**Acquis :** A : 127.0.0.0, B : 128.0.0.0 – 191.255.0.0, C : 192.0.0.0 – 223.255.255.0

- Oublier pas d’enlever le broadcast et l’adresse du réseau au calcule du nombre des machines.   
- Un routeur sert à sortir à l'extérieur du réseau, segmenter un réseau.  
- La couche 1 sert à coordonner la suite de signaux et la synchronisation des systèmes émetteurs et récepteurs (répéteur).  
- Couche 3 c’est le routeur, la 2 (liaison) c’est le pont et le répartiteur, la couche 7 (passerelle)  
- Le hub et le switch fonctionne en mode « promiscues »  
- Le fonctionnement de base d’un réseau Ethernet : c'est un réseau maillé qui relie des réseaux, CSMA/CD, multiple access  
- Le switch peut remplacer un routeur car il possède toutes ces fonctionnalités

**FAI :** Fournisseur d’Accès à Internet = ISP

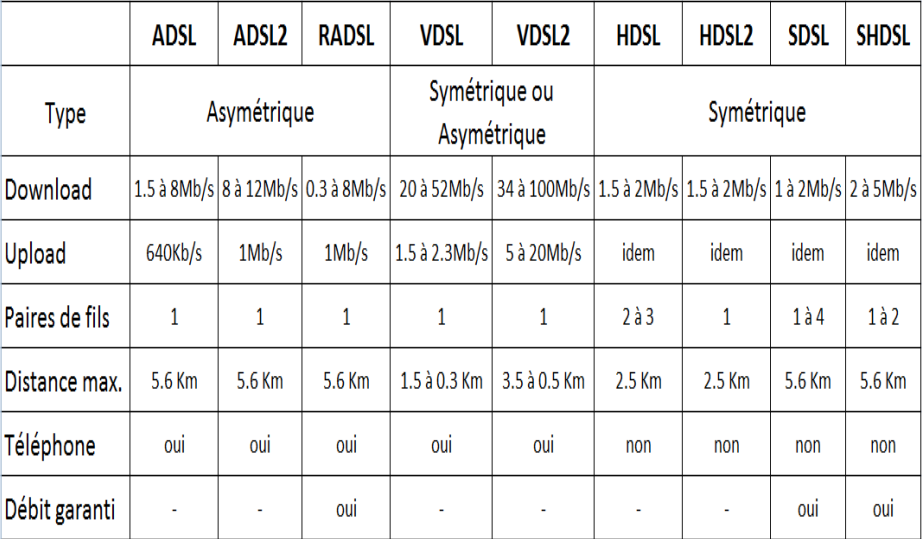
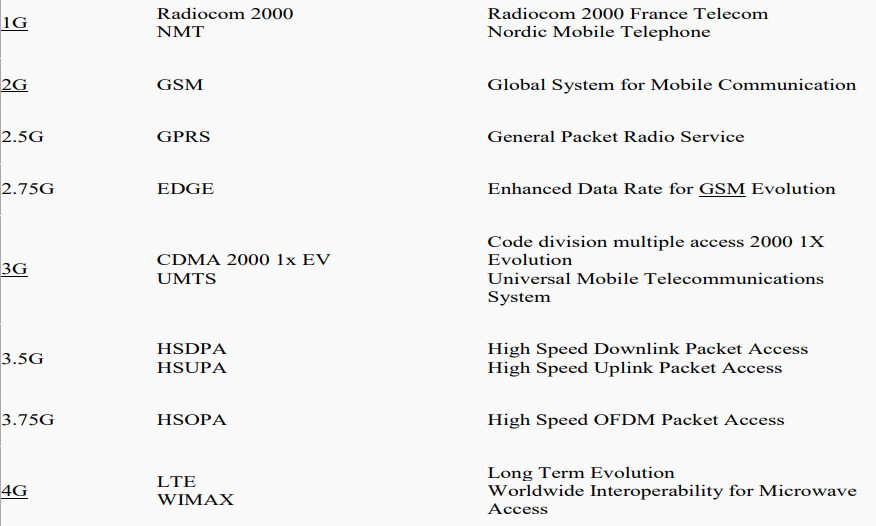
A voir : la couverture, la bande passante, prix, l’accès, le service téléphonique, le service technique, IP fixe, hébergement.

