REPUBLIQUE DU CAMEROUN
****
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
****
INSTITUT SUPERIEUR DE MANAGEMENT ET DE L'ENTREPRENEURIAT
****

REPUBLIC OF CAMEROON
****
MINISTRY OF HIGHER EDUCATION
****
HIGHER INSTITUTE OF MANAGEMENT AND ENTREPRENEURSHIP
****

EXPOSE DE RESEAUX ET SERVICES TCP/IP

LES PROTOCOLES RESEAUX ET SERVICES TCP/IP

Rédigé et présenté par :

TSANE ZEUKENG PEGUY FRANCK

MEDOM FOUDJIN MICHELE

ALI

Sous l'encadrement de :

Ing patrice KAINNAING

Année académique
2020-2021

PLAN DETAILLE DU TRAVAIL

INTRODUCTION

Afin d'échanger des données de manière structurée au sein d'un réseau, il faut avoir recours à des règles qui commandent le déroulement des communications : les protocoles. Un protocole réseau est un ensemble de règles et de procédures de communication utilisées de part et d'autre par toutes les stations qui échangent des données sur le réseau. Il existe de nombreux protocoles réseaux (NETWORK PROTOCOLS) utilisés dans de nombreux modèles(familles) différents. Ces protocoles n'ont pas tous ni le même rôle ni la même façon de procéder. Certains protocoles réseaux fonctionnent au niveau de plusieurs couches du modèle utilisé, d'autres peuvent être spécialisés dans la réalisation d'une tâche correspondant à une seule couche du modèle. Un paquet transmis sur le réseau est constitué de plusieurs couches d'informations correspondant aux différents traitements de chacun des protocoles de la pile. Notre travail consistera à présenter les protocoles réseaux dans cet expose.

I- LES FAMILLES DE PROTOCOLES

Une famille de protocole est un modèle en couche. On dénombre plusieurs familles parmi lesquelles :

1- La famille DECnet

DECnet est une famille de protocoles réseau développée par DEC (Digital Équipement Corporation) en 1975. Elle a été développée à la base pour connecter deux micro-ordinateurs PDP-11 mais elle a évolué pour devenir l'une des premières architectures réseau Peer-to-Peer transformant ainsi DEC en une centrale de réseautage.

Initialement conçu avec trois couches il a évolué plus tard en un protocole réseau a 7 couches compatibles OSI. DECnet a été intégré au
Système d'exploitation phare de DEC VMS depuis sa création. Plus tard Digital l'a porté sur Ultrix ainsi que sur Apple Macintosh et IBM PC exécutant des variantes DOS et Microsoft Windows sous le nom de DEC Pathworks, permettant à ces systèmes de se connecter aux réseaux DECnet de machines VAX en tant que nœuds terminaux.

2- famille Appletalk

Au départ nommé AppleBus, Appletalk est une suite exclusive de protocoles réseau sortie en 1985 et développée par Apple Inc pour leurs ordinateurs Macintosh. Néanmoins certaines versions ont quand même été développées pour les pc IBM et compatibles et l'Apple IIGS. La prise en charge d'Apple Talk était également disponible dans la plupart des imprimantes en réseau, certains serveurs de fichiers et un certain nombre de routeurs. AppleTalk comprend un certain nombre de fonctionnalités qui permettent aux réseaux locaux d'être connectés sans configuration préalable ou sans avoir besoin d'un routeur ou d'un serveur centralisé de quelque sorte que ce soit. Les systèmes connectés équipés d'Apple Talk attribuent automatiquement des adresses, mettent à jour l'espace de noms distribué et configurent tout routage interréseau requis.

3- La famille SNA d'IBM

La famille SNA a été développée par IBM antérieurement au modèle OSI.
C'est l'évolution d'une architecture hiérarchique contrôlée par un seul hôte à une structure non hiérarchique permettant la communication d'égal à égal entre tous les nœuds du réseau. SNA est un modèle en couches qui suppose l'utilisation d'une interface d'accès au réseau de type VTAM (Virtual Telecom Access Method), c'est-à-dire un logiciel qui s'occupe de la gestion des ressources du réseau SNA en liaison avec un autre logiciel implanté dans le contrôleur de communication.la famille SNA est désormais largement remplacée par le modèle OSI.

4- La famille OSI (Open Systems InterConnect)

Le modèle OSI est né en 1984 après la naissance d'internet, car sa naissance découle de notre expérience acquise sur la communication entre les ordinateurs. Il tient donc compte des communications existantes mais aussi des communications futures et de leurs évolutions potentielles.

L'objectif du modèle OSI est de normaliser les communications pour garantir un maximum d'évolutivité et d'interopérabilité entre les ordinateurs. Ainsi le modèle OSI est une norme qui préconise comment les ordinateurs devraient communiquer entre eux.

5- Le modèle TCP/IP

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP
(Transmission Control Protocol) qu'on utilise « par-dessus » un protocole réseau IP (Internet Protocol).

Ce qu'on entend par modèle TCP/IP c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage TCP/IP peut donc designer deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

Le protocole TCP/IP s'est progressivement imposé comme modèle de référence en lieu et place du modèle OSI. Cela tient tout simplement à son histoire. En effet, contrairement au modèle OSI le modèle TCP/IP est né d'une implémentation, la normalisation est venue ensuite.

II- LES PROTOCOLES DU MODELE OSI

Chaque couche du modèle OSI comporte de nombreux protocoles :

1- Protocole de la couche 1-physique

- ISDN : Un **réseau numérique à intégration de services** (**RNIS**, en anglais *ISDN* pour *Integrated Services Digital Network*) est un réseau de télécommunications constitué de liaisons numériques permettant, par rapport au réseau téléphonique analogique, une meilleure qualité et des débits pouvant atteindre 2 Mbit/s (accès E1) contre 56 kbit/s pour un modem classique analogique.

- L'**étalement de spectre par saut de fréquence** parfois appelé « étalement de spectre par évasion de fréquence » (**FHSS** ou *frequency-hopping spread Spectrum* en anglais) est une méthode de transmission de signaux par ondes radio qui utilise alternativement plusieurs canaux (sous-porteuses) répartis dans une bande de fréquence selon une séquence pseudo-aléatoire connue de l'émetteur et du récepteur.

