Support réseau des accès utilisateurs :

Présentation :

Ce module présente le maintien en condition opérationnelle de solutions techniques d’accès au réseau et au paramétrage de leur connexion. Comment mettre en place un réseau informatique.

Chapitre 1 : Les réseaux informatiques

I. Présentation des réseaux :

Il existe de nombreux types de réseaux, chacun offrant des types de services différents. Au cours d’une journée ordinaire, la même personne peut téléphoner, regarder la télévision ou encore faire des recherches sur Internet grâce aux réseaux.

Les réseaux permettent de mettre en relation des personnes et du matériel, quelle que soit leur zone géographique. Les gens utilisent ces réseaux sans se préoccuper de la manière dont ils fonctionnent ou de ce que serait leur vie sans eux.

Dans les années 90 la technologie des communications nécessitait des réseaux dédiés pour mettre en œuvre les communications voix, vidéo et numériques. La question qui se posait alors, était comment accéder à tous ces services en même temps.

Les nouvelles technologies ont apportés une réponse grâce au développement d’un nouveau type de réseau, capable de fournir plusieurs services à la fois. (VOIP = Voice over IP)

Ces nouveaux réseaux sont capables d’acheminer des services de techniques vocales, vidéo et de de données sur le même canal de communication ou la même structure réseau. Le terme « réseau » fait référence à ces nouveaux réseaux multiservices.

III. Avantages et inconvénients des réseaux :

Les avantages de la mise en réseau d’ordinateurs et d’autres périphériques incluent la réduction des coûts et une amélioration de la productivité. Dans un réseau, les ressources peuvent être partagées pour éviter d’endommager ou de dupliquer les données

Les avantages des réseaux informatiques sont :

* Le partage de l’information et l’accès aux informations distantes : Les réseaux offrent de nombreux outils de collaboration différents, employés pour la communication entre les utilisateurs du réseau.
* Le partage des ressources (réduction des équipements et des périphériques) pour éviter la duplication des données
* La capacité de stockage augmentée (serveur de stockage SAN)
* La connexion à distance (télétravail : économie de temps et de transports)
* La simplification de l’installation des programmes (serveur d’applications)
* Les ressources préservées : le traitement des données peut être réparti sur plusieurs ordinateurs, pour éviter qu’un ordinateur seul soit surchargé par les tâches de traitement (répartition de charges ou load balancing).
* Cout de licences réduit : De nombreux éditeurs de logiciels proposant des licences de site pour les réseaux. Une licence de site permet à un groupe de personnes ou à une entreprise entière d’utiliser l’application pour un prix forfaitaire unique.
* L’administration centralisée qui permet de réduire le personnel en charge de la gestion des périphériques et des données du réseau, ce qui diminue le temps de travail et les coûts d’exploitation pour l’entreprise.
* Chaque utilisateur du réseau n’a pas à gérer individuellement ses propres données et périphériques.

Les inconvénients des réseaux informatiques sont :

* La sécurité qui est déjouée par les pirates informatique à l’aide de différents outils.
* La propagation des virus qui constitue une grande menace et qui peut corrompre les informations du système d’information de l’entreprise.

IV. Les catégories de réseaux :

Les réseaux informatiques évoluent en permanence en matière de complexité, d’utilisation et de conception. Un réseau informatique est identifié par les caractéristiques suivantes :

* La zone qu’il dessert ;
* La façon dont les données dont stockées,
* La manière dont les ressources sont gérées,
* La manière dont le réseau est organisée,
* Le type de périphérique réseau utilisés,
* Le moyen utilisé pour connecter les périphériques.

La classification par étendue géographique est généralement utilisée, bien que non stricte. Un réseau est identifié par une appellation qui est généralement liée à sa zone de couverture. Il y a quatre grandes familles : les réseaux personnels (PAN, 1 m), les réseaux locaux (LAN, 100 m), les réseaux métropolitains (MAN, 10 km) et les réseaux étendus (WAN, 100 km).

**Les réseaux personnels :** Le réseau personnel (PAN) relie des périphériques tels que des souris, des claviers, des imprimantes, des smartphones et des tablettes sur une portée très limitée, pour une seule personne. Tous ces périphériques sont dédiés à un seul hôte et utilisent généralement une connexion Bluetooth.