• E0 (64Kbps) • E1 = 32 lignes E0 (2Mbps) • E2 = 128 lignes E0 (8Mbps) • E3 = 16 lignes E1 (34Mbps) • E4 = 64 lignes E1 (140Mbps)

Connexions: Fibre, Ligne téléphonique, Satellite, Wifi

**DSL :**

La DSL est une technologie de transmission numérique à large bande qui consiste à acheminer des signaux numériques sur une ligne d’abonné numérique.

Le terme **DSL ou xDSL** peut se décliner en plusieurs groupes : HDSL, SDSL, (<= symétrique) ADSL, RADSL, VDSL. A chacun de ces groupes correspond une utilisation et des caractéristiques particulières. Les différences entre ces technologies sont à différencier par : • La vitesse de transmission. • La distance maximale de transmission. • La variation de débit entre le flux montant et le flux descendant. • Le caractère symétrique ou non de la liaison. • Le nombre de paires cuivre utilisées. Les technologies **xDSL** sont divisées en deux grandes familles. • Celle utilisant une transmission asymétrique. • Celle utilisant une transmission symétrique.

Différents protocoles sont utilisés pour se connecter à Internet : GPRS (General Packet Radio Service, 2.5G) EDGE (Enhanced Data Rates for GSM Evolution, 2.75G) UMTS (Universal Mobile Telecommunications System, 3G) HSDPA (High Speed Downlink Packet Access, 3.5G) LTE (Long Term Evolution, 4G). Exemple de débit de données de ces différent protocoles : GPRS: jusqu’à 85.6 Kb/s EDGE: jusqu’à 236.8 Kb/s UMTS: jusqu’à 384 Kb/s HSDPA: jusqu’à 7.2 Mb/s / 2.0 Mb/s LTE: jusqu’à 300 Mb/s / 75 Mb/s

**Routeur :**

Les paramètres du Wi-Fi sont par défaut : - Wi-Fi activé - SSID visible sur le réseau local (e.g.: Zyxel) - Sécurité désactivé (pas de Wep, pas de Wpa2, …) - Pas de liste de droits d’accès

**Ports :**

Les ports permettent d’exécuter de nombreux programmes TCP/IP simultanément sur Internet. Chaque application est liée à une adresse unique sur la machine, codée sur 16 bits, un port. La combinaison de l’adresse IP et du port est alors une adresse unique au monde qui est appelée un socket. L'adresse IP sert donc à identifier de façon unique un ordinateur. Le numéro de port indique l'application à laquelle les données sont destinées. (OSI 4, DNS : 53, 65’536 possibilités, Les ports 0 à 1023 sont les « ports réservés » pour les services bien connus « Well-Know Services » (processus système), Les ports 1024 à 49151 sont appelés «ports enregistrés», Les ports 49152 à 65535 sont les «ports dynamiques et/ou privés»). Liste de ports : *%SystemRoot%\System32\Drivers\etc\Service*

**NAT :**

Translation d’Adresse Réseau, L’objectif du NAT est de changer une adresse IP par une autre.

*NAT statique* : on associe 1 adresse interne avec 1 adresse externe, on ne touche pas au port, on a besoin d’autant d’adresse externes que de machines sortantes du réseau.  
*NAT dynamique* : on dispose d’un pool d’adresses externes: on associe 1 adresse interne à 1 adresse du pool seulement quand c’est nécessaire et pour un temps limité. Le routeur conserve la correspondance dans une table, on utilise un minimum d’adresses externes, on doit limiter le nombre d’accès simultanés à l’extérieur, la correspondance change (on ne peut pas joindre une machine interne de l’extérieur facilement).  
*NA-PAT*: on utilise 1 ou plusieurs adresses extérieures et l’on remplace l’adresse interne ET le port interne par une adresse extérieure et un port externe libre. Le routeur conserve la correspondance dans une table, moins de limitations, la correspondance change (on ne peut pas joindre un machine interne de l’extérieure facilement), plus de calculs au niveau du routeur

**Du port forwarding** peut être utilisé à la place du NAT statique (pour les paquets entrants on détermine l’hôte interne en se basant uniquement sur le port. Pour par exemple différencier le trafic vers le serveur web, le web mail, le vpn, le ftp … Utile si on a 1 adresse seulement)

On peut dans un réseau typique utiliser le NAT statique pour des serveurs accessibles depuis l’extérieur (extranet, webmail, site internet…) et du NAT-PAT pour les postes de travail.