  Il a été inventé par Hedy Lamarr en 1941, en collaboration avec George Antheil. Hedy Lamarr proposa son système secret de communication[3,4,5,6] applicable

  aux torpilles radio-guidées, qui permettait au système émetteur-récepteur de la torpille de changer de fréquence, rendant pratiquement impossible la détection de l'attaque sous-marine

par l'ennemi. Il s'agit d'un principe de transmission (étalement de spectre par saut de fréquence) toujours utilisé pour le positionnement par satellites (GPS, GLONASS…), les liaisons chiffrées militaires, les communications des navettes spatiales avec le sol ou dans certaines techniques Wi-Fi.

L'étalement de spectre offre trois avantages par rapport à l'utilisation d'une fréquence unique :

- ❖ Il rend le signal transmis plus résistant aux interférences,
- ❖ Le signal est plus difficile à intercepter,

Les signaux transmis de cette manière peuvent partager des bandes de fréquence avec d'autres types de transmission, ce qui permet d'utiliser plus efficacement la bande passante ; le partage des fréquences ajoute un minimum de bruit à l'un et à l'autre types de transmission.

- Le **Symmetric Digital Subscriber Line** (**SDSL**, en français *ligne d'abonné numérique à débit symétrique*) est une technique d'accès datant de la fin des années 1990 qui permet de transporter des données à haut débit (jusqu'à 2 Mbit/s avec une portée maximale de 2,4 km) via un réseau. SDSL est une des techniques de la famille DSL. Comme son nom l'indique la ligne SDSL a, contrairement aux lignes ADSL, des débits symétriques : son débit en réception (*débit descendant* ou *download*) est égal au débit en émission (*débit montant* ou *upload*).

Le SDSL utilise seulement une paire torsadée (deux conducteurs) alors que les précédents standards DSL en utilisaient deux voire trois. Le débit de la SDSL peut être accru en utilisant plusieurs paires torsadées.

Cette utilisation de plusieurs paires de fils de cuivre est peu fréquente en Europe ; 4 paires de cuivre sont nécessaires pour atteindre un débit de 8 Mb/s au maximum. L'opérateur va tout simplement regrouper plusieurs paires de cuivre, ce n'est donc pas de l'agrégation de liens.

L'offre d'accès SDSL était destinée aux établissements professionnels : elle permet l'échange de données à haut débit entre plusieurs sites distants d'une même entreprise.

Contrairement à l'ADSL, le SDSL utilise également la bande spectrale utilisée communément pour le transport de la voix (de 300 à 3 400 Hz). Il n'est alors plus possible d'utiliser le service téléphonique classique, la ligne est donc dédiée. De ce fait, il n'est pas nécessaire d'utiliser de filtre, tout comme en dégroupage total ou en ADSL nu.

2- Protocole de couche 2 – liaison de donnée

- FDDI : ***Fiber Distributed Data Interface*** (***FDDI***) est un type de réseau informatique *LAN* ou *MAN* permettant d'interconnecter plusieurs *LAN* à une vitesse de 100 Mbit/s sur de la fibre optique (ce qui lui permet d'atteindre une distance maximale de 200 km).*FDDI* a vu le jour en 1986 sous l'appellation X3T9.5 par l'ANSI et a été normalisé IS9314 par l'ISO.

La technologie *LAN FDDI* est une technologie d'accès au réseau sur des lignes de type fibre optique. Il s'agit en fait d'une paire d'anneaux (l'un est dit « primaire », l'autre, permettant de rattraper les erreurs du premier, est dit « secondaire »). *FDDI* est un protocole utilisant un

anneau à jeton à détection et correction d'erreurs (c'est là que l'anneau secondaire prend son importance).

Le jeton circule entre les machines à une vitesse très élevée. Si celui-ci n'arrive pas au bout d'un certain délai, la machine considère qu'il y a eu une erreur sur le réseau.

La topologie *FDDI* ressemble de près à celle de *token ring*, à la différence près qu'un ordinateur faisant partie d'un réseau *FDDI* peut aussi être relié à un concentrateur *MAU* (*Media Access Unit*) d'un second réseau. **Ses Particularités**

- Débit de 100 Mb/s, avec codage 4B/5B et *NRZI*. ○ Anneau de longueur pouvant atteindre 100 km.
- Technique d'accès au médium par droit à l'émission (Jeton) proche de la recommandation IEEE802.5.
- Distance : en multimode 62,5/125 µm ⇒ 2 km, et en monomode ⇒ 60 km.

- FDDI-2 : Conçu pour voix et données

  - **Bluetooth** est une norme de communication permettant l'échange bidirectionnel de données à courte distance en utilisant des ondes radio UHF sur la bande de fréquence de 2,4 GHz. Son but est de simplifier les connexions entre les appareils électroniques à proximité en supprimant des liaisons filaires. Elle peut remplacer par exemple les câbles entre ordinateurs, tablettes, haut-parleurs, téléphones mobiles entre eux ou avec des imprimantes, scanneurs, claviers, souris, manettes de jeu vidéo, téléphones portables, assistants personnels, systèmes avec mains libres pour microphones ou écouteurs, autoradios, appareils photo numériques, lecteurs de code-barres et bornes publicitaires interactives.

- HDCL : Le **HDLC** (sigle anglais pour ***H**igh-Level **D**ata **L**ink **C**ontrol*) est un protocole de niveau 2 (couche de liaison) du Modèle OSI, dérivé de SDLC (*Synchronous Data Link Control*). Son but est de définir un mécanisme pour délimiter des trames de différents types, en ajoutant un contrôle d'erreur. Il est défini par l'*Organisation internationale de normalisation* sous la spécification ISO 3309 (Cette norme a été révisée par: ISO/IEC 13239:2002). Les interfaces série des routeurs Cisco utilisent une version propriétaire de HDLC par défaut[1].