Bluetooth est une technologie sans fil qui permet aux périphériques de communiquer sur des distances courtes. Cette spécification technique est décrite par la norme IEE 802.15.1. Les périphériques Bluetooth sont capables de gérer de la voix et des données. Les périphériques Bluetooth fonctionnent dans une gamme de fréquences radio allant de 2,4 à 2,485 GHz, soit la bande ISM (Industriel, Scientifique et Médical).

**Les réseaux locaux :** Un réseau individuel couvre généralement une seule zone géographique et fournit des services et des applications aux membres d’une même structure. C’est ce qu’on appelle un réseau local LAN. Un réseau local peut être constitué de plusieurs réseaux locaux. Les réseaux regroupés au sein d’un même réseau local dépendent d’un même groupe de contrôle d’administration. Cependant la définition de « réseau local » a évolué, et ce terme peut aujourd’hui faire référence à des réseaux locaux interconnectés et composés de plusieurs centaines de périphériques répartis sur plusieurs sites.

**Les réseaux locaux sans-fil (WLAN) :** Un réseau local sans fil (WLAN) est un réseau local utilisant des ondes radio pour transférer des données entre les périphériques. Dans un réseau local traditionnel, les périphériques sont interconnectés par le biais d’un câblage en cuivre. Dans certains environnements, l’installation de câbles en cuivre peut être difficile, indésirable, voire impossible. Des périphériques sans fil sont donc utilisés pour transmettre et recevoir les données via les ondes radio. Tout comme pour les réseaux locaux classiques, les réseaux locaux sans fil permettent de partager des ressources telles que les fichiers et les imprimantes, et d’accéder à internet. Dans un réseau local sans fil, les périphériques se connectent aux points d’accès situés au sein d’une zone déterminée. Les points d’accès sont généralement connectés au réseau par des câbles en cuivre.

**Les réseaux métropolitains (MAN) :** Un réseau métropolitain (MAN) est un réseau qui couvre une vaste zone, comme un grand complexe ou une ville. Il comprend plusieurs bâtiments interconnectés en réseaux fédérateurs sans fil ou à fibres optiques. Les lignes et équipements de communication appartiennent à un consortium d’utilisateurs ou à un fournisseur d’accès, qui vend ce service aux utilisateurs. La technologie des réseaux métropolitains est également exploitée pour relier des réseaux d’entreprise. Un MAN peut être un réseau à haut débit permettant le partage de ressources locales.

**Les réseaux étendus (WAN) :** Un réseau étendu (WAN) relie entre eux plusieurs réseaux plus petits (des réseaux locaux ou des réseaux métropolitains) situés sur des sites éloignés les uns des autres. Internet est un vaste réseau étendu composé de millions de réseaux locaux interconnectés. Les prestataires de services dans le domaine des télécommunications sont chargés d’interconnecter ces réseaux locaux dispersés géographiquement. La technologie des réseaux étendus est également exploitée pour relier des réseaux d’entreprise.

V. Les types d’organisation en réseau :

Les réseaux sont organisés de façon centralisée ou décentralisée. Les organisations centralisées sont :

* Les premiers réseaux étaient propriétaires et centralisés, ils étaient conçus, fabriqués et mise en œuvre par une seule société (c’était le temps du monopole d’IBM).
* L’architecture d’un réseau propriétaire était centralisée autour d’un gros ordinateur très puissant, pour l’époque, et de terminaux passif qui interrogeaient le super calculateur central.

Les organisations décentralisées sont :

* Désormais, la conception d’une machine et l’organisation d’un réseau se sont largement ouvertes aux autres.
* L’on parle de réseaux décentralisés, répartis ou distribués. Les petites machines sont devenues bien plus puissantes avec les progrès de la technologie.
* C’est l’ère de la compatibilité, de la normalisation, de l’interopérabilité et des environnements hétérogènes (plusieurs types de machines peuvent cohabiter sur un réseau, plusieurs systèmes d’exploitation doivent coopérer ensembles, l’organisation interne et externe des réseaux est bien plus ordonnée et contrôlée).
* Internet est un exemple de réseau distribué.