**Proxy :**

Un serveur proxy ou « serveur mandataire »» est une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et Internet.

Les principales fonctions d'un serveur proxy sont le **cache**, le **filtrage**, **l’authentification**, **le reverse proxy**, **masquage**. La fonction cache est la capacité de garder en mémoire les pages, des sites Web, les plus souvent visités par les utilisateurs. Le filtrage permet, d’une part, d’assurer un suivi des connexions (logging, tracking) et d’autre part de filtrer les accès à Internet. L’authentification permet de donner l’accès à certaines ressources externes aux personnes autorisées. Le reverse-proxy (relais inverse) permet aux utilisateurs d’Internet d’accéder indirectement à certains serveurs internes. Le proxy anonyme ou masquage peut masquer les informations concernant votre ordinateur (OS, adresse IP, …). En plus, il peut supprimer les cookies, les pop-ups, les bannières, les scripts, les informations confidentielles (Identifiant et mot de passe).

Un proxy peut aussi faire de la translation d'adresse. Il peut transformer les adresses locales privées en adresses routables (NAT). Il peut aussi sortir avec une adresse différente de celles des stations locales. Cette dernière méthode augmente la sécurité et permet d’escamoter l’adresse locale.

Un proxy peut avoir un lien avec la DMZ. On le trouvera derrière le pare-feu, du côté du réseau local. Il aussi possible qu’il se trouve directement dans la DMZ entre deux pare-feu.

**Firewall :**

En informatique l'usage du terme « pare-feu » est donc métaphorique, il évoque une porte empêchant les flammes d'Internet d'entrer chez soi et/ou de « contaminer » un réseau informatique.

- un programme installé sur un ordinateur. - un appareil à part entière (e.g: Cisco ASA 5585-X). - une service installé sur un routeur «multitâches» (e.g: Zyxel 460N, …)

**Un système pare-feu** contient un ensemble de règles prédéfinies. Il permet d'autoriser la connexion, de bloquer la connexion, de rejeter la demande de connexion sans avertir l'émetteur. ♣ **Allow** : autoriser la connexion ♣ **Deny** : bloquer la connexion ♣ **Drop** : rejeter la demande de connexion, On distingue deux types de politiques de sécurité : • autoriser uniquement les communications ayant été explicitement autorisées ; • empêcher les échanges qui ont été explicitement interdits.

**Un système pare-feu fonctionne** sur le principe du filtrage simple de paquets. Les paquets de données, analysés par le pare-feu, possèdent les entêtes suivantes : • adresse IP de la machine émettrice; • adresse IP de la machine réceptrice; • type de paquet (TCP, UDP, etc.); • numéro de port. [Règle, Action, IP source, IP dest, Prot., port source, port dest] any -> n’apport

**Le filtrage dynamique** de paquets permet d'effectuer un suivi des transactions entre le client et le serveur. De nombreux services, comme FTP, initient une connexion sur un port statique, mais ouvrent dynamiquement un port afin d'établir une session entre la machine serveur et la machine cliente. Le filtrage dynamique permet de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage (OSI 3 et 4). De cette manière, l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

**Le filtrage applicatif** permet de filtrer les communications application par application (OSI 7). Un firewall effectuant un filtrage applicatif est appelé généralement passerelle applicative ou proxy. Il est recommandé de dissocier le pare-feu du proxy, afin de limiter les risques de compromission. Il faut surveiller le journal d'activité du pare-feu et se tenir au courant des alertes de sécurité.

