Correction exercice 7 série 4

Exercice 7

1. Quelle est la différence entre multicaste et unicaste
2. Quelle est la différence entre multicaste et brodcast.
3. Différence entre Répéteur et Amplificateur
4. Différence entre un Pont et une Passerelle – Réseau informatique
5. Différence entre Un pare-feu (firewall) et passerelle (getway)
6. Différence entre internet, intranet
7. Donner une comparaison entre Fibre optique et cable coaxiale
8. C'est quoi Network Interface Card (NIC) ou (Carte d'Interface Réseau)
9. Quel est le connecteur des câbles à paires torsadées ?

1.

	Broadcast	**Multicast**
Définition	Le paquet est transmis à tous les hôtes connectés au réseau.	Le paquet est transmis uniquement aux destinataires prévus dans le réseau.
Trafic	Le trafic inutilement énorme est généré dans le réseau.	Le trafic est sous le contrôle.
Bande passante	La bande passante est gaspillée.	La bande passante est utilisée efficacement.
Processus	Lourd	Rapide
La gestion	Broadcast ne nécessite aucune gestion de groupe.	Multicast nécessite une gestion de groupe pour définir le groupe d'hôtes / stations qui recevront les paquets.

2.

	Broadcast	**Multicast**
Définition	Le paquet est transmis à tous les hôtes connectés au réseau.	Le paquet est transmis uniquement aux destinataires prévus dans le réseau.
Trafic	Le trafic inutilement énorme est généré dans le réseau.	Le trafic est sous le contrôle.

	Broadcast	Multicast
Bande passante	La bande passante est gaspillée.	La bande passante est utilisée efficacement.
Processus	Lourd	Rapide
La gestion	Broadcast ne nécessite aucune gestion de groupe.	Multicast nécessite une gestion de groupe pour définir le groupe d'hôtes / stations qui recevront les paquets.

3.

	Répéteur	Amplificateur
Définition	Il décode le signal et extrait le signal original et régénère le signal puis le retransmet.	Cela augmente simplement l'amplitude du signal.
Génération de bruit	Le répéteur élimine le bruit en régénérant le signal.	L'amplificateur amplifie le signal avec le bruit.
Propriétés	Les répéteurs sont utilisés dans l'environnement stationnaire où le signal de fréquence radio est stable, tels que les bâtiments. Au contraire,..	**les amplificateurs** sont utilisés dans l'environnement mobile où le signal radio est faible et change constamment, par exemple, les zones éloignées

4.

Pont	Passerelle
- Pont(Bridge) transmet les trames entre deux segments séparés de LAN. - Un **pont** fonctionne sur les deux couches, la couche physique et la couche liaison données. - un **pont** est utilisé pour joindre deux types de réseaux similaires, est utilisé uniquement pour transférer la trame vers la destination attendue, dans un chemin le plus efficace.	- Passerelle(Gateway) est un convertisseur de protocole. - Une **passerelle** fonctionne sur toutes les sept couches du modèle OSI. - une **passerelle** est utilisée pour joindre deux réseaux différents. Elle permet à deux réseaux différents utilisant des protocoles différents de communiquer entre eux.

5.