Les réseaux sont dits soit :

* Des réseaux « postes à postes » également appelés des réseaux « Peer to Peer ou point à point » ou « d’égal à égal ».
* Des réseaux sur serveur (également appelé réseaux client/serveur).
* Dans un réseau Peer-to-Peer (P2P), il n’y a pas de serveur dédié ni de hiérarchie entre les ordinateurs.
* Chaque périphérique (ou « client ») possède des fonctionnalités et responsabilités équivalentes.
* Chaque utilisateur est responsable de ses propres ressources et peut décider quelles données et quels périphériques partager ou installer.
* De ce fait, il n’existe aucun point central de contrôle ou d’administration du réseau.
* Les réseaux Postes à Postes sont faciles et pas cher à installer et conviennent pour les petites structures (moins de quinze postes) avec des utilisateurs compétents pour administrer eux-mêmes leur propre machine, et où la sécurité des données n’est pas un enjeu déterminant.
* Le modèle Peer-to-Peer est un exemple d’architectures distribuées ou chaque ordinateur est à la foi serveur de données et client des autres.
* Lorsqu’un ordinateur accède à des informations ou des ressources sur un autre ordinateur cible, l’ordinateur cible voit ses performances diminuer.

Les réseaux P2P présentent toutefois plusieurs inconvénients :

* Il n’y a pas d’administration centralisée ; de ce fait, il est difficile de déterminer qui contrôle les ressources du réseau.
* Il n’y a pas de sécurité centralisée ; Chaque ordinateur doit utiliser des mesures de sécurité distinctes pour la protection des données.
* Le réseau devient plus complexe et plus difficile à gérer à mesure que le nombre d’ordinateurs augmente.
* Il n’y a pas forcément de stockage commun et centralisé des données. Il faut gérer des sauvegardes de données séparées. Cette tâche est de la responsabilité de chaque utilisateur.

Les réseaux client/serveur sont :

* Les logiciels installés sur les serveurs permettent à ces derniers de fournir des services, comme la messagerie ou les sites Web, à des clients.
* Chaque service nécessite un logiciel serveur distinct.
* Par exemple, un serveur nécessite un logiciel de serveur Web pour pouvoir fournir des services Web au réseau.
* Dans un réseau client-serveur, le client demande des informations ou des services au serveur.
* Le serveur fournit les informations ou les services demandés au client.
* Cela permet une administration réseau centralisée ; de ce fait, il est facile de déterminer qui contrôle les ressources du réseau.
* Le serveur devra être véritablement multitâche afin de pouvoir servir un grand nombre de requêtes en même temps et de façon équitable, c’est-à-dire en octroyant le même temps processeur à chaque client.
* Un même ordinateur peut offrir plusieurs services (ex : serveur de fichiers, serveur Web et serveur de messagerie).
* Un seul ordinateur peut également exécuter différents types de logiciel client. Un logiciel client doit être installé pour chaque type de service requis.
* A l’aide des différents logiciels clients, l’ordinateur peut se connecter à différents serveurs simultanément.
* Par exemple, un utilisateur peut consulter sa messagerie électronique et une page Web en même temps qu’il utilise la messagerie instantanée et écoute la radio sur Internet.
* Avec une architecture Client/serveur, il est facile de savoir qui contrôle les ressources sur les réseaux grâce à son administration de réseau centralisée.
* L’administration réseau implémente les sauvegardes des données et les mesures de sécurité. Il contrôle aussi l’accès des utilisateurs aux ressources du réseau.
* Toutes les données du réseau sont stockées sur un serveur de stockage centralisé.
* Chaque utilisateur doit fournir un nom d’utilisateur et un mot de passe valides pour pouvoir accéder aux ressources réseau que l’administrateur lui a autorisé.

Chapitre 2 : Normalisation des réseaux

I. Normes Ethernet :

Plusieurs organismes de normalisation internationaux sont chargés de la conception des normes de mise en réseau. Ces normes sont utilisées par des fabricants dans la mise au point de leurs technologies, particulièrement dans le domaine des communications et de la mise en réseau. Les normes permettent de garantir la compatibilité entre périphériques de différents fabricants, grâce à l’utilisation de technologies communes. Les groupes de normalisation créent, étudient et mettent à jour les normes. Ces normes répondent aux attentes du marché en termes d’augmentation de la bande passante, d’efficacité des communications et de fiabilité du service.

IEEE 802.3 est une norme pour les réseaux informatiques édictée par l’Institute of Electrical and Electronics Engineers (IEEE). Cette norme est généralement connue sous le nom d’Ethernet.