- ARCnet : **ARCnet** est un acronyme anglais (Attached Resource Computer Network). C'est un protocole de réseau local (LAN) similaire à Ethernet ou Token Ring.

  Il a été développé par Datapoint Corp. en 1976 pour mettre en cluster des terminaux (par exemple les Datapoint 2200). Ces machines, censées être au départ de simples terminaux de saisie programmables, se révélèrent vite capables de devenir de véritables micro-ordinateurs dès lors que leur langage DATABUS, un COBOL propriétaire, fut complété du langage BASIC et d'un système d'exploitation sur ses disquettes 8 pouces de 160 ko (un ou deux lecteurs ; des modèles à cassette existaient également).

  ARCnet fut inventé afin de permettre à ces machines de communiquer. Il fut annoncé dès 1975 (disponibilité début 1977), soit 6 ans avant la sortie aux États-Unis du premier IBM PC et 8 ans avant sa sortie en France.

Une première version d'Ethernet existait alors, mais ARCnet utilisait des adaptateurs moins onéreux.

On compta jusqu'à 11 millions de nœuds ARCnet dans le monde.

ARCnet fonctionne à 2,5 Mb/s, utilise du câble coaxial, et une topologie logique à base de bus ou d'étoile à jeton

- TOKEN BUS : Un réseau ***token bus*** ou anneau à jeton adressé (« *token* » en anglais signifie « jeton ») implémente un protocole de type token ring sur un anneau virtuel constitué de postes reliés par un câble coaxial.

Le token bus a été standardisé par l'IEEE qui le désigne sous le nom « 802.4 ». Il n'est plus en fonctionnement

3- Protocole de la couches 2 et 3—Réseau et liaison

- ATM : Le **mode de transfert asynchrone** (en anglais ***Asynchronous Transfer Mode*** ou ***ATM***) est un protocole réseau de « niveau réseau » au sens du « modèle OSI » à commutation de cellules, qui a pour objectif de multiplexer différents flots de données sur un même lien physique en utilisant une technique de TDM ou MRT (multiplexage à répartition dans le temps).

  ATM a été conçu pour fournir un standard réseau unifié qui pourrait supporter un trafic réseau synchrone (SDH), aussi bien qu'un trafic utilisant des paquets (IP, relais de trames…) tout en supportant plusieurs niveaux de qualité de service (QdS).

  ATM est un protocole asynchrone, s'appuyant fréquemment sur une couche de transport synchrone. C'est-à-dire que les cellules ATM sont envoyées de manière asynchrone, en fonction des données à transmettre, mais sont insérées dans le flux de données synchrones d'un protocole de niveau inférieur pour leur transport

- Le **relayage de trames** (ou **FR**, pour l'anglais ***Frame Relay***) est un protocole à commutation de paquets situé au niveau de la couche de liaison (niveau 2) du modèle OSI, utilisé pour les échanges intersites (WAN). Il a été inventé par Eric Scace, ingénieur chez Sprint International.

Sur le plan technique, il peut être vu :

  - comme un successeur de X.25 : il a en effet remplacé ce protocole pour le raccordement des sites des entreprises aux infrastructures des opérateurs qui offrent des services RPV.
  - comme une étape vers l'ATM : il a souvent été présenté ainsi par les opérateurs très « UIT », c'est-à-dire les opérateurs ayant « voulu » X.25 et l'ATM, comme France Télécom par exemple. Le Frame Relay est en effet issu d'une volonté américaine, de l'ANSI en particulier, X.25 n'ayant jamais été très populaire aux États-Unis

comme faisant partie du RNIS (ISDN) : c'est ainsi que l'UIT l'a considéré et a défini des normes qui n'ont jamais été implémentées.

- L'**Address Resolution Protocol** (ARP, protocole de résolution d'adresse) est un protocole utilisé pour traduire une adresse de protocole de couche réseau (typiquement une adresse IPv4) en une adresse de protocole de couche de liaison (typiquement une

adresse MAC). Il se situe à l'interface entre la couche réseau (couche 3 du modèle OSI) et la couche de liaison (couche 2 du modèle OSI).

Fonctionnement ○ Un ordinateur connecté à un réseau informatique souhaite émettre une trame ethernet à destination d'un autre ordinateur dont il connaît l'adresse IP et placé dans le même sous-réseau. Dans ce cas, cet ordinateur va placer son émission en attente et effectuer une requête ARP en *broadcast* de niveau 2.

Cette requête est de type « quelle est l'adresse MAC correspondant à l'adresse IP *adresseIP* ? Répondez à *monAdresseIP* ». ○ Puisqu'il s'agit d'un *broadcast*, tous les ordinateurs du segment vont recevoir la requête. En observant son contenu, ils pourront déterminer quelle est l'adresse IP sur laquelle porte la recherche. La machine qui possède cette adresse IP sera la seule à répondre en envoyant à la machine émettrice une réponse ARP du type « je suis *adresseIP*, mon adresse MAC est *adresseMAC* ». Pour émettre cette réponse au bon ordinateur, il crée une entrée dans son cache ARP à partir des données contenues dans la requête ARP qu'il vient de recevoir. ○ La machine à l'origine de la requête ARP reçoit la réponse, met à jour son cache ARP et peut donc envoyer à l'ordinateur concerné le message qu'elle avait mis en attente.

Il suffit donc d'un *broadcast* et d'un *unicast* pour créer une entrée dans le cache ARP de deux ordinateurs.

4- Protocole de la couches 4--Transport

- **Transmission Control Protocol** (littéralement, « protocole de contrôle de transmissions »), abrégé **TCP**, est un protocole de transport fiable, en mode connecté, documenté dans la RFC 793[1] de l'IETF.

  Dans le modèle Internet, aussi appelé modèle TCP/IP, TCP est situé au-dessus de IP. Dans le modèle OSI, il correspond à la couche transport, intermédiaire de la couche réseau et de la couche session. Les applications transmettent des flux de données sur une connexion réseau. TCP découpe le flux d'octets en *segments* dont la taille dépend de la MTU du réseau sous-jacent (couche liaison de données).