**DMZ :**

La DMZ (DeMilitarized Zone) est une zone tampon d'un réseau, située entre le réseau local et le réseau public (Internet). Elle contient des services publics comme HTTP, SMTP, FTP, DNS, etc… Son premier but est d'éviter toute connexion directe du réseau interne à Internet. Son deuxième but est de bloquer toute attaque extérieure depuis le réseau public (Internet). **La gestion de cette zone DMZ peut être gérée par un pare-feu et/ou un serveur proxy.**

*La politique de sécurité* mise en œuvre sur la DMZ est généralement la suivante : • trafic du réseau externe vers la DMZ autorisé, mais limité par les règle du pare-feu ; • trafic du réseau externe vers le réseau interne interdit ; • trafic du réseau interne vers la DMZ autorisé, mais limité par les règle du pare-feu ; • trafic du réseau interne vers le réseau externe autorisé ; • trafic de la DMZ vers le réseau interne interdit ; • trafic de la DMZ vers le réseau externe refusé.

**Variantes** : La DMZ possède donc un niveau de sécurité intermédiaire, on ne stockera pas des données critiques. Il est possible d’installer des DMZ en interne afin de cloisonner le réseau interne. L'inconvénient est que si cet unique pare-feu est compromis, plus rien n'est contrôlé. Il est cependant possible d'utiliser deux pare-feu en cascade afin d'éliminer ce risque. Il existe aussi des architectures de DMZ situées entre le réseau Internet et le réseau local, séparée de chaque côté par un pare-feu.

**IP Forwaring :**

L’IP Forwarding permet de rendre accessible un serveur (ou une station) se trouvant du côté LAN depuis l’extérieur (Internet). Le serveur se trouvant du côté LAN ne sera accessible que pour une application donnée. L’application sera définie par son port correspondant. Il est possible qu’une application utilise plusieurs ports. Pour accéder au service du serveur depuis l’extérieur, l’adresse du routeur côté WAN sera utilisée.

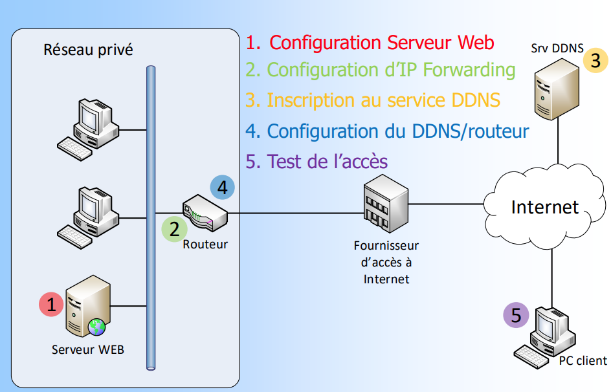
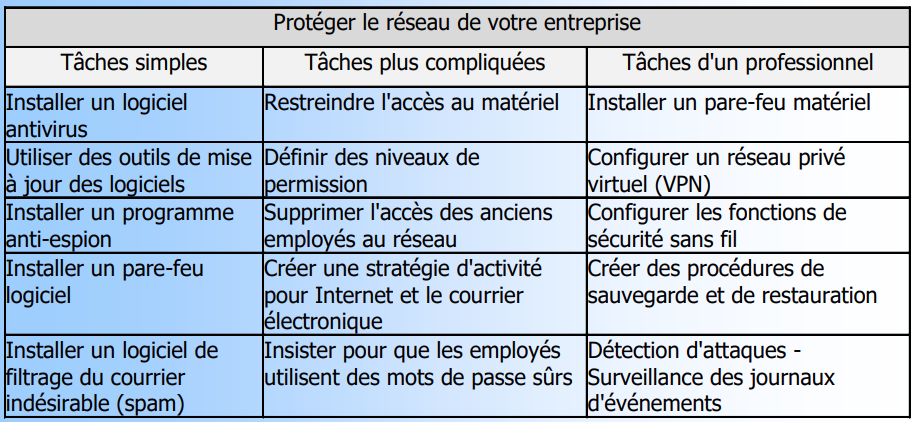
**Port mapping :**