II. Modèles de référence :

Un modèle architectural est un cadre de référence commun servant à expliquer les communications Internet et à développer des protocoles de communication. Il sépare les fonctions des protocoles en couches distinctes pouvant être gérées individuellement. Chaque couche a une fonction, spécifique dans la communication réseau. Au début des années 1980, l’Organisation internationale de normalisation (ISO) a mis au point le modèle de référence OSI (Open Systems Interconnect), destiné à normaliser la manière dont les périphériques communiquent sur un réseau. Le modèle OSI est un modèle comprenant 7 couches.

Bien qu’il existe d’autres modèles, la plupart des fournisseurs de solutions réseau actuels conçoivent leurs produits sur la base de ce cadre. Un système qui met en œuvre une gestion des protocoles en les implémentant dans la série des couches de ce modèle fonctionne en utilisant une « pile de protocoles ». Les piles de protocoles peuvent être implémentées au niveau logiciel ou matériel, ou les deux. Généralement, seules les couches basses du modèle sont implémentées au niveau matériel, tandis que les couches supérieures sont implémentées au niveau logiciel. Chaque couche du modèle OSI est responsable d’une part du traitement, pour préparer les données à leur transmission sur le réseau.

Les données transférées traversent virtuellement chaque couche du modèle OSI (de la plus haute à la plus basse) au niveau de l’ordinateur expéditeur, puis elles remontent ces mêmes couches dans l’ordinateur de destination. Lorsqu’un utilisateur envoie des données, par exemple un e-mail, le processus d’encapsulation démarre à la couche Application. La couche Application fournit un accès réseau aux applications. Les informations traversent les trois couches supérieures et sont considérées comme des données lorsqu’elles arrivent à la couche Transport (4).

Au niveau de l’ordinateur de destination, une opération appelée désencapsulation a lieu. Il s’agit de l’inverse de l’encapsulation. Les bits arrivent à la couche Physique du modèle OSI de l’ordinateur de destination. La remontée virtuelle du modèle OSI, sur l’ordinateur de destination, amène les données jusqu’à la couche Application, où un programme de messagerie électronique affiche l’e-mail.

**Remarque :** Il existe des moyens mnémotechniques pour vous aider à mémoriser les sept couches du modèle OSI.

Le modèle OSI et le modèle TCP/IP sont tous deux des modèles de référence utilisés pour décrire le processus de communication des données. Le modèle TCP/IP est utilisé spécifiquement avec la suite de protocoles TCP/IP et le modèle OSI sert dans le développement d’une communication normalisée, entre les différents fabricants d’équipements et éditeurs d’applications. Un modèle TCP/IP fonctionne sur le même principe que le modèle OSI, mais il utilise quatre couches au lieu de sept.

On utilisera un câblage croisé pour connecter deux machines de même type, pour connecter deux machines de types différents on utilisera un câble droit.

Chapitre 4 : L’adressage des équipements réseaux.

I. Adresse physique :

Toutes les formes de communication nécessitent un moyen d’identifier la source et la destination. Dans la communication humaine, la source et la destination sont représentées par des noms. Lorsqu’un nom est prononcé, la personne qui le porte, écoute le message et y répond. Les autres personnes présentes dans la pièce peuvent entendre le message, mais l’ignorent car il ne leur est pas adressé. Sur les réseaux Ethernet, une méthode similaire existe pour identifier les hôtes source et de destination. (Ce cas se présentera plutôt dans la situation de communication avec un HUB.)

Chaque hôte connecté à un réseau Ethernet possède une adresse physique qui sert à identifier l’hôte sur le réseau. Elles constituent un moyen d’identifier les gens. Sur un hôte, l’adresse MAC (Media Access Control, contrôle d’accès au support) est attribuée à la carte réseau de l’hôte. On l’appelle également « adresse physique ». L’adresse physique ne change pas, quel que soit l’emplacement de l’hôte sur le réseau, de la même manière que les empreintes digitales d’une personne restent identique où qu’elle aille.

Les adresses MAC sont définies par le standard IEE 802. Elles sont physiquement écrites sur la PROM, de la carte réseau par les constructeurs. Elles sont constituées de 6 groupes de 2 valeurs hexadécimales, s éparés par un tiret ( - ) ou un double point ( : ). Par exemple : E0 :2A :82 :A5 :2E:57.