  TCP, comme UDP, utilise le numéro de port pour identifier les applications. À chaque extrémité (client/serveur) de la connexion TCP est associé un numéro de port sur 16 bits (de 1 à 65535) assigné à l'application émettrice ou réceptrice. Ces ports sont classés en trois catégories :

○ Les *ports bien connus* sont assignés par l'IANA (Internet Assigned Numbers Authority) dans la plage 0-1023, et sont souvent utilisés par des processus système ou ayant des droits privilégiés. Les applications bien connues qui fonctionnent en tant que serveur et sont en attente de connexions utilisent généralement ces types de ports.
Exemples : FTP (21), SSH (22), Telnet (23), SMTP (25), HTTP (80), POP3 (1 10).

○ Les *ports enregistrés* sont généralement utilisés par des applications utilisateur comme ports sources éphémères pour se connecter à un serveur, mais ils peuvent aussi identifier des services non enregistrés par l'IANA.

- Les *ports dynamiques/privés* peuvent aussi être utilisés par des applications utilisateur, mais plus rarement. Ils n'ont pas de sens en dehors d'une connexion TCP particulière.

- Le ***User Datagram Protocol*** (**UDP**, en français **protocole de datagramme utilisateur**) est un des principaux protocoles de télécommunication utilisés par Internet. Il fait partie de la couche transport du modèle OSI, quatrième couche de ce modèle, comme TCP. Il a été défini par David P. Reed **(en)** et est détaillé dans la RFC 768.

Le rôle de ce protocole est de permettre la transmission de données (sous forme de datagrammes) de manière très simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port. Aucune communication préalable n'est requise pour établir la connexion, au contraire de TCP (qui utilise le procédé de handshaking). UDP utilise un mode de transmission sans connexion.

L'intégrité des données est assurée par une somme de contrôle sur l'en-tête. L'utilisation de cette somme est cependant facultative en IPv4 mais obligatoire avec IPv6. Si un hôte n'a pas calculé la somme de contrôle d'un datagramme émis, la valeur de celle-ci est fixée à zéro. La somme de contrôle inclut également les adresses IP de la source et de la destination.

À cause de l'absence du mécanisme d'établissement de liaison (handshaking), ce protocole expose le programme qui l'utilise aux problèmes éventuels de fiabilité du réseau ; ainsi, il n'existe pas de garantie de protection quant à la livraison, l'ordre d'arrivée, ou la duplication éventuelle des datagrammes. Si des fonctionnalités de correction d'erreur sont requises, alors une application peut se tourner vers les protocoles TCP ou SCTP qui sont conçus à cet effet. UDP est donc adapté à un usage pour lequel la détection et la correction d'erreurs ne sont pas nécessaires, ou sont effectuées directement par l'application.

La nature du protocole UDP le rend utile pour transmettre rapidement de petites quantités de données, depuis un serveur vers de nombreux clients ou bien dans des cas où la perte éventuelle d'un datagramme est préférée à l'attente de sa retransmission. Le DNS, la voix sur IP ou les jeux en ligne sont des utilisations typiques de ce protocole.

Utilisation

Il est utilisé quand il est nécessaire soit de transmettre des données très rapidement, et où la perte d'une partie de ces données n'a pas grande importance, soit de transmettre des petites quantités de données, là où la connexion « *3-WAY* » TCP serait inutilement coûteuse en ressources. Par exemple, dans le cas de la transmission de la voix sur IP, la perte occasionnelle d'un paquet est tolérable dans la mesure où il existe des mécanismes de substitution des données manquantes, par contre la rapidité de transmission est un critère primordial pour la qualité d'écoute.

Il est également utilisé pour émettre des données à plusieurs récepteurs simultanément (multicast, broadcast), la connexion TCP n'étant que point-àpoint.

Exemples d'utilisation :

- les protocoles DHCP/BOOTP, DNS, SNMP, TFTP, xPL
- le *streaming* ;

- les jeux en réseau (exemple : jeux de tir à la première personne) ;
- Le **Datagram Congestion Control Protocol** (DCCP) est un protocole de communication de couche de transport orienté message. Il a été développé à l'IETF et est normalisé dans le RFC 4340.

DCCP implémente la mise en place d'une connexion fiable, le démontage, la notification explicite de congestion (ECN), le contrôle de la congestion et la négociation des fonctionnalités.

- **Real-Time Transport Protocol** (RTP) est un protocole de communication informatique permettant le transport de données[1] soumises à des contraintes de temps réel, tels que des flux média audio ou vidéo[2].

Utilisation

RTP est à l'heure actuelle principalement utilisé comme transport de média pour les services de la voix sur IP ou de vidéo conférence, voire de *streaming*. En mode unidirectionnel, il est toujours associé avec un autre protocole de signalisation qui gère l'établissement de session et permet l'échange du numéro de port utilisé par les deux extrémités. On peut citer :

- le protocole SIP pour les services de VoIP et de visioconférences ;
- le protocole H.323 pour les mêmes services (ancienne génération) ;
- le protocole RTSP pour le *streaming* bien que ce dernier possède un mode d'encapsulation TCP.

Le protocole ajoute un en-tête spécifique aux paquets UDP pour

- spécifier le type et le format (codec) du média transporté ;
- numéroter les paquets afin de pouvoir gérer les pertes et les déséquencements ;
- fournir une indication d'horloge pour gérer la gigue.

RTP sera utilisé avantageusement sur un réseau temps réel (par exemple un réseau ATM à bande passante garantie, un canal optique, une radiodiffusion ou un canal satellite).

RTP est **unidirectionnel** mais peut être utilisé en mode diffusion (*multicast*) *via* satellite. Il est alors extrêmement économique en termes de ressources réseau pour servir un grand nombre de récepteurs, ce qui permet d'augmenter considérablement le débit utile et la qualité de codage du contenu.

5- Protocole de la couches 5 –Session

- En informatique, le protocole **Datagram Transport Layer Security** (**DTLS**, en français **sécurité de la couche transport en datagrammes**) fournit une sécurisation des échanges basés sur des protocoles en mode datagramme. Le protocole DTLS est basé sur le protocole TLS et fournit des garanties de sécurité similaires.

