Examen 1 :

1) Quelle est la différence entre un routeur et un switch d'un point de vue utilité ?

Un routeur connecte et dirige le trafic entre différents réseaux, tandis qu'un switch connecte et dirige le trafic entre les dispositifs d'un même réseau local.

2) La passerelle par défaut (Default Gateway) n'est pas configuré au niveau du hôte : l'hôte ne connaît pas l'adresse IP de sa passerelle. Quelle sera la conséquence ?

Si la passerelle par défaut n'est pas configurée, l'hôte ne pourra pas communiquer avec des dispositifs situés en dehors de son réseau local.

3) ping www.google.fr : à quoi sert cette commande ?

La commande "ping www.google.fr" sert à vérifier la connectivité et la latence entre l'ordinateur exécutant la commande et le serveur de www.google.fr.

4) Un administrateur réseau est en train de configurer un switch. Dans quel fichier les commandes saisies sont-elles sauvegardées ? Que doit faire l'administrateur pour sauvegarder sa configuration de façon pérenne et ne pas tout perdre au redémarrage du switch ?

Les commandes saisies sont sauvegardées temporairement dans le fichier "running-config". L'administrateur doit utiliser la commande "copy running-config startup-config" pour sauvegarder la configuration de manière pérenne.

5) Sur combien de bits une adresse IPv6 est-elle codée ?

Une adresse IPv6 est codée sur 128 bits.

6) A quoi sert l'interface vlan 1 du switch ?

L'interface VLAN 1 du switch sert de VLAN par défaut pour la gestion et la configuration du switch.

7) Donner dans l'ordre les noms des 7 couches du modèle OSI

Les 7 couches du modèle OSI sont : 1) Couche physique, 2) Couche liaison de données, 3) Couche réseau, 4) Couche transport, 5) Couche session, 6) Couche présentation, 7) Couche application.

8) Donner un exemple d'adresse mac.

Exemple d'adresse MAC : 00-1A-22-3B-4C-5D.

9) Expliquer la complémentarité entre les adresses IP et les adresses mac d'un point de vue utilité.

Les adresses IP identifient les dispositifs au niveau du réseau, tandis que les adresses MAC identifient les dispositifs au niveau de la liaison de données. Les deux types d'adresses sont nécessaires pour acheminer correctement le trafic.

10) On vous donne un câble UTP. Comment faire pour vérifier rapidement si c'est un câble droit ou croisé ? Dans quel cas utiliser un câble droit et dans quel cas a-t-on besoin d'un câble croisé ? A quoi sert le câble console ?

Pour vérifier si un câble UTP est droit ou croisé, comparez les séquences de couleurs des fils aux deux extrémités du câble. Un câble droit a les mêmes séquences de couleurs aux deux extrémités. Utilisez un câble droit pour connecter des dispositifs différents (ordinateur à switch) et un câble croisé pour connecter des dispositifs similaires (switch à switch). Le câble console sert à établir une connexion directe entre un ordinateur et un dispositif réseau pour la configuration et la gestion.

11) Donner un avantage et un inconvénient de chacun de ses supports de transmission : câble UTP, fibre optique.

Câble UTP : Avantage - coût faible, Inconvénient - sensibilité aux interférences.
Fibre optique : Avantage - débit et distance élevés, Inconvénient - coût élevé.

12) Le champ adresse MAC destination d'un trame est égal à : 01-00-5E-00-00-C8. Que pouvez-vous en conclure concernant cette trame ?

L'adresse MAC de destination indique qu'il s'agit d'une trame multicast.

13) Définir et expliquer le protocole ARP

Le protocole ARP (Address Resolution Protocol) permet de résoudre les adresses IP en adresses MAC, facilitant la communication entre les dispositifs au niveau de la liaison de données.

14) A quoi sert la "Mac Address Table" au niveau du switch ?

La "Mac Address Table" au niveau du switch sert à associer les adresses MAC des dispositifs connectés aux ports du switch, permettant au switch de diriger efficacement le trafic vers les dispositifs appropriés.

15) Définir et expliquer le NAT

Le NAT (Network Address Translation) permet de traduire les adresses IP privées en adresses IP publiques (et vice versa) pour permettre aux dispositifs d'un réseau local d'accéder à Internet.

16) IPv6 présente un entête simplifié par rapport à IPv4. Certains champs comme ceux relatifs à la fragmentation ont été supprimés. Malgré cette simplification, l'entête IPv6 a une taille (en nombre de bits) deux fois plus grande que l'entête IPv4. Expliquer pourquoi

L'en-tête IPv6 est plus grand que l'en-tête IPv4 en raison de l'augmentation de la taille des adresses IP (128 bits contre 32 bits), malgré la simplification des autres champs de l'en-tête.