Parfeu	Passerelle
- Un pare-feu, ou firewall, est conçu pour surveiller le trafic réseau entrant et sortant et pour déterminer si un trafic spécifique doit être autorisé ou bloqué en fonction d'un ensemble de règles de sécurité ou protocoles. - Un pare-feu peut être logiciel ou matériel. Un pare-feu logiciel est un programme installé sur chaque ordinateur et qui régule le trafic par le biais de numéros de port et d'applications, tandis qu'un pare-feu physique est une pièce d'équipement installée entre votre réseau et la passerelle. Les pare-feu remplissent trois fonctions de sécurité de base pour un réseau : le filtrage des paquets, l'inspection dynamique et le rôle de proxy des applications. • Dans le filtrage des paquets, le pare-feu opère au niveau du paquet et examine le paquet de données lorsqu'il entre ou sort du réseau informatique. Le pare-feu utilise ensuite des règles définies par l'utilisateur pour décider d''accepter ou de rejeter le paquet. Si les données sont conformes, elles peuvent être reçues et inversement, si elles ne correspondent pas aux règles, elles sont rejetées. Le filtrage des paquets est généralement assez efficace pour résister aux attaques d'un réseau local. • Contrairement au filtrage des paquets, le filtrage statique vérifie les en-têtes des paquets et divers éléments de chaque donnée, et les compare aux informations fiables de la base de données. Pendant l'examen, le paquet sera analysé par couches, en enregistrant l'adresse IP et le numéro de port, de sorte que la sécurité est plus stricte que le filtrage des paquets. • Lorsque le pare-feu agit comme un proxy d'application, il travaille au niveau de l'application pour arrêter les informations (par exemple, les logiciels malveillants qui tentent de s'introduire dans votre système) entre votre réseau interne et externe.	- La passerelle permet une communication entre deux réseaux différents avec des architectures et des protocoles différents. - Elles peuvent être mises en place sous forme de matériel, de logiciel ou d'une combinaison des deux. Selon ses fonctions, la passerelle peut être classée en trois types : passerelle de protocole, passerelle d'application et passerelle de sécurité. - La passerelle de protocole est utilisée pour la conversion de protocole entre des réseaux utilisant différents protocoles, ce qui représente la fonction la plus courante des passerelles. - La passerelle d'application peut connecter deux applications différentes au niveau de la couche application, ce qui convient à la traduction de protocoles pour une application particulière. - Quant à la passerelle de sécurité, elle peut offrir une protection contre les menaces de sécurité en ligne en appliquant les politiques de sécurité de l'entreprise et en filtrant le trafic internet malveillant en temps réel. Il existe également des passerelles multiservices sur le marché, qui utilisent une architecture multicœur haute performance et intègrent des fonctions telles que le pare-feu dynamique, la passerelle VPN, le contrôle du trafic réseau, etc., ce qui en fait des solutions idéales pour les réseaux de petite et moyenne taille.

6.

Définition d'Internet

Internet est un réseau mondial qui établit une connexion et assure la transmission entre différents ordinateurs. Il utilise à la fois le mode de communication filaire et sans fil pour envoyer et recevoir des informations telles que données, audio, vidéo, etc.

Définition de l'intranet

Un **intranet** est une partie d'Internet qui est la propriété privée d'une organisation. Il connecte tous les ordinateurs et permet d'accéder aux fichiers et dossiers du réseau. Il a un pare-feu entourant le système pour éviter que l'utilisateur non autorisé accède au réseau. Seuls les utilisateurs autorisés ont l'autorisation d'accéder au réseau.

Différences clés entre Internet et Intranet

- L'**Internet** fournit des informations illimitées qui peuvent être consultées par tout le monde alors que, dans l'**intranet**, les données circulent au sein de l'organisation.
- **Internet** permet d'accéder à tout le monde alors que l'**intranet** permet uniquement d'authentifier les utilisateurs.
- **Internet** n'appartient à aucune organisation unique ou multiple, alors que **Intranet** est un réseau privé appartenant à une entreprise ou à une institution.
- **Internet** est accessible à tous alors que l'**intranet** est restreint.
- Un **intranet** est plus sûr par rapport à **Internet**.

6.

Network Interface Card (NIC) ou (Carte d'Interface Réseau) est un composant matériel sans lequel un ordinateur ne peut pas être connecté via un réseau. Il s'agit d'une carte de circuit imprimé installée dans un ordinateur qui fournit une connexion réseau dédiée à l'ordinateur. Il est également appelé contrôleur d'interface réseau, adaptateur réseau ou adaptateur LAN.

- La carte réseau (NIC) permet les communications filaires et sans fil.
- La carte réseau permet les communications entre les ordinateurs connectés via un réseau local (LAN) ainsi que les communications via un réseau à grande échelle via le protocole Internet (IP).
- La carte réseau fonctionne à la fois au niveau de la couche physique et au niveau de la couche liaison de données, c'est-à-dire qu'elle fournit le circuit matériel nécessaire pour que les processus de couche physique et certains processus de couche liaison de données puissent s'exécuter sur celle-ci.

En règle générale, une LED situé à côté du connecteur informe l'utilisateur si le réseau est actif ou si des données y sont transférées. Selon la carte ou la carte mère, les taux de transfert peuvent être de 10, 100 ou 1000 mégabits par seconde.	

7.

Le connecteur standard pour le câblage à paires torsadées non blindées est le connecteur RJ-45. Il s’agit d’un connecteur en plastique qui ressemble à un grand connecteur de type téléphone. RJ signifie Registered Jack, ce qui implique que le connecteur est conforme à une norme empruntée au secteur téléphonique. Cette norme désigne quel fil va avec chaque broche à l’intérieur du connecteur.