- **NetBIOS** (NETwork Basic Input Output System) est une architecture réseau codéveloppée par IBM et Sytek (en) au début des années 1980. NetBIOS est utilisé principalement par Microsoft. Ce n'est pas un protocole réseau, mais un système de

nommage et une interface logicielle qui permet d'établir des sessions entre différents ordinateurs d'un réseau.

- **SOCKS** est un protocole réseau qui permet à des applications clientserveur d'employer d'une manière transparente les services d'un pare-feu. SOCKS est l'abréviation du terme anglophone « *sockets* » et « *Secured Over Credential-based Kerberos* ».

Les applications du réseau protégées derrière le pare-feu qui souhaitent accéder à des serveurs extérieurs doivent se connecter via un serveur proxy de type SOCKS. Un tel serveur décide de l'éligibilité du client à accéder au serveur externe et transmet sa requête au serveur. SOCKS peut également être employé de manière inverse, permettant aux applications à l'extérieur de se connecter aux serveurs derrière le pare-feu.

Le protocole a été à l'origine développé par David Koblas, un des administrateurs système de la société MIPS. L'année du rachat de MIPS par Silicon Graphics, en 1992, Koblas a présenté un papier sur SOCKS à un colloque sur la sécurité Usenix, et SOCKS est devenu de fait un protocole public. Le protocole a été amélioré dans sa version 4 par Ying-Da Lee de la société NEC.

La version 4a, « officieuse », ajoute le support des serveurs de résolution de noms à SOCKS.

L'actuelle version 5 du protocole, spécifiée dans la RFC 1928, étend la version précédente en ajoutant la possibilité de transmettre de l'UDP, permet l'authentification, la résolution des noms de domaines par le serveur SOCKS lui-même, et IPv6.

L'architecture et l'application cliente de référence sont la propriété de Permeo Technologies.

D'après le modèle OSI, le protocole SOCKS est une couche intermédiaire entre la couche applicative et la couche transport.

6- Protocole de la couches 6 –présentation

- L'***Extensible Markup Language***, généralement appelé **XML**, « langage de balisage extensible[1] » en français, est un métalangage informatique de balisage générique qui est un sous-ensemble du Standard Generalized Markup Language (SGML). Sa syntaxe est dite « extensible » car elle permet de définir différents langages avec pour chacun son vocabulaire et sa grammaire, comme XHTML, XSLT, RSS, SVG… Elle est reconnaissable par son usage des chevrons (<, >) encadrant les noms des balises. L'objectif initial de XML est de faciliter l'échange automatisé de contenus complexes (arbres, texte enrichi, etc.) entre systèmes d'informations hétérogènes (interopérabilité). Avec ses outils et langages associés, une application XML respecte généralement certains principes :
    - la structure d'un document XML est définie et validable par un schéma ;
    - un document XML est entièrement transformable dans un autre document XML.
        - ***HyperText Markup Language***, généralement abrégé **HTML** ou dans sa dernière version **HTML5**, est le langage de balisage conçu pour représenter les pages web.

Ce langage permet :

- d'écrire de l'hypertexte, d'où son nom, ○ de structurer sémantiquement la page, ○ de mettre en forme le contenu, ○ de créer des formulaires de saisie,
- d'inclure des ressources multimédias dont des images, des vidéos, et des programmes informatiques,
- de créer des documents interopérables avec des équipements très variés de manière conforme aux exigences de l'accessibilité du web. Il est souvent utilisé conjointement avec le langage de programmation JavaScript et des feuilles de style en cascade (CSS). HTML est inspiré du *Standard Generalized Markup Language* (SGML). Il s'agit d'un format ouvert.

- ***Multipurpose Internet Mail Extensions*** (*MIME*) ou **Extensions multifonctions du courrier Internet**[1] est un standard internet qui étend le format de données des courriels pour supporter des textes en différents codage des caractères autres que l'ASCII, des contenus non textuels, des contenus multiples, et des informations d'en-tête en d'autres codages que l'ASCII. Les courriels étant généralement envoyés via le protocole SMTP au format MIME, ces courriels sont souvent appelés courriels *SMTP/MIME*.

  À l'origine, SMTP avait été prévu pour ne transférer que des fichiers textes (codés en ASCII). Avec l'apparition du multimédia et l'utilisation croissante des applications bureautiques, le besoin s'est fait sentir d'échanger, en plus des fichiers textes, des fichiers binaires (format des applications bureautiques, images, sons, fichiers compressés).

  Les types de contenus définis par le standard MIME peuvent être utilisés à d'autres fins que l'envoi de courriels, dans les protocoles de communication comme le HTTP pour le World Wide Web.

- L'***American Standard Code for Information Interchange*** (Code américain normalisé pour l'échange d'information), plus connu sous l'acronyme **ASCII** ([aski:]), est une norme informatique de codage de caractères apparue dans les années 1960. C'est la norme de codage de caractères la plus influente à ce jour. ASCII définit 128 codes à 7 bits, comprenant 95 caractères imprimables : les chiffres arabes de 0 à 9, les lettres minuscules et capitales de A à Z, et des symboles mathématiques et de ponctuation. ASCII suffit pour représenter les textes en anglais, mais il est trop limité pour les autres langues, dont le français et ses lettres accentuées. Les limitations du jeu de caractères ASCII sont encore sensibles au XXI^{e} siècle, par exemple dans le choix restreint de caractères généralement offerts pour composer une adresse email.

- **Unix to Unix Copy** (UUCP) est un ensemble de programmes qui permettent à deux machines d'échanger des fichiers et d'exécuter des commandes sur la machine distante en passant par une ligne téléphonique (modem), mais aussi sur une couche TCP/IP (souvent à travers SSH), voire via un câble série direct (*null modem*). Le mode modem reste cependant

le cas de figure le plus utilisé. Son nom dérive de "cp", la commande permettant la copie de fichiers localement sur un système Unix.