17) A quoi sert le champ Hop Limit dans IPv6 ? Il est équivalent à quel champs dans IPv4 ?

Le champ Hop Limit dans IPv6 sert à empêcher la circulation indéfinie des paquets sur le réseau en limitant le nombre de sauts (hops) qu'un paquet peut traverser. Ce champ est équivalent au champ Time To Live (TTL) dans IPv4

18) Voici les lignes d'une table de 3 lignes et 2 colonnes (les colonnes sont séparées par des ",") : Ligne 1 = Route, Next Hop or Exit Interface; Ligne 2 = 192.168.10.0 /24, G0/0/0; Ligne 3 : 209.165.200.224/30, G0/0/1. Expliquer la deuxième ligne de cette table

La deuxième ligne de cette table indique que pour atteindre le réseau 192.168.10.0/24, l'interface de sortie à utiliser est l'interface G0/0/0.

Examen 2 :

1. Quelle est la différence entre un hub et un switch d'un point de vue utilité ?

   Un hub transmet les paquets de données à tous les ports connectés, tandis qu'un switch transmet les paquets uniquement au port de destination approprié.

2. Qu'est-ce qu'un masque de sous-réseau ? Pourquoi est-il important ?

   Un masque de sous-réseau est utilisé pour diviser une adresse IP en deux parties : identifiant de réseau et identifiant d'hôte. Il permet de déterminer la taille et la structure d'un réseau.

3. traceroute www.google.fr : à quoi sert cette commande ?

   La commande "traceroute www.google.fr" affiche le chemin emprunté par les paquets entre l'ordinateur exécutant la commande et le serveur de www.google.fr.

4. Qu'est-ce que le mode de configuration globale dans un routeur ou un switch ? Comment y accéder ?

   Le mode de configuration globale permet de configurer des paramètres qui s'appliquent à l'ensemble du routeur ou du switch. Pour y accéder, entrez "configure terminal" ou "conf t" depuis le mode d'exécution privilégié.

5. Quelle est la différence entre une adresse IPv6 unicast et multicast ?

   Les adresses IPv6 unicast identifient un seul hôte, tandis que les adresses multicast identifient un groupe d'hôtes.

6. Qu'est-ce que le protocole STP (Spanning Tree Protocol) et à quoi sert-il ?

   Le protocole STP (Spanning Tree Protocol) empêche les boucles de commutation dans les réseaux en créant une topologie en arbre sans boucle.

7. Décrire brièvement le rôle de chaque couche du modèle TCP/IP.

   Modèle TCP/IP : 1) Couche Application - communication entre applications ; 2) Couche Transport - établissement et maintien des connexions ; 3) Couche Internet - routage des paquets ; 4) Couche Accès réseau - communication sur le support physique.

8. Donner un exemple d'adresse IP en version 4 et en version 6.

   Exemple d'adresse IPv4 : 192.168.1.1 ; Exemple d'adresse IPv6 : 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

9. Expliquer la différence entre les adresses IP publiques et privées.

   Les adresses IP publiques sont uniques et accessibles sur Internet, tandis que les adresses IP privées sont réservées à une utilisation au sein de réseaux locaux et ne sont pas routables sur Internet.

10. Qu'est-ce que la paire torsadée (Twisted Pair) ? Quelles sont les différences entre les catégories de câbles Ethernet ?

    La paire torsadée est un type de câble constitué de fils torsadés en paires. Les catégories de câbles Ethernet varient en termes de débit, de distance maximale et de blindage.

11. Donner un avantage et un inconvénient des réseaux sans fil par rapport aux réseaux câblés.

    Avantage des réseaux sans fil : mobilité et facilité d'installation ; Inconvénient : débit et portée inférieurs, plus vulnérables aux interférences.

12. Qu'est-ce qu'un VLAN ? Pourquoi est-il utilisé dans les réseaux d'entreprise ?

    Un VLAN (Virtual Local Area Network) permet de segmenter un réseau en sous-réseaux logiques, isolant ainsi le trafic et améliorant la sécurité et les performances.

13. Définir et expliquer le protocole DHCP.

    DHCP (Dynamic Host Configuration Protocol) attribue automatiquement des adresses IP et d'autres paramètres réseau aux hôtes.

