débit moyen d'une connexion TCP sur une durée plus longue. Notons w la taille de la fenêtre de congestion (en octets) et un temps aller-retour de RTT secondes. Le débit est approximativement w/RT T. Appelons W la valeur atteinte par w lorsqu'un phénomène de perte se présente. En partant du principe que RTT et W sont relativement constants dans le temps, le débit varie entre 1 2W/RTT et W/RTT. Le débit moyen sur la connexion sera donc à peu près $\frac{3}{4}$W/RTT.

API *Application Programmers' Interface.* Interface entre l'application et le réseau.

ARP *Autonomous Systems Protocol.* Protocole permettant la conversation des adresses LAN et IP.

AS *Autonomous Systems.* Régions de routeurs s'autogérant.

ASN *Autonomous System Number.* Numéro d'identification unique des systèmes autonomes BGP.

BGP *BGP Protocol.* Le protocole de routage inter-domaine BGP. BGP se définit comme un protocole à vecteur de chemin. Les routeurs BGP voisins, connus sous le nom de partenaires BGP, s'échangent des informations détaillées sur les chemins à emprunter (plutôt que des indications sur la distance comme dans les protocoles à vecteur de distance). BGP est un protocole distribué, dans le sens où les routeurs BGP ne communiquent qu'avec leurs voisins directs. Le routage BGP se fait en direction de réseaux de destination plutôt qu'en direction de routeurs ou de serveurs ; une fois qu'un datagramme a atteint son réseau de destination,

il est pris en charge par le routage interne de celui-ci jusqu'à son destinataire final. Dans le cadre de BGP, les systèmes autonomes s'identifient à l'aide d'un numéro de système autonome unique (ASN, Autonomous System Number). BGP assure trois grandes fonctions :

- Réception et filtrage d'annonces de parcours en provenance de routeurs voisins. Les annonces de parcours sont des promesses que tout paquet reçu sera transmis au prochain routeur placé sur le chemin vers la destination. Il en profite pour supprimer les chemins le faisant passer par lui-même (ce qui provoquerait des boucles de routage).
- Sélection de chemin. Un routeur BGP peut recevoir plusieurs annonces de parcours différentes pour un même système autonome, parmi lesquelles il doit faire un choix.
- Envoi d'annonces de parcours aux routeurs voisins.

BIND *Berkeley Internet Name Domain.* Logiciel standard pour les serveurs de nom Unix.

CARP *Cache Array Routing Protocol.*

CDMA *Code Division Multiple Access.* Protocole d'accès multiple par répartition de code.

CDN *Content Distribution Networks.* Réseaux de distribution de contenu.

CIDR *Classless InterDomain Routing.*

DHCP *Dynamic Host Configuration Protocol.* Protocole d'obtention d'IP automatique. Nous savons déjà que le protocole DHCP (Dynamic Host Configuration Protocol) est souvent utilisé pour l'attribution dynamique d'adresses IP. Il s'agit d'un protocole client-serveur. Normalement chaque réseau est doté d'un serveur DHCP. Ce protocole propose un processus en quatre étapes aux hôtes cherchant à se connecter à un réseau :

- Détection d'un serveur DHCP : Un nouvel arrivant envoie un message de détection de DHCP, via UDP, avec le numéro d'accès 67. Le nouvel arrivant ne connaissant aucune adresse IP du réseau, il l'envoie sur l'adresse de diffusion 255.255.255.255 avec pour adresse d'origine 0.0.0.0. Ce message sera reçu par toutes les interfaces du réseau, y compris celle(s) du/des serveur(s) DHCP.
- Proposition(s) du serveur DHCP : Le serveur DHCP répond d'un message de proposition DHCP, contenant une adresse IP, le masque de sous-réseau et une indication sur la durée de validité de l'adresse fournie.
- Requête DHCP : Le nouvel arrivant fait son choix parmi les propositions et y répond par une requête DHCP.
- Acquittement DHCP. Le serveur répond à cette requête au moyen d'un acquittement (ACK) qui confirme les paramètres sollicités.

Le client peut alors commencer à utiliser son adresse IP pendant la durée impartie.

DNS *Domain Name System.* Annuaire de correspondance entre les noms de domaines et les adresses IP.

CRC *Cyclic Redundancy Check.* Champ de détection des erreurs au sein d'une trame Ethernet.

DSL *Digital Subscriber Line.* Ligne d'abonné numérisée.