7- Protocole de la couches 7 –Application

En informatique, le **POP** (***Post Office Protocol***, littéralement « protocole de bureau de poste »), est un protocole qui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique. En dehors d'un paramétrage spécifique, POP se connecte au serveur de messagerie, s'authentifie, récupère le courrier, « peut » effacer le courrier sur le serveur, et se déconnecte.

Il est important de savoir, que tout comme IMAP, l'autre protocole de relève de mails, POP permet tout à fait de lire ses mails depuis différents appareils, (PC, smartphones, webmail). Il suffit de parametrer les clients mails pour qu'ils ne suppriment pas les messages après chaque relève.

Ce protocole a été réalisé en plusieurs versions; respectivement **POP1**, **POP2** et actuellement **POP3**.

Cette opération transite sur un réseau TCP/IP et utilise le protocole de transfert TCP via le port 110. Ce protocole est défini par la RFC 1939.

POP3S (POP3 over SSL) – ou **POPS** –) permet de chiffrer la communication avec le serveur au moyen de TLS. Ce protocole est défini par la RFC 2595. Selon cette dernière, l'usage d'un port spécifique pour ces communications chiffrées (initialement TCP 995 avec le chiffrement SSL) est maintenant déconseillé.

L'opération inverse, c'est-à-dire la remise de courrier à un serveur afin qu'il soit distribué, s'effectue généralement avec un autre protocole : SMTP.

- **TFTP** (pour ***Trivial File Transfer Protocol*** ou **protocole simplifié de transfert de fichiers**) est un protocole simplifié de transfert de fichiers.

  Il fonctionne en UDP sur le port 69, au contraire du FTP qui utilise lui TCP. L'utilisation d'UDP, protocole « non fiable », implique que le client et le serveur doivent gérer eux-mêmes une éventuelle perte de paquets. En termes de rapidité, l'absence de fenêtrage nuit à l'efficacité du protocole sur les liens à forte latence. On réserve généralement l'usage du TFTP à un réseau local.

  Les principales simplifications visibles du TFTP par rapport au FTP sont qu'il ne gère pas le listage de fichiers, et ne dispose pas de mécanismes d'authentification, ni de chiffrement. Il faut connaître à l'avance le nom du fichier que l'on veut récupérer. De même, aucune notion de droits de lecture/écriture n'est disponible en standard.

  À cause de ces fonctionnalités absentes, FTP lui est généralement préféré. TFTP reste très utilisé pour la mise à jour des logiciels embarqués sur les équipements réseaux (routeurs, pare-feu, etc.) ou pour démarrer un PC à partir d'une carte réseau.

  La dernière version de ce protocole est la version 2, définie dans RFC 1350[2]. Elle est la plus utilisée.

Une extension de ce protocole, définie dans RFC 2347[3], permet de négocier des options pour le modifier : une option est toujours demandée par le client, le serveur peut l'accepter, la modifier, ou la refuser, notamment s'il ne la connaît pas.

 Extensible Messaging and Presence Protocol (qu'on peut traduire par « protocole extensible de présence et de messagerie »), souvent abrégé en **XMPP**, est un ensemble de protocoles standards ouverts de l'*Internet Engineering Task Force* (IETF) pour la messagerie instantanée, et plus généralement une architecture décentralisée

d'échange de données. XMPP est également un système de collaboration en quasitemps-réel et d'échange multimédia par son extension Jingle, dont la voix sur réseau IP (téléphonie sur Internet), la visioconférence et l'échange de fichiers sont des exemples d'applications.

XMPP est constitué d'un protocole TCP/IP basé sur une architecture clientserveur permettant les échanges décentralisés de messages instantanés ou non, entre clients, au format Extensible Markup Language (XML). XMPP est en développement constant et ouvert au sein de l'IETF.

Les serveurs peuvent être privés (en intranet) ou bien publics, c'est-à-dire reliés aux autres serveurs publics via l'Internet (comme chez Facebook). L'ensemble des serveurs publics créent, ce que l'on appelle, le réseau Jabber (ou le réseau XMPP).

XMPP est ainsi utilisé à travers le monde par des centaines de serveurs publics et privés, et des millions d'utilisateurs. De nombreux acteurs industriels utilisent XMPP,
comme Apple, Cisco, Gizmo5, GNOME, Google[1], IBM, Oracle Corporation,

Le protocole XMPP est séparé en deux parties différentes :

- Le protocole de base contient les concepts fondamentaux pour faire fonctionner une infrastructure Jabber. Il est défini par les RFC 6120[2], 6121[3], 6122[4] (qui remplacent depuis 2011 les 3920[5] et 3921[6]), 3922[7] et 3923[8]. Théoriquement, une telle infrastructure ne peut pas fonctionner sans appliquer complètement ces protocoles.
- Les *XMPP Extension Protocols* (XEP) sont des propositions d'ajout de fonctionnalités au protocole Jabber. Les serveurs ou clients ne sont pas obligés d'adopter ces extensions. Cela peut bloquer certaines fonctionnalités entre deux utilisateurs.

XMPP est conçu de manière plus large et ouverte que la simple messagerie instantanée populaire et propriétaire. Il est ainsi utilisé par les entreprises et administrations dans le cadre d'échanges de données entre applications (ETL, EAI, ESB) au sein des systèmes d'informations, mais aussi dans le cadre du *grid computing*, des notifications d'alertes ou d'informations, de la supervision système et réseau, ou le *cloud computing*. Enfin, XMPP est également utilisé dans le domaine du partage et de la collaboration en quasitemps-réel comme le tableau blanc (« *whiteboard* ») ou l'édition et le

développement collaboratifs, mais aussi des jeux sur Internet (notamment les jeux de cartes et de plateau).

 Border Gateway Protocol (**BGP**) est un protocole d'échange de route externe (un EGP), utilisé notamment sur le réseau Internet. Son objectif principal est d'échanger des informations de routage et d'accessibilité de réseaux (appelés *préfixes*) entre *Autonomous Systems* (AS). Comme il circule sur TCP, il est considéré comme appartenant à la couche application du modèle OSI[1].

