JOB 2

Qu’est-ce qu’un réseau ?

Un réseau est un ensemble de dispositifs interconnectés qui communiquent entre eux pour partager des ressources, des informations ou des services. Ces dispositifs peuvent être des ordinateurs, des serveurs, des routeurs, des commutateurs, des imprimantes, des téléphones, des objets connectés et d'autres appareils compatibles avec les communications en réseau.

À quoi sert un réseau informatique ?

Un réseau informatique sert à faciliter la communication et le partage de ressources entre des dispositifs informatiques interconnectés.
-Partage de ressources
-Communication
-Accès à distance
-Partage de fichiers
-Sauvegarde des données

Quel matériel avons-nous besoin pour construire un réseau ? Détaillez les fonctions de chaque pièce.

Pour construire un réseau informatique, nous avons besoin de divers composants matériels.
Dispositifs actifs:
-Routeurs
-Commutateurs
-Points d'accès Wi-Fi
-Firewalls
Dispositif passifs:
-Câbles
-Connecteurs
-Panneaux de brassage
-Prises murales
Dispositifs de stockage:
-Systèmes de stockage en réseau
Dispositifs d'accès:
-Ordinateurs et périphériques
-Câblage structuré
-Alimentation électrique
-Équipement de refroidissement
-Contrôle d'accès et sécurité

-Gestion de réseau

JOB 4

Qu’est-ce qu’une adresse IP ?

Une adresse IP (Internet Protocol address) est un identifiant numérique attribué à chaque appareil connecté à un réseau informatique qui utilise le protocole Internet pour la communication.
-IPv4 (Internet Protocol version 4)
-IPv6 (Internet Protocol version 6)

À quoi sert un IP ?

Une adresse IP (Internet Protocol) sert principalement à deux fins principales dans le contexte des réseaux informatiques :
-Identification des dispositifs
-Routage des données

Qu’est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control) est un identifiant unique attribué à chaque carte réseau, que ce soit une carte réseau filaire (Ethernet) ou sans fil (Wi-Fi) d'un dispositif informatique. Contrairement aux adresses IP, qui sont utilisées pour identifier des dispositifs sur un réseau IP, les adresses MAC sont spécifiques à la couche de liaison de données du modèle OSI et sont utilisées pour identifier de manière unique une carte réseau sur un réseau local (LAN).

Qu’est-ce qu’une IP publique et privée ?

Les adresses IP publiques et privées sont deux types d'adresses IP utilisées dans le cadre de la communication en réseau. Elles servent à différencier les dispositifs sur un réseau local (LAN) d'un réseau étendu (WAN) comme Internet. Voici une explication de chacun de ces types d'adresses :
-Adresse IP publique :

- Une adresse IP publique est une adresse qui est routable sur Internet. Cela signifie qu'elle peut être utilisée pour communiquer directement avec des dispositifs sur Internet et est accessible depuis n'importe quel endroit sur le réseau mondial.
- Les adresses IP publiques sont attribuées par les autorités de régulation d'Internet, telles que l'IANA (Internet Assigned Numbers Authority), aux fournisseurs de services Internet (FSI) et aux organisations qui ont besoin d'une connectivité Internet.
- Chaque dispositif connecté à Internet, qu'il s'agisse d'un serveur, d'un ordinateur personnel ou d'un routeur, possède une adresse IP publique unique qui le distingue sur le réseau mondial.

-Adresse IP privée :

- Une adresse IP privée est utilisée au sein d'un réseau local (LAN) pour identifier les dispositifs connectés à ce réseau. Les adresses IP privées ne sont pas routables sur Internet, ce qui signifie qu'elles ne sont pas accessibles directement depuis l'extérieur du réseau local.
- Les adresses IP privées sont généralement utilisées pour gérer les dispositifs au sein du réseau local, tels que les ordinateurs, les imprimantes, les téléphones, les caméras de sécurité, etc.
- Il existe des plages d'adresses IP privées réservées à cet usage, notamment celles définies par les spécifications RFC 1918 pour IPv4.
- Les adresses IP privées ne sont pas uniques à l'échelle mondiale et peuvent être utilisées de manière répétée dans de nombreux réseaux locaux distincts.

Quelle est l'adresse de ce réseau ?

JOB5
Vérifions l'adresse IP
PIERRE

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::260:2FFF:FEB0:13D3
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```

ALICIA

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20A:F3FF:FE5A:DEAB
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```

Quelle ligne de commande avez-vous utilisée pour vérifier l'id des machines ?

`'ipconfig /all'`

JOB6

PIEERE

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=6ms TTL=128
Reply from 192.168.1.1: bytes=32 time=6ms TTL=128
Reply from 192.168.1.1: bytes=32 time=20ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 20ms, Average = 8ms
```

ALCIA

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=16ms TTL=128
Reply from 192.168.1.2: bytes=32 time=14ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 7ms
```

Quelle est la commande permettant de Ping entre des PC ?

ping adress_IP_destination

JOB7

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ? NON
Expliquez pourquoi.
Parce que le PC de pierre est éteint
JOB8

Quelle est la différence entre un hub et un switch ?
Un hub et un switch sont deux types de dispositifs de réseau utilisés pour connecter plusieurs appareils dans un réseau local (LAN - Local Area Network). Ils jouent des rôles similaires en termes de distribution de données, mais il existe des différences significatives dans leur fonctionnement et leurs performances. Voici les principales différences entre un hub et un switch :
-Méthode de transmission des données :

- Hub : Un hub fonctionne au niveau de la couche physique du modèle OSI. Il diffuse les données à tous les ports, quel que soit le destinataire. Cela signifie que lorsque des données sont envoyées à un port, le hub les transmet à tous les autres ports, créant ainsi du trafic inutile.
- Switch : Un switch opère au niveau de la couche liaison de données du modèle OSI. Il maintient une table de correspondance (table MAC) qui enregistre les adresses MAC des appareils connectés à ses ports. Lorsqu'il reçoit des données, le switch les transmet uniquement au port du destinataire, minimisant ainsi le trafic inutile.