Le Port Mapping est une variante de l’IP Forwarding. Ce système permet aussi de rendre accessible une station se trouvant du côté LAN depuis l’extérieur comme l’IP Forwarding. La différence se trouve dans le numéro du port utilisé entre le routeur et l’application. Le numéro du port utilisé pour l’application sera différent de celui utilisé pour donner l’accès au niveau du routeur. L’avantage est la sécurité, car pour accéder au service, il faut connaître le port paramétré sur le routeur

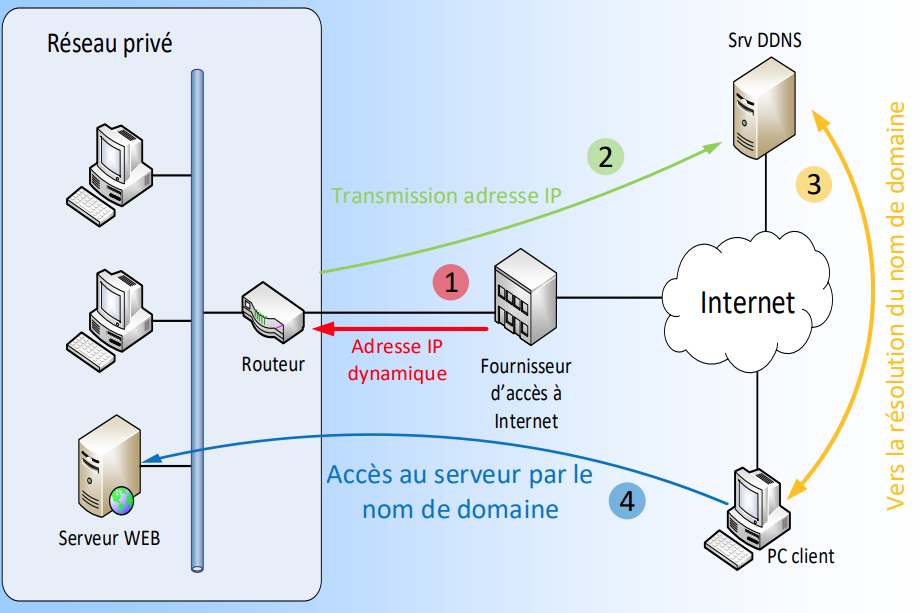
**Topologies :**

Dans la topologie en étoile, chaque station est reliée à un nœud central qui peut être soit un hub soit un switch. Maillé tout est interconnecté.

**Sécurité :**



**DDNS :**

****Le DDNS est un service qui permet de lier une adresse IP dynamique à un nom domaine fixe. Si vous voulez, par exemple, rendre accessible un serveur Web installé dans un réseau local (adresse privé). Votre serveur ne sera atteignable que par l’adresse externe de votre routeur (WAN). Grâce à ce service, chaque fois que votre routeur reçoit une nouvelle adresse, distribuée par votre provider, votre routeur informera le service DDNS. Sans le DDNS, il faut connaître l’adresse du routeur côté WAN et si celle-ci change, c’est ennuyant. Il faut évidemment avoir paramétré votre routeur pour rendre accessible votre serveur Web depuis l’extérieur (IP forwarding).

**QoS :**

Le QoS, ou la Qualité de Service, est le fait de mettre une priorité à certains services utilisant le réseau, comme la téléphonie VoIP, la messagerie, les vidéo-conférences ou la vidéosurveillance. Il permet de classer les différents types d'applications selon leur importance, afin d'y assigner plus ou moins de bande passante et ainsi d'optimiser le réseau et de diminuer la latence. La mise en place d'un QoS est particulièrement recommandée si votre réseau gère des applications lourdes et sensibles à la latence (flux vidéo, voix, …) ou si vous avez des liens de faible qualité entre du matériel critique (serveurs,…).

Le délai de transit ou latence est un délai dans les communications informatiques. Elle désigne le temps nécessaire à un paquet de données pour passer de la source à la destination à travers un réseau. Le débit est la bande passante utilisé par un flux. Celui-ci peut être constant ou variable. La gigue dans un flux de paquets IP est la variation du délai de transit entre plusieurs paquets IP. Ce paramètre est très important pour les applications de voix sur IP (VoIP) car les codecs de compression de la voix sont très sensibles à la gigue. La perte de paquets est le pourcentage de paquets IP perdus sur le réseau.