Contrairement aux protocoles de routage interne, BGP n'utilise pas de métrique classique mais fonde les décisions de routage sur les chemins parcourus, les attributs des préfixes et un ensemble de règles de sélection définies par l'administrateur de l'AS. On le qualifie de protocole à vecteur de chemins (*path vector protocol*).

BGP prend en charge le routage sans classe et utilise l'agrégation de routes afin de limiter la taille de la table de routage. Depuis 1994, la version 4 du protocole est utilisée sur Internet, les précédentes étant considérées comme obsolètes. Ses spécifications sont décrites dans la RFC 4271[2] *A Border Gateway Protocol 4 (BGP-4)*.

BGP a remplacé Exterior Gateway Protocol (EGP) qui était utilisé dans la dorsale ARPANET et a permis la décentralisation du routage sur Internet. Il a pour intérêt son passage à l'échelle (*scalabilité*)[3]: il peut traiter un très grand nombre de routes entre de nombreux *Autonomous Systems* en évitant les boucles, et masque la topologie interne des AS entre eux.

Certaines extensions de BGP permettent l'échange de routes IPv6 (RFC 2545), les premières versions se limitant à IPv4, et l'extension multi-protocole (MP-BGP, RFC 2858[5]) permet d'utiliser BGP pour convoyer des informations de routage pour de nombreux autres protocoles, notamment les routes liées à des VPN MPLS (IPv4[6], IPv6[7], VPLS...).

 Telnet (***te**rmina**l** **net**work* ou ***tel**ecommunication **net**work*, ou encore ***tel**etype **net**work*) est un protocole utilisé sur tout réseau TCP/IP, permettant de communiquer avec un serveur distant en échangeant des lignes de texte et en recevant des réponses également sous forme de texte.

Il était notamment utilisé pour administrer des serveurs UNIX distant ou de l'équipement réseau, avant de tomber en désuétude par défaut de sécurisation (le texte étant échangé en clair) et l'adoption de SSH.

Détail du protocole :

Telnet est un protocole de type client-serveur s'appuyant sur TCP. Les clients se connectent généralement sur le port 23 du serveur.

Parmi les caractères envoyés par le serveur Telnet, il y a évidemment les caractères de texte à afficher, mais il y a aussi des séquences de caractères qui permettent de contrôler l'affichage, par exemple pour effacer le contenu de la ligne courante. Par souci de

portabilité, Telnet définit des séquences d'échappement qui ne dépendent pas du type de terminal. Le protocole de présentation correspondant est appelé NVT (Network Virtual Terminal). Le client Telnet est censé interpréter ces séquences portables de contrôle du terminal.

NVT s'appuie sur :

- des caractères de contrôle empruntés au code ASCII, comme le caractère Form Feed de code hexadécimal 0C pour effacer l'écran ; ○ des séquences de plusieurs caractères introduites par le code hexadécimal FF appelé IAC (*interpret as command*), comme la séquence hexadécimale FF F8 pour effacer une ligne.

NVT va au-delà des fonctionnalités d'affichage et permet par exemple d'envoyer de façon urgente des signaux d'interruption au serveur pour interrompre l'application en cours. Il permet aussi de négocier des options entre le client Telnet et le serveur Telnet : on peut ainsi négocier le type de terminal, ce qui permet d'utiliser des séquences de contrôle de l'affichage comme celles du terminal VT100 qui soient moins rudimentaires que celles que NVT propose.

NVT est conçu pour des caractères de texte sur 7 bits et n'est par défaut pas adapté à une transmission sur 8 bits. Ce protocole est repris sous une forme simplifiée pour la connexion de contrôle du protocole de transfert de fichier FTP.

- **Local Mail Transfer Protocol** (**LMTP**, protocole local de transfert de courrier) est une variante de ESMTP **(en)**, l'extension de *Simple Mail Transfer Protocol* (*SMTP*). LMTP est défini dans la RFC 2033[1].

  LMTP a été conçu comme une alternative aux échanges SMTP normaux dans les situations où la partie réceptrice ne possède pas de file d'attente des messages reçus (les files d'attente sont une exigence inhérente à SMTP). C'est le cas par exemple d'un agent de transfert du courrier agissant en tant qu'agent de distribution du courrier. En effet, LMTP va rejeter un message s'il ne peut pas être immédiatement distribué à son destinataire, ce qui supprime le besoin d'une file d'attente des messages.

  LMTP est un protocole applicatif du modèle OSI. Comme SMTP, il utilise un transport TCP, mais ne doit pas utiliser le numéro de port 25, le port bien connu de SMTP.

III- LES PROTOCOLES DU TCP/IP

Le protocole TCP/IP (Transmission Control Protocol / Internet Protocol) est le plus connu des protocoles parce que c'est celui qui est employé sur le réseau des réseaux, c'est à dire Internet. Historiquement, TCP/IP présentait deux inconvénients majeurs, sa taille et sa lenteur.

1- Les protocoles de la pile TCP/IP

- ARP (Adress Resolution Control) fait correspondre des adresses logiques (IP) avec les adresses physiques (MAC). Chaque maintient à jour une table ARP associant une adresse logique a une adresse physique. Pour pallier les changements de matériels ou d'adressage logique, cette table est dynamique et ses entrées ont une durée de vie limitée.

- RIP (Routing Information Protocol) trouve la route la plus rapide entre deux ordinateurs. C'est un routage basé sur le nombre de routeur intermédiaire entre deux réseaux.

- SPF (Open Shortest Path First) est une amélioration de RIP, plus rapide et plus fiable. Routage basé sur l'état des liens.
- Le protocole IMAP Le protocole IMAP (Internet Message Access Protocol) est un protocole alternatif au protocole POP3 mais offrant beaucoup plus de possibilités : • IMAP permet de gérer plusieurs accès simultanés • IMAP permet de gérer plusieurs boîtes aux lettres • IMAP permet de trier le courrier selon plus de critères
- Le protocole POP3 Le protocole POP (Post Office Protocol que l'on peut traduire par "protocole de bureau de poste") permet comme son nom l'indique d'aller récupérer son courrier sur un serveur distant (le serveur POP). Il est nécessaire pour les personnes n'étant pas connectées en permanence à Internet afin de pouvoir consulter les mails reçus hors connexion.

