

1. Quel est la meilleure catégorie de câble RJ45 ?

- La catégorie 8 jusqu'à 40 G.

2. Combien de bits faut-il pour résoudre l'adresse IP ?

- Pour une adresse IPv4, il faut 32 bits.
- Pour une adresse IPv6, il faut 128 bits

3. Quelle est la différence entre un câble perte-torsadé droit ou un câble perte-torsadé croisé ?

- C'est le câble, l'entrée et la sortie, dans le droit, à la même configuration, donc l'ordre des couleurs est la même, alors que le croisé est inversé.
- Le droit, c'est pour la communication internet, et le croisé, c'est pour la communication inter-machine.

4. Quelle différence entre topologie physique ou logique ?

- Physique : Indique comment les différentes stations sont raccordées physiquement.
- Logique : Définit comment distribuer le droit à la parole.

5. Que fait la commande ping ?

- Elle affiche le chemin que les paquets empruntent.
- Teste l'accessibilité d'une autre machine à travers un réseau IP.

6. Que signifie l'acronyme DNS ?

- Domain Name System.

7. Que veut dire ISO ?

- International Standard Organization.

8. Combien y a-t-il de types de topologie réseaux ?

- 5.

9. Quelles sont les 8 couleurs des fils constituant un câble pair torsadé ?

- Vert, vert/blanc, bleu, bleu/blanc, brun, brun/blanc, rouge, rouge/blanc.

10. Quel est le rôle du routeur ?

- Un routeur relie différents réseaux et dirige le trafic.

11. Quel est le rôle d'un masque de sous-réseaux ?

- Détermine quelle partie d'une adresse IP appartient au réseau et au hôte.

12. Combien y a-t-il de couches dans le modèle OSI ?

- 7.

13. Quelle est la 3ème couche du modèle OSI ?

- Réseau.

14. Quelle est la différence entre un hub et un switch ?

- Le concentrateur (hub) est moins sécurisé que le commutateur (switch).
- Le commutateur n'intervient pas à la même couche OSI.

15. À quoi sert le port mirroring ?

- Vous prenez un port et vous le dirigez sur un autre port.

16. Quelle est l'importance de la redondance dans l'infrastructure réseau ?

- La redondance permet d'assurer la disponibilité et le contenu du réseau en cas de défaillance matérielle.

17. Qu'est-ce qu'un serveur DHCP et comment fonctionne-t-il dans un réseau ?

- Un serveur DHCP est un dispositif dans un réseau qui permet d'attribuer des adresses IP aux appareils pour les identifier sur le réseau.

18. Que signifie CIDR ?

- Classless Inter-Domain Routing.

19. Expliquez le processus de conversion binaire.

- Il faut convertir le nombre en multipliant par des puissances de 2 et en additionnant les valeurs.

20. Deux protocoles qui permettent de sécuriser une communication ?

- SSL (Secure Sockets Layer) et TLS (Transport Layer Security).

21. Quels sont les avantages de l'utilisation de VLAN dans un réseau ?

- Les VLANs (Virtual Local Area Networks) permettent de segmenter un réseau physique en plusieurs réseaux logiques. Cela améliore la sécurité, la gestion du trafic et la performance globale du réseau en isolant le trafic entre les différentes parties du réseau.

22. Qu'est-ce qu'une adresse MAC et à quoi sert-elle ?

- Une adresse MAC (Media Access Control) est une adresse unique attribuée à chaque interface réseau pour la communication au niveau des couches de liaison de données (couche 2) dans le modèle OSI. Elle sert à identifier de manière unique un appareil sur un réseau local (LAN).

23. Quelle est la différence entre TCP et UDP ?

- TCP (Transmission Control Protocol) est un protocole de transport orienté connexion qui garantit la livraison des paquets dans l'ordre. UDP (User Datagram Protocol) est un protocole de transport sans connexion qui ne garantit pas la livraison ni l'ordre des paquets, mais qui est plus rapide et efficace pour les applications qui peuvent tolérer la perte de paquets (comme la diffusion vidéo en direct).

24. Qu'est-ce qu'un pare-feu (firewall) et pourquoi est-il important ?

- Un pare-feu est un dispositif de sécurité réseau qui surveille et contrôle le trafic réseau entrant et sortant en fonction de règles de sécurité prédéfinies. Il est important pour protéger le réseau contre les accès non autorisés, les attaques malveillantes et les fuites de données.

25. Quelle est la fonction du DNS (Domain Name System) dans un réseau ?

- Le DNS (Domain Name System) traduit les noms de domaine lisibles par l'homme (comme www.example.com) en adresses IP lisibles par les machines (comme 192.0.2.1). Cela permet aux utilisateurs d'accéder aux sites web en utilisant des noms de domaine faciles à retenir plutôt que des adresses IP numériques.

26. Qu'est-ce qu'un VPN (Virtual Private Network) et comment fonctionne-t-il ?

- Un VPN (Virtual Private Network) est une technologie qui crée une connexion sécurisée et cryptée sur un réseau moins sécurisé, comme Internet. Il permet aux utilisateurs de transmettre des données de manière sécurisée et privée en masquant leur adresse IP et en chiffrant tout le trafic entre leur appareil et le serveur VPN.

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

- Une adresse IP publique est une adresse unique attribuée à un appareil sur Internet, accessible depuis n'importe quel endroit dans le monde. Une adresse IP privée est utilisée au sein d'un réseau local (LAN) et n'est pas routable sur Internet. Les adresses IP privées sont définies par les plages spécifiées dans les normes RFC 1918.

28. Qu'est-ce qu'une passerelle par défaut (default gateway) ?

- Une passerelle par défaut est un routeur ou un dispositif de réseau qui sert de point de passage vers d'autres réseaux lorsque l'appareil ne connaît pas la route exacte pour atteindre une destination spécifique. Elle permet aux appareils d'un réseau local de communiquer avec des appareils sur d'autres réseaux, y compris Internet.

29. Comment fonctionne le protocole ARP (Address Resolution Protocol) ?

- ARP (Address Resolution Protocol) est utilisé pour mapper une adresse IP (niveau réseau) à une adresse MAC (niveau liaison de données) sur un réseau local. Lorsqu'un appareil veut communiquer avec un autre appareil sur le même réseau, il utilise ARP pour trouver l'adresse MAC correspondante à l'adresse IP.

30. Qu'est-ce qu'un serveur proxy et à quoi sert-il ?

- Un serveur proxy agit comme un intermédiaire pour les requêtes des clients cherchant des ressources sur d'autres serveurs. Il permet de masquer l'adresse IP du client, de filtrer les requêtes pour des raisons de sécurité ou de performance, et de mettre en cache les contenus pour améliorer la vitesse d'accès.