FTP *File Transfert Protocol.* Protocole de transfert de fichiers.

GBN *Go-Back-N.* Protocole de transport à fenêtre glissante.

GPRS *General Packet Radio Service.* Technologie d'accès mobile par paquets.

HFC *Hybrid Fiber Coaxial Cable.* Liaison hybride fibre et coaxial (câble).

HTTP *Hypertext Transfert Protocol.*

ICMP *Internet Control Message Protocol.* Protocole de rapport d'erreur de couche réseau. Le protocole ICMP (Internet Control Message Protocol) est utilisé par les serveurs, routeurs et passerelles pour échanger des informations de couche réseau, principalement des rapports d'erreurs. Bien que les messages soient véhiculés par des paquets IP, IMCP est souvent considéré comme partie intégrante de la couche IP, bien qu'il appartienne architecturalement à une couche supérieure. Lorsqu'un serveur reçoit un paquet IP annon- çant ICMP (champ Type de service), il procède au démultiplexage en direction d'ICMP, de la même manière qu'en direction de TCP ou UDP.

IP *Internet Protocol.*

IETF *Internet Engineering Task Force.* Groupe d'étude de l'ingénierie de l'Internet.

ISP *Internet Service Provider.* Fournisseur d'accès à l'Internet.

FDM *Frequency Division Multiplexing.* Multiplexage fréquentiel.

LAN *Local Area Network.* Réseau local à grande vitesse.

MTU *Maximum Transfert Unit.* Volume maximum de données qui peut être porté par un paquet de la couche liaison.

NAP *Network Access Points.* Points d'accès au réseau.

NAT *Network Address Translation.* Traduction d'adresses réseau. Dès que l'on souhaite mettre en place un réseau local reliant différents ordinateurs d'un même espace de travail, il faut obtenir autant d'adresses IP

auprès de son fournisseur d'accès. Mais que se passe-t-il s'il a déjà alloué les adresses contiguës à celles du réseau en extension à un autre client ? C'est pour régler ce genre de problème qu'existe la traduction d'adresse réseau (NAT, network Address Translation). La figure ci-dessous représente le fonctionnement d'un routeur NAT. Ce routeur est doté d'une interface appartenant au réseau domestique et une interface orientée vers l'Internet. Le type d'adressage s'effectuant au sein du mini-réseau est exactement le même que celui que nous avons déjà décrit : les quatre interfaces se partagent le réseau 10.0.0.0/24. Le routeur doté d'une fonction NAT se comporte vis-à-vis du monde extérieur comme un équipement isolé muni d'une seule adresse IP 138.76.29.7 et tout trafic entrant doit être doté de cette adresse de destination. Le routeur NAT obtient son adresse auprès de son FAI via DHCP et il a recours à un DHCP local pour l'attribution des adresses IP du mini-réseau. Lorsqu'un datagramme arrive de l'extérieur, le routeur a besoin d'une table de traduction d'adresses pour savoir à quel hôte du mini-réseau le remettre. Il utilisera pour ça une astuce avec les numéros de port. Prenons l'exemple de l'hôte d'interface 10.0.0.1 qui sollicite une page Web (accès 80) sur l'interface 128.119.40.186. Le terminal 10.0.0.1 assigne à son datagramme le numéro d'accès d'origine (arbitraire) 3345 et l'envoie au travers du réseau local. Sur réception de ce datagramme, le routeur NAT remplace l'adresse IP de l'expéditeur (10.0.0.1) par son adresse orientée vers l'Internet (138.76.29.7), choisit un port arbitraire (5001 par exemple) nouvellement créé, retient ces correspondances et envoie le nouveau datagramme sur l'Internet. Le serveur Web renverra naturellement les données de la requête sur l'interface 138.76.29.7 et l'accès 5001, qui seront converties en 10.0.0.1 et 3345 par le serveur NAT et renvoyées sur le réseau local.