-Efficacité et performance :

- Hub : En raison de sa méthode de diffusion, un hub génère davantage de collision et de trafic superflu, ce qui limite les performances du réseau. Les réseaux utilisant des hubs sont généralement plus lents et moins efficaces.
- Switch : Les switches sont beaucoup plus efficaces car ils acheminent intelligemment les données uniquement vers les destinataires appropriés, réduisant ainsi les collisions et améliorant les performances du réseau.

-Sécurité :

- Hub : En raison de sa diffusion à tous les ports, un hub n'offre pas de sécurité intrinsèque. Toutes les données sont accessibles à tous les appareils connectés au hub.

- Switch : Les switches offrent une certaine isolation des données, car ils ne transmettent les données qu'aux destinataires appropriés. Cela offre une certaine sécurité de base dans un réseau local.

-Coût :

- Hub : Les hubs sont généralement moins chers que les switches en raison de leur simplicité et de leurs fonctionnalités limitées.
- Switch : Les switches sont plus coûteux, mais ils offrent des performances et une gestion de réseau supérieures.

Comment fonctionne un hub et quels sont ses avantages et ses inconvénients ?

Un hub est un dispositif de réseau qui opère au niveau de la couche physique (couche 1) du modèle OSI. Son fonctionnement est relativement simple, mais il présente des avantages et des inconvénients. Voici comment fonctionne un hub, ainsi que ses avantages et inconvénients :

Avantages d'un hub :

- Simplicité : Les hubs sont simples et faciles à configurer. Il n'y a généralement pas besoin de paramètres complexes.
- Coût : Les hubs sont moins chers que les switches, ce qui les rend abordables pour les petits réseaux ou dans des situations où la performance n'est pas critique.
- Utilisation de base : Dans certaines situations, où le trafic réseau est limité et où la sécurité n'est pas une préoccupation majeure, un hub peut suffire.

Inconvénients d'un hub :

- Performance : En diffusant les données à tous les ports, les hubs génèrent beaucoup de trafic inutile et de collisions. Cela peut entraîner une baisse significative des performances du réseau, en particulier lorsque de nombreux appareils sont connectés.
- Sécurité : Les hubs ne fournissent pas de sécurité intrinsèque, car toutes les données sont accessibles à tous les appareils connectés. Cela peut être un problème dans les réseaux où la confidentialité est importante.
- Gestion : Les hubs offrent peu ou pas de capacités de gestion. Vous ne pouvez pas segmenter le réseau ou optimiser la distribution du trafic.
Obsolescence : Les hubs sont devenus obsolètes dans la plupart des environnements réseau modernes en raison de leurs limitations en matière de performance et de sécurité.

Quels sont les avantages et inconvénients d’un switch ?

Un switch est un dispositif de réseau qui opère à la couche liaison de données (couche 2) du modèle OSI. Il offre des fonctionnalités plus avancées par rapport à un hub, ce qui présente à la fois des avantages et des inconvénients. Voici les principaux avantages et inconvénients d'un switch :

Avantages d'un switch :

- Performance : Les switches sont conçus pour acheminer intelligemment le trafic réseau. Ils transmettent les données uniquement au port du destinataire, ce qui réduit les collisions et améliore les performances du réseau.
- Efficacité : En réduisant le trafic inutile, les switches optimisent l'utilisation de la bande passante, ce qui permet d'obtenir des débits plus élevés et une latence réduite.
- Sécurité : Les switches créent une isolation des données en transmettant les données uniquement aux destinataires appropriés, améliorant ainsi la sécurité du réseau. Les données ne sont pas diffusées à tous les ports.
– Gestion : Les switches offrent des fonctionnalités de gestion avancées, telles que la surveillance du trafic, la configuration de VLAN (Virtual Local Area Network), la qualité de service (QoS) et la gestion des adresses MAC.
- Évolutivité : Les switches sont évolutifs, ce qui signifie que vous pouvez ajouter de nouveaux ports ou même connecter plusieurs switches pour étendre un réseau.

Inconvénients d'un switch :

- Coût : Les switches sont généralement plus chers que les hubs en raison de leurs fonctionnalités avancées. Le coût peut être un facteur limitant pour les petits réseaux.
- Complexité : La configuration et la gestion des switches peuvent être plus complexes que celles des hubs. Une certaine expertise est nécessaire pour optimiser leur utilisation.
- Besoin d'adresses MAC uniques : Pour fonctionner efficacement, les switches nécessitent que chaque appareil connecté ait une adresse MAC unique. Cela peut nécessiter une gestion des adresses MAC dans des environnements où les appareils ne sont pas tous gérés de manière centralisée.
- Dépendance à l'électricité : Contrairement à certains hubs passifs, les switches actifs dépendent de l'alimentation électrique. En cas de panne de courant, le réseau peut devenir indisponible.

Comment un switch gère-t-il le trafic réseau ?

Un switch gère le trafic réseau de manière efficace et intelligente en utilisant des informations contenues dans les trames réseau et en se basant sur des tables de correspondance pour diriger ces trames vers les ports de destination appropriés. Voici comment un switch gère le trafic réseau :

- Apprentissage des adresses MAC
- Filtrage des trames
- Mise à jour de la table MAC
- Gestion de la diffusion (broadcast)
- Gestion des trames inconnues