14. A quoi sert le "Port Mirroring" au niveau du switch ?

    Le "Port Mirroring" au niveau du switch permet de copier le trafic d'un port ou d'un groupe de ports vers un autre port pour l'analyse et la surveillance.

15. Définir et expliquer le concept de tunneling.

    Le tunneling encapsule un protocole de réseau dans un autre protocole, permettant ainsi de transporter des données incompatibles ou de traverser des réseaux intermédiaires.

16. Pourquoi IPv6 a-t-il été développé en remplacement d'IPv4 ?

    IPv6 a été développé pour pallier la pénurie d'adresses IPv4, offrir une meilleure sécurité et améliorer les performances du routage.

17. Quelle est la différence entre le protocole ICMP et le protocole IGMP ?

    ICMP (Internet Control Message Protocol) est utilisé pour signaler des erreurs et échanger des informations sur l'état des réseaux et des hôtes, tandis que l'IGMP (Internet Group Management Protocol) est utilisé pour gérer la communication entre les membres d'un groupe multicast.

18. Voici les lignes d'une table de 3 lignes et 2 colonnes (les colonnes sont séparées par des ",") : Ligne 1 = Route, Next Hop or Exit Interface; Ligne 2 = 10.0.0.0/8, S0/0/0; Ligne 3 : 172.16.0.0/12, S0/0/1. Expliquer la troisième ligne de cette table.

    La troisième ligne de cette table indique que pour atteindre le réseau 172.16.0.0/12, le prochain saut ou l'interface de sortie à utiliser est l'interface S0/0/1.

Examen 3 :

1. Quelle est la différence entre un pont (bridge) et un répéteur (repeater) dans un réseau ?

   Solution : Un pont (bridge) fonctionne sur la couche 2 (liaison de données) du modèle OSI et relie deux réseaux en filtrant et transmettant les trames. Un répéteur (repeater) fonctionne sur la couche 1 (physique) et amplifie les signaux électriques ou optiques pour étendre la portée d'un réseau.

2. Qu'est-ce que le masque de sous-réseau ? Pourquoi est-il utilisé ?

   Solution : Le masque de sous-réseau est un nombre binaire qui permet de séparer l'adresse IP en deux parties : l'identifiant réseau et l'identifiant hôte. Il est utilisé pour déterminer si deux adresses IP appartiennent au même réseau et pour diviser un réseau en sous-réseaux.

3. Qu'est-ce que DHCP et quel est son rôle dans un réseau ?

   Solution : DHCP (Dynamic Host Configuration Protocol) est un protocole qui attribue automatiquement des adresses IP et d'autres paramètres de configuration réseau aux dispositifs clients.

4. Quelle est la différence entre TCP et UDP ?

   Solution : TCP (Transmission Control Protocol) est un protocole orienté connexion qui fournit une communication fiable et garantit la livraison des données. UDP (User Datagram Protocol) est un protocole sans connexion qui fournit une communication rapide mais sans garantie de livraison.

5. Qu'est-ce qu'un pare-feu (firewall) et quelle est son utilité dans un réseau ?

   Solution : Un pare-feu est un dispositif ou un logiciel qui contrôle et filtre le trafic entrant et sortant d'un réseau en fonction de règles de sécurité prédéfinies. Il protège le réseau contre les menaces extérieures et les intrusions.

6. Qu'est-ce que le protocole STP et pourquoi est-il utilisé dans les réseaux Ethernet ?

Solution : Le protocole STP (Spanning Tree Protocol) est un protocole de la couche 2 qui prévient les boucles de commutation dans les réseaux Ethernet en désactivant les liens redondants et en créant une topologie en arbre.

7. Qu'est-ce que QoS (Quality of Service) et pourquoi est-il important dans les réseaux ?

Solution : QoS (Quality of Service) est un ensemble de techniques visant à garantir une qualité de service pour les applications critiques en priorisant le trafic et en gérant la bande passante. Il est important pour assurer la performance et la fiabilité des services sensibles à la latence, tels que la VoIP et le streaming vidéo.

8. Qu'est-ce qu'un réseau VPN (Virtual Private Network) et quel est son objectif ?

Solution : Un VPN (Virtual Private Network) est un réseau privé virtuel qui permet d'établir des connexions sécurisées et chiffrées entre les dispositifs et les réseaux distants sur Internet. Son objectif est de protéger la confidentialité et l'intégrité des données lors de leur transmission.

9. Qu'est-ce qu'une topologie en étoile et quels sont ses avantages et inconvénients ?

Solution : Une topologie en étoile est une topologie de réseau dans laquelle tous les nœuds sont connectés à un nœud central (hub, switch ou routeur). Avantages : facilité de gestion et de dépannage, meilleure performance car les transmissions sont isolées. Inconvénients : dépendance du nœud central, besoin de câblage supplémentaire.