OSPF *Open Shortest Path First.* Protocole de routage avec priorité au plus court chemin. Tout comme RIP, OSPF (conçu pour succéder à RIP) sert au routage interne, et possède certaines propriétés avancées. A la base il s'agit d'un protocole à état de lien ayant recours à la technique d'inondations d'informations et à l'algorithme de Dijkstra. Les routeurs élaborent une carte topologique complète du système autonome puis déterminent un arbre de plus court chemin vers tous les réseaux du système, se considérant comme noeud racine. C'est à partir de cet arbre que peuvent être formées les tables de routage. Les valeurs de liaisons individuelles sont laissées à l'administrateur. Les routeurs communiquent leurs informations de routage à tous les routeurs de leur système autonome. Ces informations sont diffusées à chaque changement d'état d'une liaison et de manière périodique. OSPF apporte les innovations suivantes :

- Sécurité : Tous les échanges entre routeurs OSPF font l'objet d'une authentification, ce qui signifie que seuls les routeurs dignes de confiance peuvent participer au protocole.
- Chemins de coût égal : OSPF ne s'oppose pas à ce que différents chemins de même coût soient empruntés pour rejoindre une même destination.
- Multidiffusion.
- Support d'une hiérarchie : Capacité de ce protocole à structurer un système autonome de manière hiérarchique (voir ci-dessous).

Un système autonome OSPF peut être divisé en différents domaines, utilisant chacun son propre algorithme de routage d'information d'état de lien et communiquant ses informations à tous les routeurs du même domaine. Les détails internes à un domaine spécifique restent ainsi invisibles aux autres routeurs. Au sein de chaque domaine OSPF, un ou plusieurs routeurs frontaliers sont responsables de l'acheminement des paquets vers l'extérieur. Par ailleurs, chaque système autonome dispose d'un domaine fédérateur ayant pour fonction l'acheminement du trafic d'un domaine à un autre et rassemblant donc tous les routeurs frontaliers, ainsi qu'éventuellement d'autres routeurs. Le dessin ci-dessous illustre parfaitement cette situation.

POP *Point Of Presence.* Point de présence d'un ISP.

PPP *Point-to-Point Protocol.* Protocole de la couche liaison pour les liaisons point à point.

P2P *Peer-to-Peer.*

PDA *Personal Digital Assistant.*

RFC *Request for Comments.* Format de documents contenant les normes IETF.

RIP *Routing Information Protocol.* Protocole d'information de routage. RIP est un protocole à vecteur de distance très similaire à celui vu précédemment. Sa version originale a recours au nombre de bonds comme mesure du coût d'un chemin donné, attribuant à chaque liaison la même valeur unitaire, avec un coût par chemin ne pouvant dépasser 15 (ce qui limite RIP à des systèmes d'une portée inférieure à 15 bonds). Les informations échangées entre routeurs voisins ont lieu à peu près toutes les 30 secondes grâce au message de réponse RIP, contenant une liste pouvant aller jusqu'à 25 réseaux de destination au sein du système autonome. Les tables de routage au sein des routeurs sont constituées de trois colonnes : le réseau de destination, l'identité du prochain routeur pour cette destination, et enfin le nombre de bonds jalonnant le chemin. Les routeurs s'échangent des annonces environ toutes les 30 secondes. Si un routeur ne reçoit pas de nouvelles de la part d'un voisin au moins une fois toutes les 180 secondes, celui-ci est considéré comme hors de portée, la table est

alors modifiée et les voisins informés des modifications. S'il le souhaite un routeur peut interroger directement ses voisins au sujet du coût de ses chemins vers une destination donnée.

RTT *Round-trip Time.* Temps nécessaire à un petit paquet pour faire un aller-retour entre un client et un serveur.

SMTP *Simple Mail Transfert Protocol.* Protocole de gestion des systèmes de messageries électroniques.

TCP *Transmission Control Protocol.* Protocole de transfert de données fiable orienté connexion.

TDM *Time Division Multiplexing.* Multiplexage temporel.

TTL *Time To Live.* Durée de vie d'un datagramme.

UDP *User Datagram Protocol.* Protocole de transfert de données non fiable sans connexion.

URL *Uniform Resource Location.* Adresse propre d'un fichier sur le Web.

UTP *Unshielded Twisted Pair.* Paire torsadée non blindée.

WAP *Wireless Access Protocol.* Protocole d'accès sans fil.

WLAN *Réseau LAN sans fil.*

WML *WAP Markup Language.* Equivalent d'HTML pour le WAP.

2 Questions et réponses

2.1 Théorie

2.1.1

(a) 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 ?

(b) Expliquez la différence entre une fibre optique monomode et une fibre multimode. Laquelle permet un débit plus élevé et pourquoi ?

(c) 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) On utilise des paires de cuivre torsadées car deux fils de cuivres parallèles créent un champ magnétique proportionnel à leur distance, ce qui induit un grand courant, et donc beaucoup de bruit. Or lorsqu'ils sont torsadés, les torsades créent chacunes leur champs magnétique et courant induit et les flux induits s'inversent dans chaque boucle adjacente. Les effets sont donc atténués. Plus les torsades sont petites, plus l'effet est efficace. Les fils de catégorie 5 sont plus torsadé que ceux de catégorie 3 et donc plus efface (100 Mbps contre 10 Mbps)

(b) La fibre optique permet de transmettre des nuages de photons, au contraire des câbles conventionnels qui transmettent des signaux électriques. Elle est composée d'un câble en verre inclus dans un autre, les deux ayant des indices de réfractions différents. Ceci permettant de piéger les signaux par réfraction. Les photons ne peuvent plus quitter le câble et se retrouvent bloqués dans le câble du centre. On utilise plusieurs types de fibre :

Multimode Le problème de la fibre optique est que les photons émis dans un même nuage prennent des trajectoires différentes (en fonction des angles de réflexions au sein du câble), les photons du signal n'arrivent donc pas en même temps au bout du câble (ni dans la même partie). Or plus la distance est longue plus cet effet grandit et plus l'écart entre les photons de tête et de queue s'agrandit, on a donc un étalement puis un chevauchement des flux. Pour éviter les chevauchement on est donc obligé d'espacer les émissions en fonction des distances et capacités de réceptions. On a donc un débit intéressant mais non optimal, qui n'est utilisé que pour de courtes distances.

Monomode Ici on utilise un verre plus étroit$(2, 4\mu)$ avec un seul mode de propagation, les photons vont donc en ligne droite, sans étalement. C'est efficace pour les grandes distances, mais plus chèr.

(c) Le « dial-up » modem est un type de connexion au réseau. Il utilise l'infrastructure téléphonique (câble de cuivre). Au dessus de 56kbps on accède directement au routeur. On peut ainsi téléphoner et surfer en même temps, le câble n'est jamais réservé seulement pour l'un. Ce système était optimisé pour la voix humaine, il a une limite de 4khertz pour les fréquences.

2.1.2

(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) GBN (Go-back N) souffre encore, malgré ses améliorations, de quelques problèmes de performances. En effet, la moindre erreur dans un paquet peut entraîner la retransmission superflue d'une grande quantité de paquets pourtant déjà arrivés intègres. Le protocole à fenêtre glissante SR (Selective Repeat) évite les retransmissions inutiles et demandent à l'expéditeur de ne retransmettre que les paquets susceptibles d'avoir été perdus ou corrompus lors de la transmission. Cela implique que le destinataire envoie un ACK pour chaque paquet correctement reçu. Comme dans GBN (Go-back N), une fenêtre permet de limiter le nombre de paquets en attente de confirmation. En revanche, certains paquets de cette fenêtre auront déjà fait l'objet d'un accusé de réception. Le destinataire renvoie un accusé pour chaque paquet valide qu'il reçoit, qu'il soit dans l'ordre ou non, et stocke dans un tampon ceux qui sont encore temporairement hors

séquence (notons que ce tampon ne dépassera jamais la taille de la fenêtre d'envoi de l'expéditeur). Afin d'éviter les problèmes de confusions avec les numéros de séquence, la quantité de numéros disponible doit être au moins deux fois plus grande que la taille de la fenêtre.

(b) ?

2.1.3

(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) Window size(N) $\leq$ *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 paquets à partir de celui sans ACK.

2.1.4

(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) ?

2.1.5 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.

?

2.1.6 Le protocole de routage inter-domaine BGP est plus apparenté à la famille des protocoles de routage intra-domaine 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) ?

2.1.7 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 inter-domaine BGP est plus apparenté à la famille des protocoles de routage intra-domaine 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.

2.1.9

(a) Nommez et expliquez succinctement les 2 grandes familles de protocoles de routage intra-domaine (IGP) en insistant sur leurs différences.

(b) Expliquez en quoi et pourquoi le protocole de routage inter-domaine de l'Internet (BGP) est différent des protocoles de routage intra-domaine (IGP) déployés dans les divers systèmes autonomes (AS) qui composent l'Internet.

(a) ?

(b) ?

2.1.10

(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) ?

2.1.11

(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) ?

2.1.12 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) ?

2.1.13

(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) ?

2.1.14

(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) Quatre éléments principaux peuvent être identifiés dans l'architecture d'un routeur :

Port d'entrée Prend en charge les fonctionnalités de la couche physique et de la couche liaison. Il assure une fonction de consultation et d'acheminement des paquets entrant dans la matrice de commutation vers le port de sortie approprié.

Matrice de commutation Relie les ports d'entrée et les ports de sortie.

Port de sortie Emmagasine les paquets qu'il reçoit de la part de la matrice de commutation. Assure les fonctionnalités inverses de la couche liaison et de la couche physique.

Processeur de routage Chargé de l'exécution des protocoles de routage, de la mise à jour des informations et des tables.

(b) Le point le plus problématique est le fait que les routeurs doivent opérer à des vitesses élevées, impliquant des millions de consultations par seconde ; on souhaite en effet que l'opération de consultation soit plus rapide que le temps qu'il faut au routeur pour recevoir un nouveau paquet. Dès que le port de sortie a été identifié, le paquet peut entrer dans la matrice de commutation. Cependant un paquet peut se voir refuser temporairement l'accès si elle est occupée à traiter des paquets qui ont été reçus sur d'autres liaisons d'entrée. Il est alors placé en file d'attente sur son port. Si la matrice de commutation n'est pas assez rapide, et du coup à mesure de l'augmentation de ces files, le risque de perte de paquets augmente.

(c) Si aucun ou peu de phénomène de mise en attente ne se produit à l'entrée, mais que tous les paquets venaient à être dirigés vers le même port de sortie, il serait très rapidement saturé. Un gestionnaire de paquets doit déterminer quel paquet de la file doit être transmis. Cette règle est généralement la règle FIFO (First In First Out).

(d) HOL : Head of the line blocking Le routeur n'a pas de vue globale des buffer input, il ne prend donc en compte que le premier paquet du buffer. Si deux paquets doivent doivent aller au même port de sortie, un des paquets se retrouve en attente avec tous ceux qui le suivent, même si ceux ci doivent aller à un port actuellement libre.

2.1.15

(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 **C**arrier **Sense** **M**ultiple **A**ccess 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 **C**ollision **D**etection : 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) ?

2.1.16 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 inter-connectés.

?

2.1.17 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) ?

2.1.18

(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 longueur 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.

2.1.19

(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) Les enregistrements sur DNS sont sous le format : (name, value, type, tt1). On a plusieurs types possibles, entre autre :
- 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 connait 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 : nom du serveur mail associé à *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 authoritaire (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 authorité sur le domaine `www.company.com` (*par exemple ns110.ovh.net*).
- Le serveur local contacte alors le serveur authoritaire, 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`.

2.1.20

(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'etape 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 envoi à B et B répond à A. Mais B ne sait pas si son message est reçu par A.

2.1.21

(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 perdus, 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 démarage 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 inversément proportionelle à son RTT, évitant la retransmission en bloc de paquets inutiles sur des connexions trop lentes.

2.1.22

(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) — Commutation par action sur la mémoire : 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 : Traite un seul paquet à la fois, lent.

1. Maximum Segment Size

— Commutation par bus : Le port d'entrée transfert 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 : C'est le délit du bus qui détermine la vitesse de commutation du routeur.
Inconvénients : C'est qu'un seul paquet est transféré à la fois, du coup il y a un risque d'attente.

— Commutation par réseau d'interconnexions : 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'entrés 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 : Améliore la limite de débit associé à un bus commun.
Inconvénients :

(b) ???

(c) ???

2.1.23

(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 donnéee, 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.

2.1.24

(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) ?

2.1.25

(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.

2.1.26 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) ?

2.1.27

(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.

2.1.28 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 converytir 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 ?

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

?

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

?

2.1.31

(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) ?

2.1.32 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) ?

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

?

2.1.34

(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) ?

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

?

2.1.36

(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) ?

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

?

2.1.38

(a) Décrivez sommairement le fonctionnement du système DNS.

(b) Comparez les deux modes de fonctionnement du protocole (avantages et inconvénients).

(a) ?

(b) ?

2.1.39

(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) ?

2.1.40

(a) 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.

(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) ?

2.1.41

(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) ?

2.1.42

(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) ?

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

?

2.1.44

(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) ?

2.1.45 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.

?

2.1.46

(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) ?

2.1.47

(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) ?

2.1.48

(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) ?

2.1.49

(a) 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.

(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) ?

2.1.50

(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) 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