- ICMP (Internet Control Message Protocol) c'est un protocole de la couche réseau offrant un ensemble d'outils et de signaux nécessaires au routage pour la gestion de l'acheminement des paquets. Bien qu'appartenant à la couche internet du modèle TCP/IP, ICMP est encapsulé dans IP, et permet ainsi non pas de fiabiliser une transmission mais de déterminer les causes éventuelles d'un problème en proposant un compte-rendu d'erreur.

- PPP (Point to Point Protocol) permet d'établir une connexion distante par téléphone. PPP (après SLIP) est utilisé par les fournisseurs d'accès à Internet.

- RARP (Reverse Adresse Résolution protocole) est un protocole de la couche liaison permettant de déterminer l'adresse logique d'un hôte à partir de son adresse physique. Il est donc exactement l'inverse du protocole ARP et utilise le même type de messages. Il nécessite la mise en place d'un serveur RARP, centralisant de manière statique les associations adresse logiciel/adresse physique.

- Le système DNS (Domain Name System) est un système d'annuaire associant un nom alphanumérique à une adresse IP. Le but de ce système est de designer un hôte avec une application beaucoup plus facilement mémorisable qu'une adresse

IP. Un nom DNS correspond donc généralement a une seule adresse IP, alors qu'une adresse IP peut cependant être associée à plusieurs noms de DNS.

• Le protocole HTTP (HyperText Transfer Protocol) est le protocole le plus utilisé sur Internet depuis 1990. Le but du protocole HTTP est de permettre un transfert de fichiers (Essentiellement au format HTML) localisés grâce à une chaîne de caractères appelée URL entre un navigateur (le client) et un serveur Web

• TCP (qui signifie *Transmission Control Protocol*, soit en français : *Protocole de Contrôle de Transmission*) est un des principaux protocoles de la couche transport du modèle TCP/IP. Il permet, au niveau des applications, de gérer les données en provenance (ou à destination) de la couche inférieure du modèle (c'est-à-dire le protocole IP). Lorsque les données sont fournies au protocole IP, celui-ci les encapsule dans des datagrammes IP, en fixant le champ protocole à 6 (Pour savoir que le protocole en amont est TCP...). TCP est un protocole orienté connexion, c'est-à-dire qu'il permet à deux machines qui communiquent de contrôler l'état de la transmission. Les caractéristiques principales du protocole TCP sont les suivantes :

- **TCP permet de remettre en ordre les datagrammes en provenance du protocole IP**
- **TCP permet de vérifier le flot de données afin d'éviter une saturation du réseau**
- **TCP permet de formater les données en segments de longueur variable afin de les "remettre" au protocole IP**
- **TCP permet de multiplexer les données, c'est-à-dire de faire circuler simultanément des informations provenant de sources (applications par exemple) distinctes sur une même ligne**
- **TCP permet enfin l'initialisation et la fin d'une communication de manière courtoise**

Le protocole TCP/IP est devenu la référence à partir de laquelle sont évalués les autres protocoles. La pile de protocole TCP/IP est la plus riche fonctionnellement.
Le protocole IP dispose de fonctions standardisées, les « API sockets » qui se comportent de la même façon sur tous les types de matériels.
Les caractéristiques du protocole TCP/IP

- **Une norme industrielle**
- **Tous les réseaux reconnaissent TCP/IP :**
- **Une interopérabilité entre ordinateurs hétérogènes**
- **Un standard pour la communication inter réseau et particulièrement entre des**
- **Réseaux hétérogènes**

- **Un protocole routable**

D'autres protocoles ont été développés spécialement pour TCP/IP :

- **SMTP pour la messagerie électronique**
- **FTP pour l'échange de fichiers**
- **SNMP pour la surveillance des réseaux**

2- Les protocoles IP routable

- IGP (Interior Gateway Protocol) : c'est un protocole de routage dynamique entre plusieurs routeurs de système autonome donc la gestion dépend d'une administration unique.
- EGP (Exterior Gateway Protocol) : protocole de routage dynamique entre routeur de différents systèmes autonomes.
- BGP (Border Gateway Protocol) : protocole utilise par internet pour afin de mettre à jour les informations de routage des quelques 200000 système autonomes déployées dans le monde.
- BGP/EGP (Border Gateway Protocol / Exterior Gateway Protocol) gère la transmission des données entre les réseaux.
- POP 3 & IMAP 4 POP 3 (Post Office Protocol version 3) et IMAP 4 (Internet Message Advertising Protocol version 4) permettent de se connecter à un serveur de messagerie et de récupérer son courrier électronique.

3- Le protocole UDP

Le protocole UDP (*User Datagram Protocol*) utilise le protocole Internet pour obtenir une unité de données, également appelée datagramme, d'un appareil à un autre sur un réseau. UDP est défini comme étant léger puisqu'il ne nécessite pas la lourde charge d'avoir des détails sur un en-tête. Les publicités de service, telles que les mises à jour du protocole de routage, la disponibilité du serveur et les applications de streaming telles que la vidéo et la voix sont quelques-unes des principales utilisations d'UDP.

4- Tableau des protocoles TCP/IP et leur couche

Protocole TCP/IP	**Couche réseau TCP/IP**
FTP, SMTP, HTTP, DNS	APPLICATION
TCP, UDP	TRANSPORT
ICMP, ARP, RARP, IP	RESEAU
PPP, ETHERNET, FDDI, TOKENGRING	HOTE RESEAU

CONCLUSION

Parvenus au terme de notre devoir ou il était question pour nous de présenter les différents protocoles utilises dans un réseau informatique, il en ressort qu'il existe plusieurs piles de protocoles utilisés dans différents modèles. Ces protocoles n'ayant pas le même rôle ou le même fonctionnement, il est important de noter que chacun d'eux intervient au niveau d'une ou de plusieurs couches du modèle utilise. Ces protocoles permettent une bonne transmission fiable et sécurisée des données au sein d'un réseau.