Chaque groupe correspond à 1 octet variant de 0 à 255. Soit un total de 48 bits pour l’adresse MAC. Il existe donc potentiellement 2^48 (environ 281 000 Milliards) d’adresses MAC possibles. L’IEE donne des préfixes de 24 bits aux fabricants, ce qui offre potentiellement 2^34 (environ 16 millions) d’adresses MAC différentes utilisables en même temps.

II. L’adressage logique :

L’adresse MAC permet d’identifier la machine. Cependant les applications doivent éviter d’utiliser cette adresse car il faudrait changer dès lors qu’on change un ordinateur ou une carte dans le réseau. Une adresse IP est un numéro utilisé pour identifier un périphérique situé sur un réseau. L’adresse IP est similaire à l’adresse postale d’une personne. On l’appelle « adresse logique », car elle est attribuée de manière logique à l’hôte en fonction de son emplacement.

L’adresse IP, ou adresse réseau basée sur le réseau local est attribué à chaque hôte par un administrateur réseau. Le protocole IP fournit une structure d’adressage chargée du transfert des données d’un ordinateur source vers un ordinateur de destination. Il permet une transmission fiable des données. Cela ressemble à l’attribution d’une adresse postale à une personne, par la municipalité, en fonction de l’organisation logique de la ville.

Une adresse IPv4 se compose d’une série de 32 bits binaire. En décimal, ce nombre est environ égal à un 4 suivi de neuf zéros. Il est très difficile pour un être humain de lire une adresse IPv4 binaire. Les 32 bits sont regroupés en quatre segments de 8 bits appelés octets. Chaque octet est présenté en valeurs décimales séparées par des points. C’est ce qu’on appelle la notation en décimal à point : 192.168.1.5.

III. Adressage IPv4 :

L’adresse IPv4 est constituée de deux parties. La 1ère partie appelée Net Id (Network Identifier) identifie le réseau et la 2ème partie appelée Host Id (Host Identifier) identifie un hôte sur ce réseau. Prenons un exemple : si un hôte a pour adresse IPv4 192.168.18.57, les trois premiers octets (192.168.18) identifient la partie réseau et le dernier octet (57) identifie l’hôte. C’est ce qu’on appelle l’adressage hiérarchique.

Les adresses IPv4 se divisent en cinq classes :

* Classe A : réseaux de grande taille, implémentés par de grandes entreprises.
* Classe B : réseaux de taille moyenne, implémentés par des universités et des entreprises de taille intermédiaire.
* Classe C : petits réseaux, implémentés par des petites entreprises ou fournisseur d’accès internet (FAI) pour les abonnements clients.
* Classe D : utilisation réservée à la multidiffusion, comme des émissions WEB ou de la vidéo en continu vers un groupe spécifique.
* Classe E : utilisation réservée aux tests expérimentaux.

Classe A :

Le premier octet représente le réseau. Si le bit de poids fort (gauche) est 0, il s’agit d’une classe A.

Poids fort -> 01110101 <- Poids faible

Le réseau de classe A peut contenir 224 – 2 = 16777214 ordinateurs.

Classe B : 128 > X < 192

Les deux premiers octets représentent le réseau. Si les deux premiers bits du poids fort sont 10, c’est une classe B.

10110101

Le réseau de classe B peut contenir 216 – 2 = 65534 ordinateurs.

Classe C :

Les trois premiers octets représentent le réseau. Si les trois premiers bits de poids fort sont 110, c’est une classe C.

11010101

Les réseaux privés :

Les réseaux privés ne sont pas reliés aux réseaux publics. Les adresses réseaux privées ne sont pas acheminées sur internet. Cela permet à des réseaux de différents sites d’utiliser le même schéma d’adressage privé sans que cela occasionne de conflits d’adressages.

Internet Assigned Number Authority (IANA)

Les adresses publiques sont utilisées sur internet alors que les adresses privées ne peuvent pas circuler sur internet.

* IP Public -> acheté ou fourni par le FAI
* IP Privée -> paramétrée par l’administrateur du réseau local.

Adressage IP privé automatique :

Si l’ordinateur n’arrive pas à communiquer avec le serveur DHCP pour obtenir une adresse IP, Windows utilise l’adresse IP privée automatique (APIPA).