**VPN :**

Le VPN est un tunnel (ou une liaison virtuelle) sécurisé permettant la communication entre deux entités (Internet). Cette technologie permet de créer une liaison virtuelle entre deux réseaux physiques distants de manière transparente pour les utilisateurs concernés. Les données envoyées au travers de ces liaisons virtuelles sont chiffrées, ceci garantit aux utilisateurs qu’en cas d’interception malveillante les données soient illisibles.

Un VPN repose sur un ou des protocoles, appelé protocoles de « tunnelisation» (tunneling).

**Fonctionnement** : Dans les faits, nous établissons une connexion sécurisée avec le serveur qui nous propose le service VPN. Ce serveur VPN nous connecte sur Internet en masquant notre adresse IP par son adresse IP. Une communication VPN peut donc être de client à serveur mais il est à prendre en considération qu’elle peut aussi se faire de serveur à serveur.

**Les principaux protocoles utilisés sont :**

**L2F** (Layer Two Forwarding) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. A noter qu’il est désormais obsolète.   
**PPTP** (Point-to-Point Tunneling Protocol) est aussi un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.  
**L2TP** (Layer Two Tunneling Protocol) est protocole de niveau 2 s’appuyant sur PPP, et qui fait converger les fonctionnalités de PPTP et L2F.  
**GRE** (Generic Routing Encapsulation) est développé par Cisco, mais qui est souvent remplacé par L2TP.   
**IPSec** est un protocole de niveau 3, issu des travaux de l’ IETF (Internet Engineering Task Force), groupe participant à l’élaboration des standards Internet). Il permet de transporter des données chiffrées pour les réseaux IP.   
**SSL** (Secure Sockets Layer) offre une très bonne solution de tunnelisation. L'avantage de cette solution est de permettre l'utilisation d'un navigateur Web comme client VPN. On peut accéder à ce type de VPN avec un navigateur web via «https». Il permet aux utilisateurs de mettre en place une connexion sécurisée au réseau depuis n’importe quel navigateur Web.

**Radius :**

Le RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification. Le protocole RADIUS a été inventé et développé en 1991 par la société Livingston, qui fabriquait des serveurs d'accès au réseau pour des matériels uniquement équipés d'interfaces série. Le RADIUS peut être utilisé par les FAI pour identifier les clients à l’aide d’un serveur LDAP ou utilisé par des points d’accès WiFi pour accéder à un réseau.

****

Une image contenant texte, Police, capture d’écran, ligne

Description générée automatiquement

Il existe 4 types de paquets pour effectuer une authentification RADIUS :

**- Access-Request** : envoyé par le NAS contenant les informations sur le client qui souhaite se connecter (login/mot de passe, adresse MAC…)   
**- Access-Accept** : Envoyé par le serveur pour autorisé la connexion si la vérification des informations est correct.   
- **Access-Reject** : Envoyé par le serveur pour refuser une connexion en cas d’échec de l’authentification ou pour mettre fin à une connexion.  
**- Access-Challenge** : Envoyé par le serveur pour demander la réémission d’un access-request ou des informations complémentaires

- Le protocole 802.1X a été mis au point par l’IEEE en juin 2001.   
- 802.1X est un standard lié à la sécurité des réseaux informatiques.   
- Il permet de contrôler l'accès aux équipements d'infrastructures réseau.  
- Il a pour but d’authentifier un client afin de lui autoriser l’accès à un réseau.   
- On utilise le protocole EAP (Extensible Authentication Protocol) et un serveur d’authentification qui est généralement un serveur RADIUS   
- Le serveur RADIUS va authentifier chaque client qui se connecte au réseau sur un port.

EAP signifie Extensible Authentication Protocol. C’est un protocole de communication réseau qui est constitué d'un échange de trames dans un format spécifique à EAP pour réaliser l'authentification d'un partenaire. C’est est un protocole de communication réseau embarquant de multiples méthodes d'authentification. Dans notre cas, c’est lui qui fait le lien entre le client (supplicant) et le client RADIUS (Authenticator).