10. Qu'est-ce qu'un serveur DNS et quel est son rôle dans un réseau ?

Solution : Un serveur DNS (Domain Name System) est un serveur qui traduit les noms de domaine en adresses IP, facilitant ainsi l'accès aux ressources sur Internet. Son rôle est de résoudre les noms de domaine en adresses IP pour permettre la communication entre les dispositifs sur le réseau.

11. Quelle est la différence entre un réseau LAN, MAN et WAN ?

Solution : LAN (Local Area Network) est un réseau local couvrant une zone géographique limitée, comme un bureau ou un bâtiment. MAN (Metropolitan Area Network) est un réseau de taille moyenne qui s'étend sur une ville ou une région métropolitaine. WAN (Wide Area Network) est un réseau de grande

envergure qui couvre une vaste zone géographique, telle qu'un pays ou un continent.

12. Qu'est-ce que le protocole SNMP et à quoi sert-il ?

    Solution : SNMP (Simple Network Management Protocol) est un protocole de gestion de réseau qui permet de surveiller et de contrôler les dispositifs réseau à distance. Il est utilisé pour collecter des informations sur les dispositifs réseau, les configurer et les contrôler.

13. Quelle est la différence entre une adresse IP publique et une adresse IP privée ?

    Solution : Les adresses IP publiques sont uniques et routables sur Internet, elles sont attribuées par les registres Internet régionaux (RIR) et utilisées pour communiquer avec des dispositifs en dehors du réseau local. Les adresses IP privées ne sont pas routables sur Internet et sont utilisées pour les communications au sein d'un réseau local.

14. Qu'est-ce que le multicast et comment est-il utilisé dans les réseaux ?

    Solution : Le multicast est une méthode de communication qui permet d'envoyer des données à un groupe d'abonnés simultanément, plutôt qu'à un seul destinataire. Il est utilisé pour économiser la bande passante et réduire la charge sur les serveurs en évitant la duplication de trafic.

15. Qu'est-ce qu'un proxy et à quoi sert-il dans un réseau ?

    Solution : Un proxy est un serveur qui agit comme intermédiaire entre un client et un serveur cible, traitant les requêtes et les réponses en leur nom. Il peut être utilisé pour améliorer la sécurité, la confidentialité, la performance, et pour contourner les restrictions d'accès aux ressources.

16. Quelle est la différence entre un VLAN et un subnet ?

    Solution : Un VLAN (Virtual Local Area Network) est un réseau logique créé en segmentant un réseau physique en plusieurs réseaux indépendants à la couche 2 (liaison de données). Un subnet (sous-réseau) est une division logique d'un réseau IP à la couche 3 (réseau) pour simplifier la gestion et améliorer la performance.

17. Qu'est-ce que le protocole DHCP et quel est son rôle dans un réseau ?

    Solution : DHCP (Dynamic Host Configuration Protocol) est un protocole qui attribue automatiquement des adresses IP et d'autres paramètres réseau aux dispositifs clients. Son rôle est de simplifier la gestion des adresses IP et de minimiser les conflits d'adresses
    .

18. Qu'est-ce que le masque de sous-réseau et comment est-il utilisé pour diviser un réseau en sous-réseaux ?

    Solution : Le masque de sous-réseau est un nombre binaire utilisé pour séparer l'adresse IP d'un hôte en deux parties : l'identifiant de réseau et l'identifiant d'hôte. Il est utilisé pour diviser un réseau en sous-réseaux en déterminant la taille et le nombre de sous-réseaux possibles.

19. Qu'est-ce qu'un pare-feu et quel est son rôle dans la sécurité d'un réseau ?

    Solution : Un pare-feu est un dispositif de sécurité réseau qui surveille et contrôle le trafic entrant et sortant en fonction de règles prédéfinies. Son rôle est de protéger les ressources du réseau contre les menaces externes et internes en bloquant ou en autorisant le trafic selon les règles établies.

20. Qu'est-ce que le protocole HTTPS et comment améliore-t-il la sécurité des communications sur Internet ?

    Solution : HTTPS (Hypertext Transfer Protocol Secure) est une version sécurisée du protocole HTTP qui utilise le protocole SSL/TLS pour crypter les communications entre le client et le serveur. Il améliore la sécurité en garantissant la confidentialité, l'intégrité et l'authentification des communications sur Internet.