- EAP-TLS (Transport Layer Security) : Authentification par certificat du client et du serveur   
- EAP-TTLS (Tunneled Transport Layer Security) : Authentification par certificat et mot de passe grâce à la génération d’un tunnel sécurisé   
- EAP-MD5 : Authentification avec mot de passe   
- PEAP (Protected EAP) : Authentification avec mot de passe via une encapsulation sécurisée   
- LEAP (protocole Cisco) : Authentification avec mot de passe via une encapsulation sécurisée Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Le Diameter est un protocole d'authentification, successeur du protocole RADIUS. Il est notamment utilisé dans le cœur des réseaux de téléphonie mobile pour accéder aux bases de données HLR et HSS permettant d'identifier, d'authentifier et de localiser les abonnés mobiles 3G et LTE /4G. Contrairement à RADIUS, son nom est un jeu de mot, diameter, signifiant diamètre en anglais, qui est le double du rayon, radius en anglais. Quelques différences avec RADIUS : Il utilise le protocole TCP, il peut utiliser le transport réseau sécurisé (IPsec ou TLS), La taille des attributs est augmentée, il est mieux adapté au roaming.

Avantages : - Sécurité - Fiabilité - Centralisation de l’authentification Inconvénients : - Lourd à mettre en place - Limité à 254 octets par attribut

# Packet tracer

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

# Questions

**1. De quoi dépend le débit d’une connexion ADSL ?**

- Distance entre le client et la centrale   
- Diamètre du câble

**2. A quoi servent les protocoles de la famille PPP ?**

À connecter un client vers une FAI

**3. Combien de bits codent un port ?**

16 bits

**4. Qu’est-ce qu’un « socket » ?**

Somme de l'adresse IP et du port

**5. Citez la plage de ports réservés.**

0 à 1023 (port reconnus)

**6. Expliquez le principe du NAT statique.**

Associer une IP publicque à une IP privée interne au réseau

**7. Qu’est-ce que le PAT et à quoi sert-il ?**

Protocole qui permet d'affecter un port source différent à chaque requête

**8. Qu’est-ce que le « port forwarding » ?**

Extension du NAT qui permet d'acéder à un serveur (réseau local) depuis l'extérieur (Internet)

**9. Qu’est-ce que le « port mapping » ?**

Port forwarding mais le port ouvert sur le routeur est différent de celui de l'application locale

**10. Quel est le principe de base de fonctionnement d'un proxy ?**

Le serveur proxy est mandaté par une application pour effectuer une requête sur Internet à sa place

**11.Qu’est-ce que le « DDNS » ?**

DNS Dynamique permet de lier une IP dynamique à un nom de domaine statique

**12. Quel est le principe du VPN ?**

Relier deux réseaux locaux de manière fiable et privée en créant un tunnel

**13. Que signifie le terme QoS ?**

Quality of Service permet de préciser des spécifications de bande passante/temps de réponse par protocole

**14. Citez les deux modes opératoires définis par le standard 802.11 ?**

Mode infrastructure : clients connectés à un point d'accès   
Mode ad hoc : clients connectés entre eux

**15.Qu’est-ce que l’ « itinérance » ou le « roaming » ?**

Lorsqu'un utilisateur nomade peut passer automatiquement d'un point d'accès à un autre

**16.Quelle est l’amélioration du système MIMO ?**

La portée et le débit

**17. Quelle est l’amélioration du système de cryptage du WPA2 ?**

Chiffrement par AES (nouvel algorithme de chiffrement du gouvernement américain)

**18. Quel est le meilleur moyen de détecter les intrusions ?**

Surveiller les journaux d'évènements

Une image contenant texte, capture d’écran, Police

Description générée automatiquementUne image contenant texte, Police, capture d’écran, algèbre

Description générée automatiquementUne image contenant texte, capture d’écran, Police, algèbre

Description générée automatiquementUne image contenant texte, capture d’écran, Police

Description générée automatiquementUne image contenant texte, capture d’écran, Police

Description générée automatiquementUne image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement