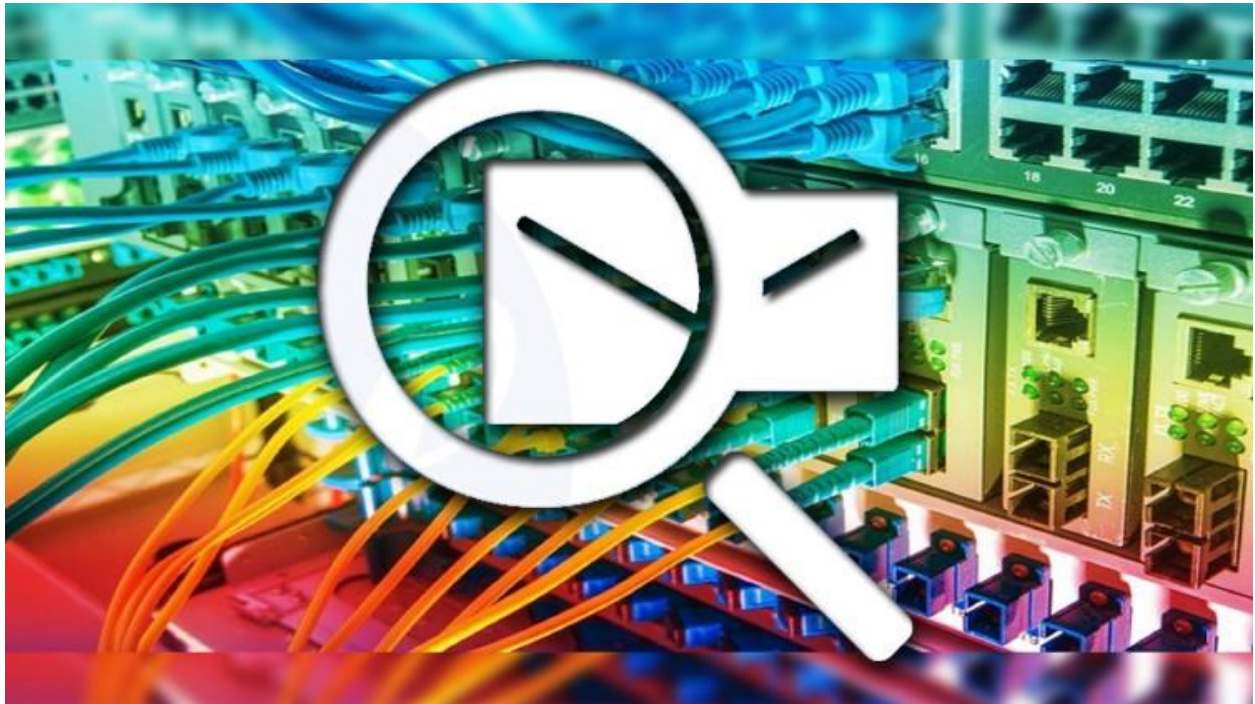


Rapport sur Cisco packet tracer



Ikhlef Mathis

20/08/2002

JOB 1 :

Téléchargement de cisco packet tracer

Présentation de Cisco Packet Tracer 8.0



Job 2 :

Travail 02 :

→ Qu'est-ce qu'un réseau ?

Un réseau informatique est un groupe d'appareils reliés entre eux pour échanger des informations. Par analogie avec un réseau, on appelle un nœud la fin d'une connexion, qui peut être l'intersection de plusieurs connexions ou appareils.

→ A quoi sert un réseau informatique ?

Un réseau informatique fait référence à des appareils informatiques interconnectés qui peuvent échanger des données et partager des ressources entre eux. Ces appareils en réseau utilisent un système de règles appelés protocoles de communication pour transmettre des informations via une technologie physique ou sans fil.

→ Quel matériel est nécessaire pour construire un réseau ? décrivez-les en détail fonction de chaque pièce.

Voici une liste des périphériques réseau les plus courants :

* Concentrateur (hub)

Contrairement aux commutateurs, les hubs ne sont pas intelligents et n'effectuent pas de commutation de paquets. Au lieu de cela, ils répètent simplement le signal reçu sur tous les ports. Cela signifie que tout signal entrant dans un port sera copié sur tous les autres ports du hub. Cela permet aux données d'être transférées vers tous les appareils connectés.

*Transformation

Contrairement aux hubs, les commutateurs effectuent une commutation intelligente des paquets. Ils analysent les trames entrantes, extraient l'adresse MAC de destination, puis acheminent ces trames uniquement vers les ports connectés au périphérique de destination, minimisant ainsi les conflits de trafic et optimisant les performances du réseau.

* routeur.

Un routeur est un appareil utilisé pour connecter différents réseaux (par exemple, un réseau local à Internet). Ils prennent en charge la communication entre les réseaux à l'aide d'adresses IP et prennent des décisions de routage pour acheminer le trafic.

* pont

Un pont est un périphérique réseau conçu pour interconnecter deux segments de réseau local (LAN) pour former un seul réseau logique. Les ponts sont utilisés pour diverses raisons et remplissent des fonctions spécifiques

*Passerelle

Une passerelle est un élément clé de l'infrastructure réseau car elle facilite la communication et l'interopérabilité entre différents réseaux ou systèmes. Il joue un rôle essentiel dans la connexion de l'ensemble de l'infrastructure informatique, en permettant aux données de circuler entre différents environnements et en fournissant les moyens de surmonter les différences de protocoles et de formats de données.

modem:

Un modem fait deux choses principales lors de la modulation : la modulation et la démodulation. Il convertit les signaux numériques en signaux analogiques pour les transmettre sur des réseaux de communications analogiques, tels que des lignes téléphoniques traditionnelles ou des câbles coaxiaux.

Lorsqu'il démodule, il fait le contraire, convertissant le signal analogique reçu en un signal numérique que les ordinateurs et autres appareils numériques peuvent comprendre.

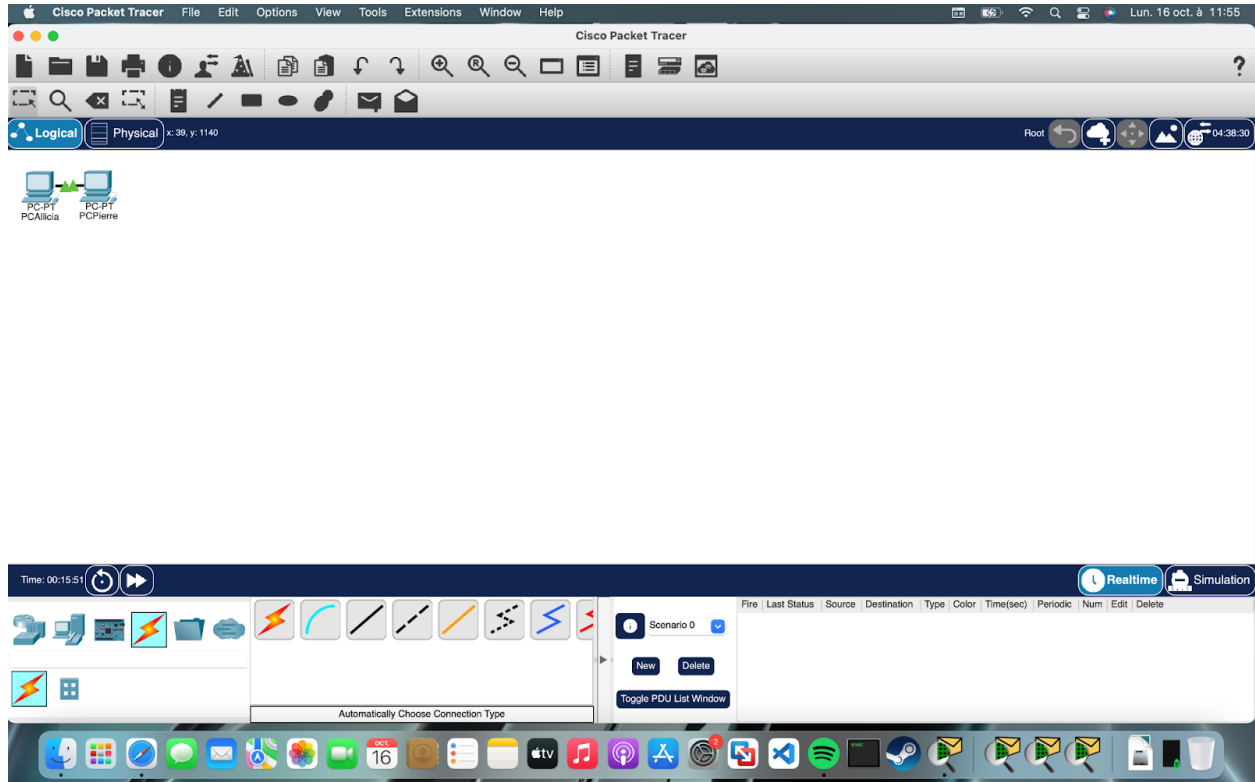
Répétiteur:

Un répéteur, parfois appelé amplificateur ou prolongateur, est un périphérique réseau conçu pour étendre la portée d'un réseau sans fil (Wi-Fi) en amplifiant et en rediffusant les signaux sans fil. Son objectif principal est d'améliorer la couverture et la qualité du signal Wi-Fi dans les zones où le signal d'origine est faible ou instable.

Point d'accès:

Un point d'accès (souvent abrégé en AP) est un périphérique réseau qui permet à des appareils sans fil tels que des ordinateurs, des smartphones et des tablettes de se connecter à un réseau local (LAN) via une connexion sans fil Wi-Fi. Les points d'accès agissent comme des passerelles entre les appareils sans fil et les réseaux filaires ou filaires existants.

Job 3:



→ Comme vous avez pu le constater, il existe des câbles croisés, droits...

Quels

câbles avez-vous choisis pour relier les deux ordinateurs ? Expliquez votre choix.

J'ai choisis le premier cable nommé "Automatically Choose Connexion Type" pour une connexion directe.

Job 04:

Maintenant que votre premier réseau est en place, configurez PC Pierre et PC Alicia comme suit :

- PC Pierre :

- Adresse IP : 192.168.1.1

- Masque de sous-réseau : 255.255.255.0

- PC Alicia :

- Adresse IP : 192.168.1.2

- Masque de sous-réseau : 255.255.255.0

PCallicia

PhysicalConfigDesktopProgrammingAttributes

IP Configuration

X

InterfaceFastEthernet0

IP Configuration

DHCP

Static

IPv4 Address

192.168.1.2

Subnet Mask

255.255.255.0

Default Gateway

0.0.0.0

DNS Server

0.0.0.0

IPv6 Configuration

Automatic

Static

IPv6 Address

/

Link Local Address

FE80::201:C9FF:FE97:832C

Default Gateway

DNS Server

802.1X

Use 802.1X Security

Authentication

MD5

Username

Password

Top

PCpierre

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface FastEthernet0 [v]

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::201:C9FF:FE27:7B9A

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5 [v]

Username

Password

☐ Top

Afin de rendre plus lisible votre schéma, ajoutez en dessous de vos PC son

adresse IP.

→ Qu'est-ce qu'une adresse IP ?

Une adresse IP (Internet Protocol) est un numéro unique attribué à chaque appareil connecté à un réseau informatique qui utilise le protocole Internet pour la communication. Les adresses IP sont essentielles pour l'acheminement des données sur Internet et sur d'autres réseaux, car elles permettent d'identifier de manière unique chaque appareil. Une adresse IP est généralement sous la forme de chiffres et de points

→ À quoi sert un IP ?

les adresses IP sont l'un des piliers fondamentaux de la communication et de la connectivité dans les réseaux informatiques, notamment sur Internet. Elles jouent un rôle central dans l'identification des appareils, le routage des données, la configuration réseau, la sécurité et l'interopérabilité, ce qui en fait un élément clé de l'infrastructure de communication moderne.

→ Qu'est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control), également connue sous le nom d'adresse matérielle, est un identifiant unique attribué à chaque carte réseau ou adaptateur réseau sur un appareil, tel qu'un ordinateur, un smartphone, une imprimante ou d'autres périphériques réseau. Contrairement à une adresse IP, qui est utilisée pour identifier un appareil sur un réseau IP, une adresse MAC identifie de manière unique le matériel du périphérique lui-même au niveau de la couche de liaison de données (couche 2) du modèle OSI.

→ Qu'est-ce qu'une IP publique et privée ?

les adresses IP publiques sont utilisées pour l'identification sur Internet, tandis que les adresses IP privées sont utilisées pour l'identification au sein d'un réseau local. Les routeurs sont responsables de la gestion de ces deux types d'adresses pour permettre la connectivité entre le réseau local et Internet.

→ Quelle est l'adresse de ce réseau ?

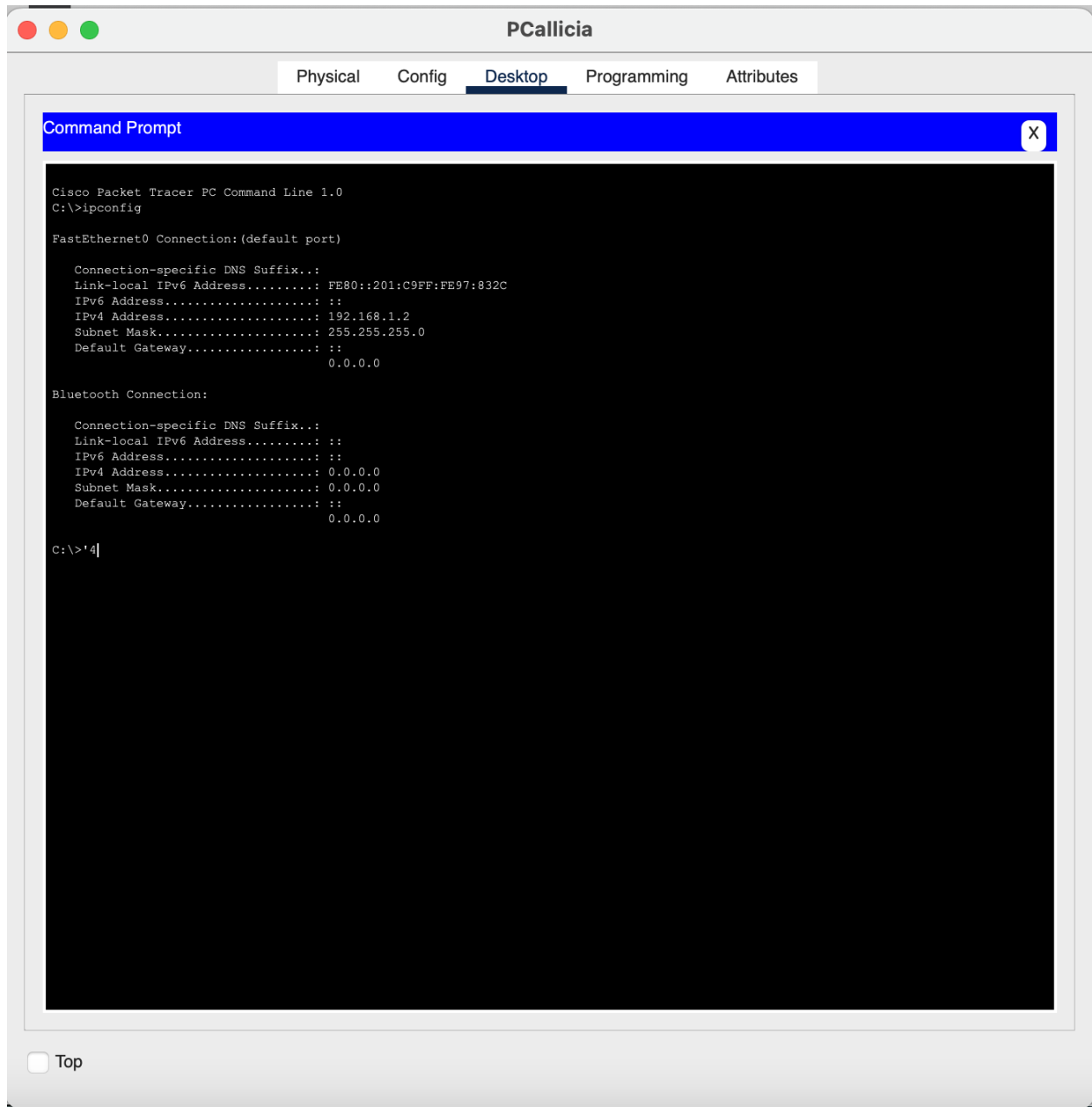
255.255.255.0

Job 05:

À l'aide du terminal, vérifier que l'IP du PC Pierre est correcte. Faites une capture d'écran et ajoutez l'image à votre documentation. Répétez les mêmes étapes avec le PC Alicia.

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

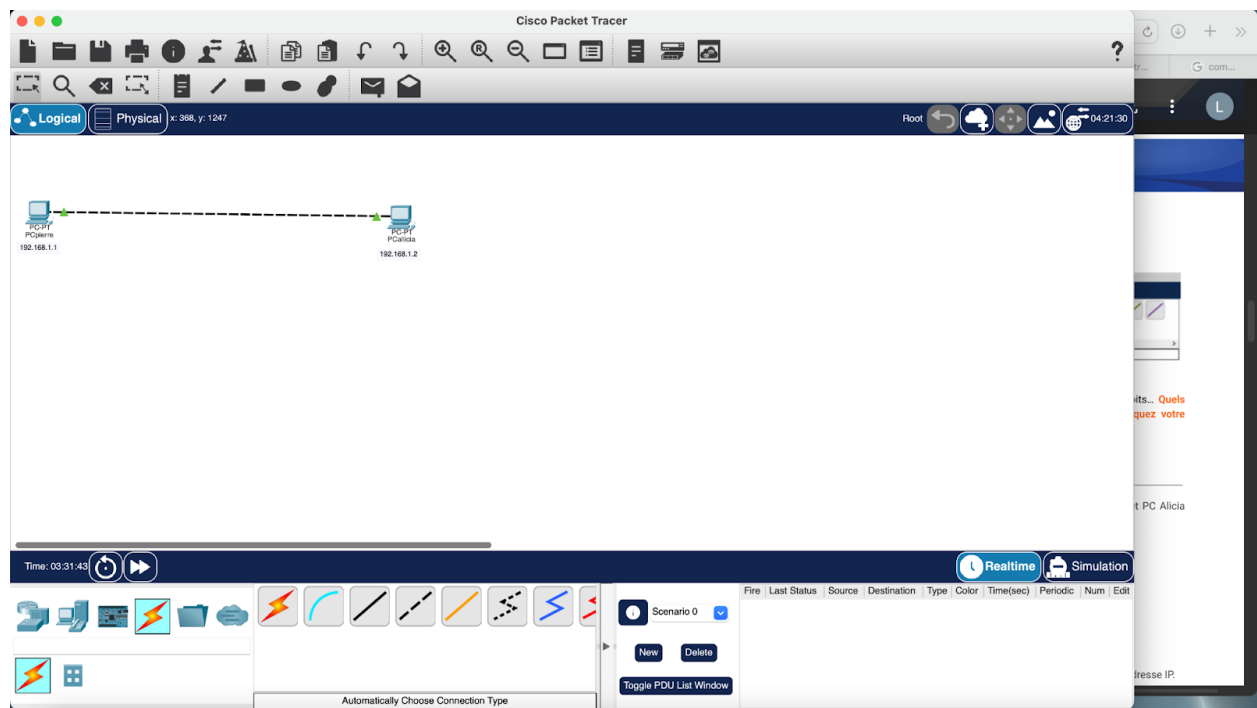
La ligne de commande utilisée pour ce job était la commande : ipconfig

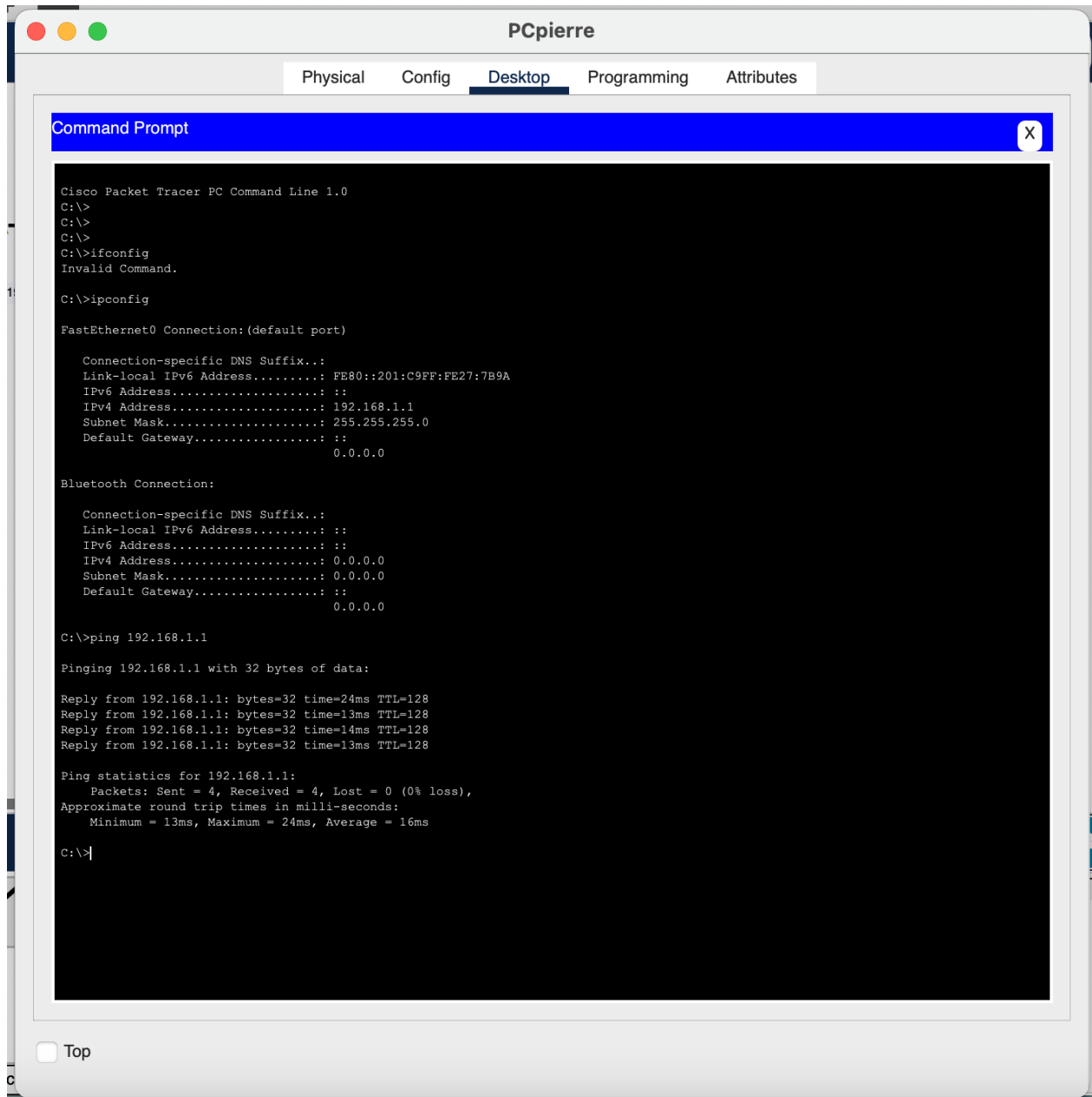


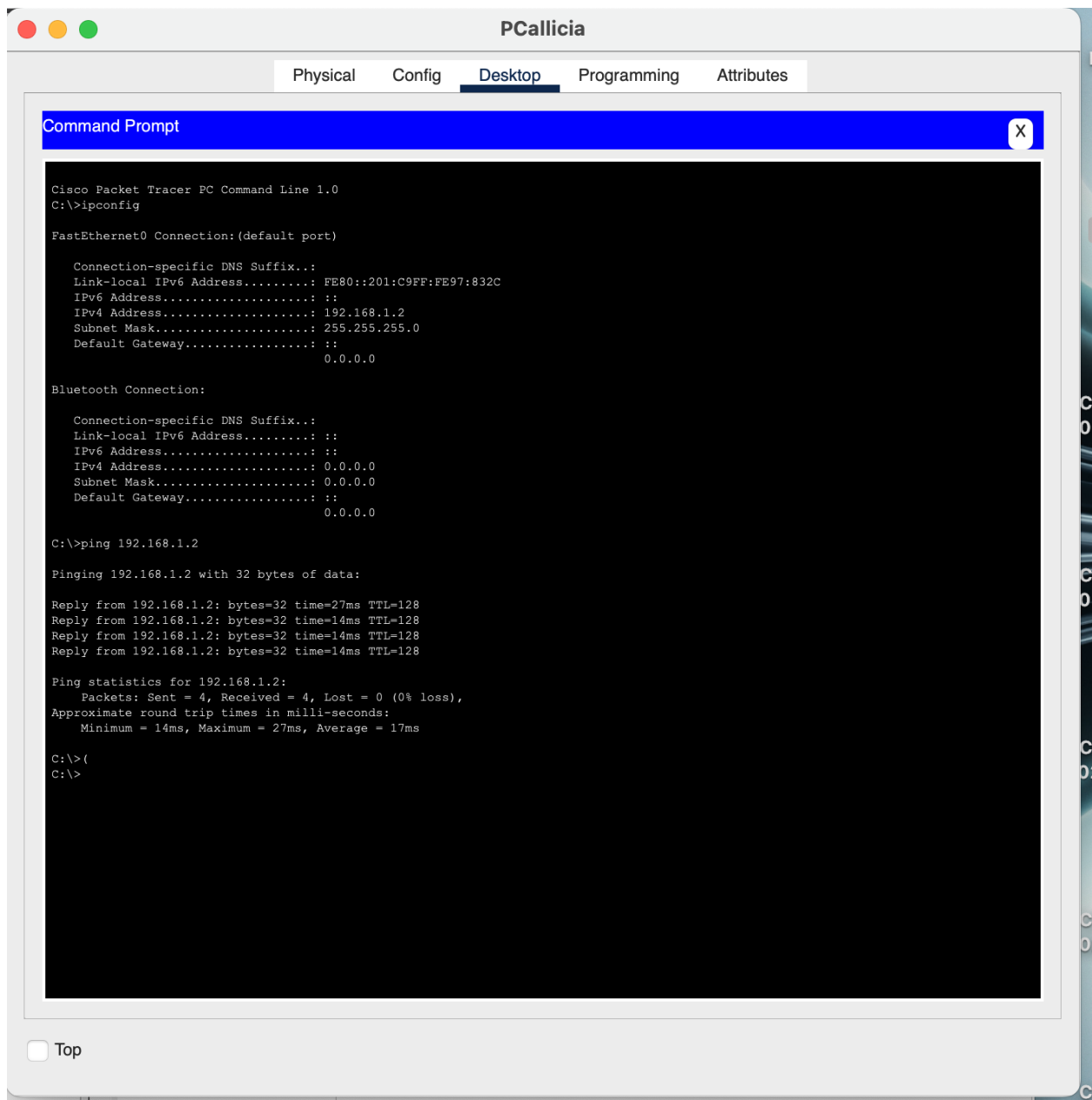
Job 06:

→ Quelle est la commande permettant de Ping entre des PC ?

l'outils permettant de ping ces "command ping"

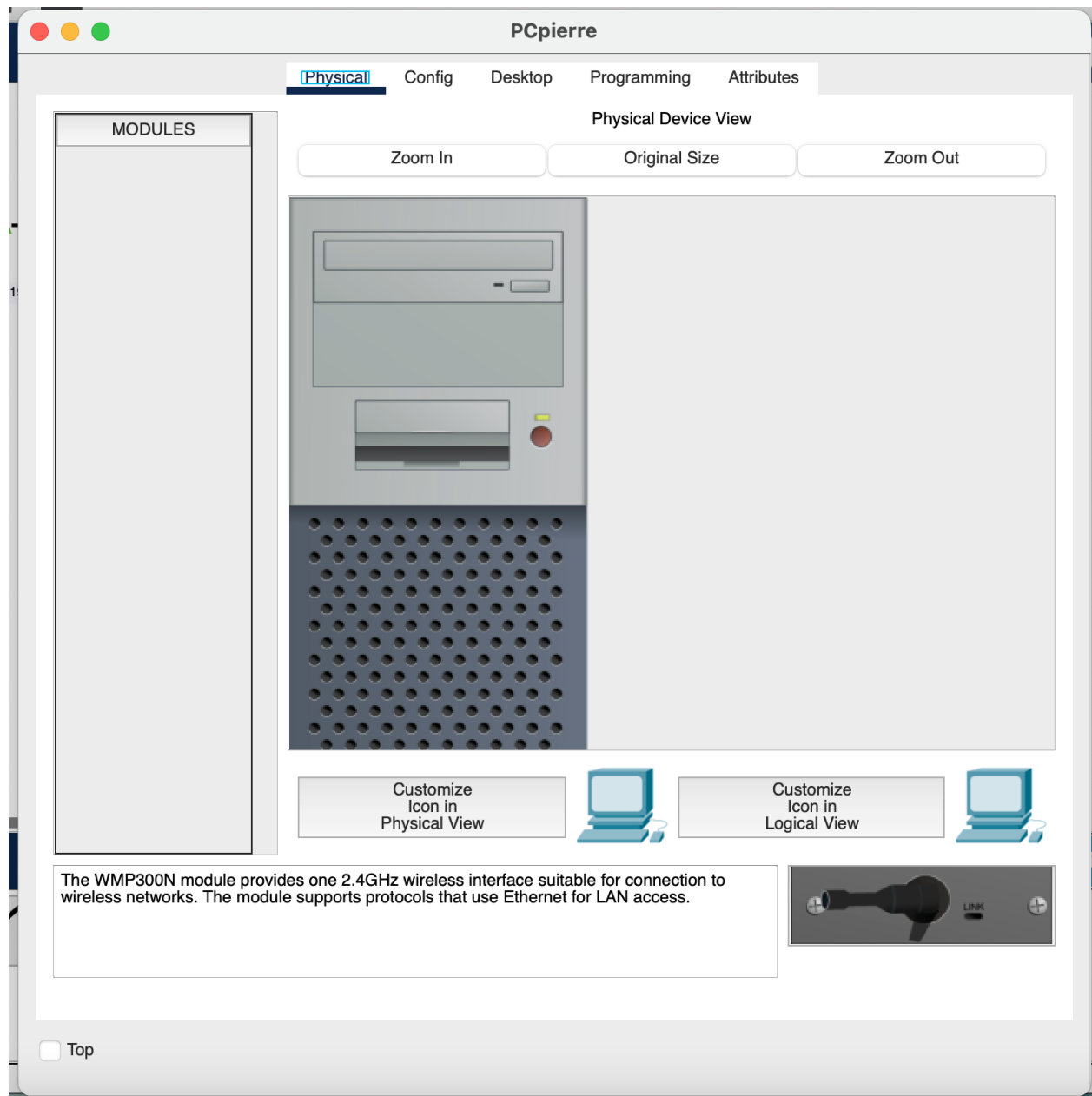


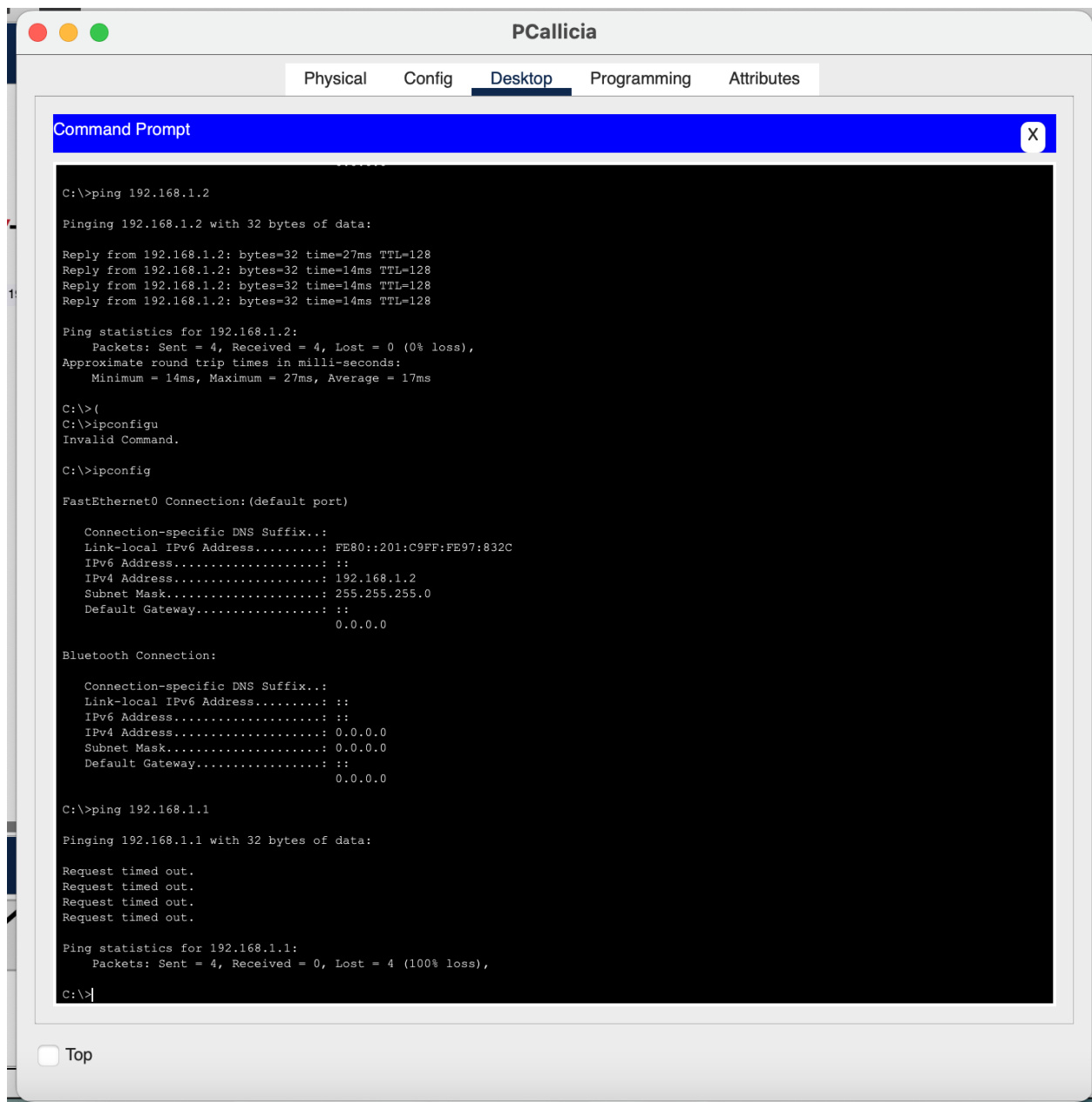




Job 07:

Éteignez le PC de Pierre. Utilisez le terminal du PC d'Alicia et PING le PC le Pierre. Faites une capture d'écran du terminal d'Alicia.





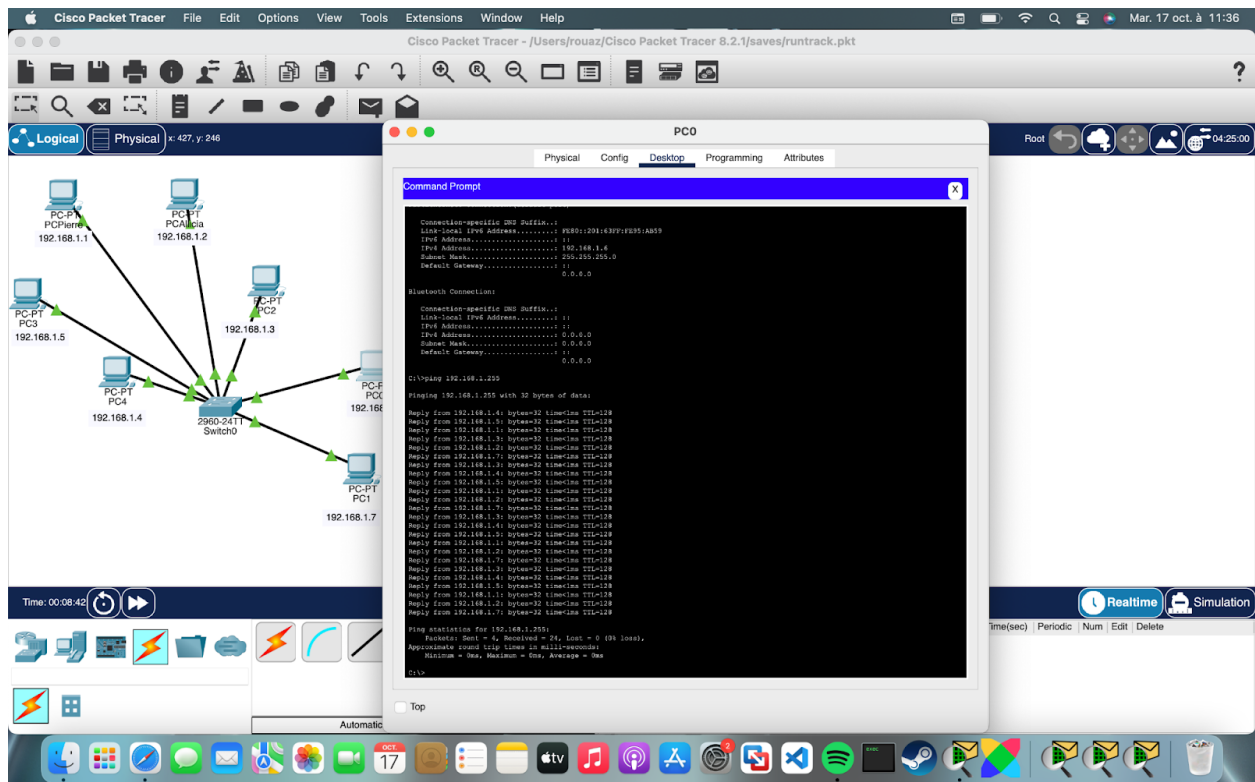
→ Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ?

Non le pc na pas reçu le paquet envoyé par alicia car le pc était éteint il n'était pas en état de recevoir de données.

→ Expliquez pourquoi.

car le pc étant éteint il n'avait aucun moyen de récupérer ou d'en envoyer d'ailleurs.

Job 08:



(mettre 255 a la fin de l'ip permet de ping toute les machine d'un coup)

→ **Quelle est la différence entre un hub et un switch ?**

La grande différence entre le hub et le switch informatique est la façon dont les trames sont livrées. Le hub n'a aucun moyen de distinguer vers quel port une trame doit être envoyée tandis que Le commutateur effectue un tri des trames afin de les orienter vers le bon port et donc vers le bon équipement.

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

un hub est un dispositif réseau simple qui diffuse les données reçues à tous les ports, ce qui le rend inefficace et peu sécurisé. Il est rarement utilisé de nos jours dans des réseaux modernes, car il a été remplacé par des commutateurs plus performants et sécurisés.

→ **Quels sont les avantages et inconvénients d'un switch ?**

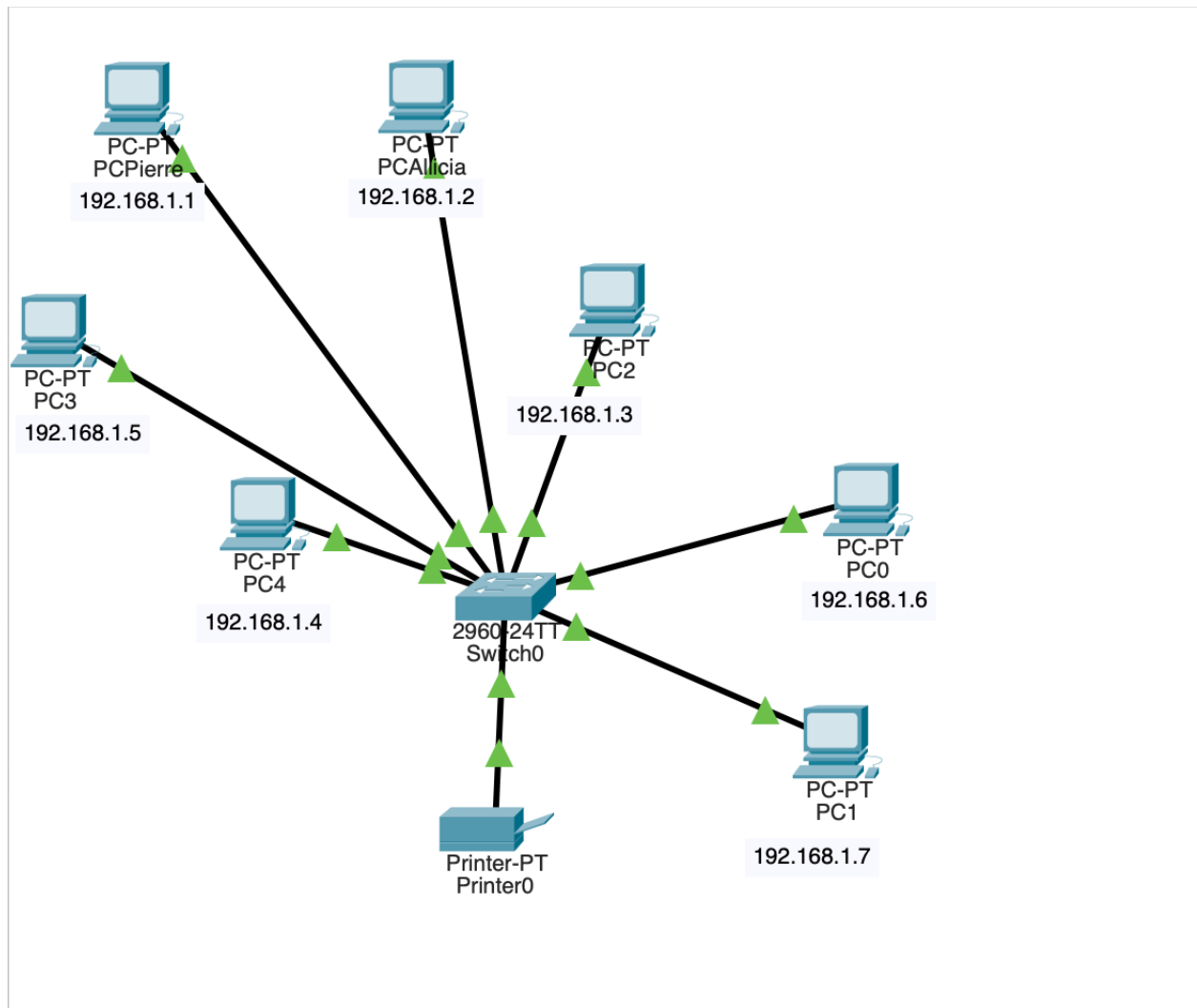
les switches offrent une gestion efficace du trafic, une meilleure sécurité et une utilisation plus

efficace de la bande passante par rapport aux hubs. Cependant, ils sont généralement plus coûteux et peuvent nécessiter des compétences de gestion avancées pour une configuration appropriée. Les avantages des switches les rendent essentiels dans les réseaux modernes.

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

un switch gère le trafic réseau en apprenant les adresses MAC des appareils connectés, en construisant une table de commutation pour associer ces adresses aux ports, en acheminant les données uniquement vers les ports appropriés en fonction des adresses MAC de destination, et en fournissant des fonctionnalités de gestion, de sécurité et de qualité de service pour optimiser les performances du réseau. Cette gestion intelligente du trafic contribue à améliorer l'efficacité et la sécurité des réseaux modernes.

Job 09:



Printer0

PhysicalConfigAttributes

GLOBAL

Settings

INTERFACE

FastEthernet0

FastEthernet0

Port Status

☒ On

Bandwidth

☒ 100 Mbps

☐ 10 Mbps

☒ Auto

Duplex

☐ Half Duplex

☒ Full Duplex

☒ Auto

MAC Address

00D0.5855.D911

IP Configuration

☐ DHCP

☒ Static

IPv4 Address

192.168.1.8

Subnet Mask

255.255.255.0

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address

/

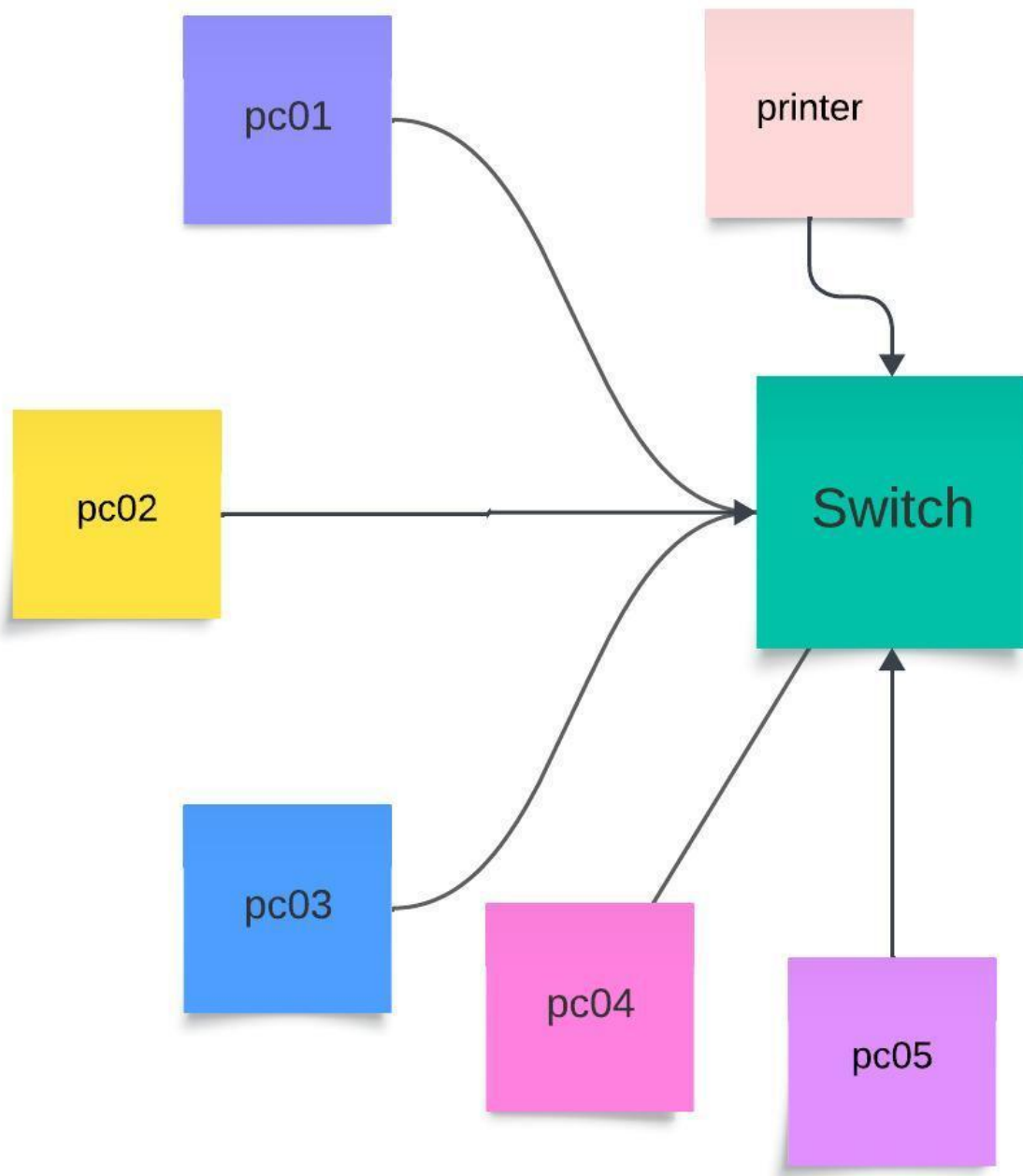
Link Local Address

FE80::2D0:58FF:FE55:D911

☐ Top

19

Schéma:



Job 10:

Server0

PhysicalConfigServicesDesktopProgrammingAttributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

DHCP

InterfaceFastEthernet0ServiceOnOff

Pool NameserverPool

Default Gateway192.168.0.100

DNS Server0.0.0.0

Start IP Address : 1921680100

Subnet Mask: 2552552550

Maximum Number of Users :100

TFTP Server:0.0.0.0

WLC Address:0.0.0.0

AddSaveRemove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168...	0.0.0.0	192.168...	255.255...	100	0.0.0.0	0.0.0.0

☐ Top

The screenshot shows a network configuration window for a device named PC1. The 'Desktop' tab is active, displaying the 'IP Configuration' section for the 'FastEthernet0' interface. In the 'IP Configuration' section, the 'DHCP' radio button is selected, and a message states 'DHCP request successful.' The assigned IPv4 address is 192.168.0.100, with a subnet mask of 255.255.255.0 and a default gateway of 192.168.0.100. The DNS server is set to 0.0.0.0. Below this, the 'IPv6 Configuration' section shows the 'Static' radio button selected. The IPv6 address is shown as two empty fields separated by a slash, with a link-local address of FE80::2E0:8FFF:FE9E:556C. The '802.1X' section has 'Use 802.1X Security' unchecked, and the authentication is set to MD5. At the bottom, there are empty fields for 'Username' and 'Password', and a 'Top' button.

→ Quelle est la différence entre une adresse IP statique et une adresse IP attribuée par DHCP ?

d'adresses IP. Voici un bref aperçu des classes A, B et C :

- Classe A :
 - Plage d'adresses : 1.0.0.0 à 126.0.0.0
 - Les adresses de classe A sont généralement utilisées pour les grandes organisations ou les fournisseurs de services Internet (FSI).
 - Le premier octet (8 bits) est réservé pour le réseau, tandis que les trois octets restants (24 bits) sont réservés pour les hôtes.
 - Cela signifie qu'une adresse de classe A peut prendre en charge un très grand

nombre d'hôtes, mais il y a un nombre limité de réseaux de classe A.

- Classe B :

● Job 11:

Nombre d'hôtes	Bit	Nombre d'adresse	Gateway	Plage d'adresse	Masque réseaux	Masque Binaire
12 hôtes	4	16 notament 14 utilisable	10.0.0.0	10.0.0.1 à 10.0.0.14	255.255.255.239 /28	1111 1111.1111 1111.1111 1111 0000
30 hôtes	5	32 notament 30 utilisable	10.0.0.16	10.0.0.17 à 10.0.0.46	255.255.255.224 /27	1111 1111.1111 1111.1111 1111 0000
30 hôtes			10.0.0.48	10.0.0.49 à 10.0.0.78		
30 hôtes			10.0.0.80	10.0.0.81 à 10.0.0.110		
30 hôtes			10.0.0.112	10.0.0.113 à 10.0.0.142		
30 hôtes			10.0.0.144	10.0.0.145 à 10.0.0.174		
120 hôtes	7	128 notament 126 utilisable	10.0.0.176	10.0.0.177 à 10.0.0.255 - 10.0.1.0 à 10.0.1.46	255.255.255.128 /25	1111 1111.1111 1111.1111 1111.1000 0000
120 hôtes			10.0.1.48	10.0.1.49 à 10.0.1.174		
120 hôtes			10.0.1.176	10.0.1.177 à 10.0.1.255 - 10.0.2.0 à 10.0.2.46		
120 hôtes			10.0.2.148	10.0.2.149 à 10.0.2.174		
120 hôtes			10.0.2.176	10.0.2.177 à 10.0.2.255 - 10.0.3.0 à 10.0.3.46		
160 hôtes	8	255 notament 253 utilisable	10.0.3.48	10.0.3.49 à 10.0.3.255 - 10.0.4.0 à 10.0.4.46	255.255.255.0 /24	1111 1111.1111 1111.1111 1111.0000 0000
160 hôtes			10.0.4.48	10.0.4.49 à 10.0.4.255 - 10.0.5.0 à 10.0.5.46		
160 hôtes			10.0.5.48	10.0.5.49 à 10.0.5.255 - 10.0.6.0 à 10.0.6.46		
160 hôtes			10.0.6.48	10.0.6.49 à 10.0.6.255 - 10.0.7.0 à 10.0.7.46		
160 hôtes			10.0.7.48	10.0.7.49 à 10.0.7.255 - 10.0.8.0 à 10.0.8.46		

→ Pourquoi a-t-on choisi une adresse 10.0.0.0 de classe A ?

- car étant plus malléable et pouvant supporter un plus grand nombre d'utilisateurs les adresses 10.0.0.0 de classe A sont les plus supportables.
- → Quelle est la différence entre les différents types d'adresses ?
- Les types d'adresses A, B et C que vous mentionnez font référence aux classes d'adresses IP utilisées dans le système de notation CIDR (Classless Inter-Domain Routing) qui est un moyen de représenter les adresses IP et de gérer l'allocation des adresses sur Internet. Cependant, il est important de noter que depuis de nombreuses années, le système de classe d'adresse IP n'est plus la norme principale pour allouer des adresses IP sur Internet. Au lieu de cela, CIDR est utilisé pour une gestion plus flexible et efficace des adresses IP. Néanmoins, il peut toujours être utile de comprendre les concepts associés aux classes
 - Plage d'adresses : 128.0.0.0 à 191.255.0.0
 - Les adresses de classe B sont généralement utilisées pour les moyennes et grandes entreprises.
 - Les deux premiers octets (16 bits) sont réservés pour le réseau, tandis que les deux octets restants (16 bits) sont réservés pour les hôtes.
 - Cela permet un nombre intermédiaire de réseaux et d'hôtes par rapport à la classe A.
-
- Classe C :
 - Plage d'adresses : 192.0.0.0 à 223.255.255.0
 - Les adresses de classe C sont généralement utilisées pour les petites entreprises et les réseaux locaux (LAN).
 - Les trois premiers octets (24 bits) sont réservés pour le réseau, tandis que le dernier octet (8 bits) est réservé pour les hôtes.
 - Cela permet un grand nombre de réseaux, mais un nombre limité d'hôtes par réseau.

Il y a également les classes D (pour la multidiffusion) et E (réservée à des fins expérimentales) qui ne sont pas mentionnées ici.

N'oubliez pas que, de nos jours, CIDR est préféré pour la gestion des adresses IP, car il permet une allocation plus souple et une utilisation plus efficace des adresses IP en utilisant une notation sous forme de préfixe (par exemple, 192.168.1.0/24) au lieu de se limiter strictement aux classes d'adresses.

Job 12:

<u>Couche OSI</u>	<u>Description des rôles</u>	<u>Matériels/Protocoles associés</u>	<u>→</u>
<u>Couche Physique</u> (Physical Layer)	<u>Gère les aspects physiques de la transmission des données, tels que le support de transmission, les signaux électriques, la fibre optique, les câbles, etc.</u>	<u>Ethernet, fibre optique, câble RJ45</u>	
<u>Couche Liaison de Données</u> (Data Link Layer)	<u>Gère la communication directe entre les dispositifs locaux, gère les adresses MAC (Media Access Control) et assure une transmission sans erreur des données.</u>	<u>Ethernet, MAC</u>	
<u>Couche Réseau</u> (Network Layer)	<u>Routage des données à travers des réseaux hétérogènes, adressage logique, et détermination du meilleur chemin pour les paquets de données.</u>	<u>IPv4, IPv6, routeur</u>	
<u>Couche Transport</u> (Transport Layer)	<u>Acheminement fiable des données d'un point à un autre, gestion du contrôle de flux, de la séquence et de la correction d'erreurs.</u>	<u>TCP, UDP</u>	
<u>Couche Session</u> (Session Layer)	<u>Gestion de l'établissement, du maintien et de la fin des sessions de communication entre les applications.</u>	<u>PPTP (Point-to-Point Tunneling Protocol), SSL/TLS</u>	
<u>Couche Présentation</u> (Presentation Layer)	<u>Traduction, compression et chiffrement des données pour s'assurer que les dispositifs de communication peuvent interpréter correctement les informations.</u>	<u>SSL/TLS</u>	
<u>Couche Application</u> (Application Layer)	<u>Couche la plus proche de l'utilisateur final, gère les applications et les services nécessitant la communication.</u>	<u>FTP, HTML</u>	

JOB13:

Quelle est l'architecture de ce réseau ?

La structure de ce réseau comprend les éléments suivants : une configuration en forme d'étoile, et il est équipé de composants tels que 2 serveurs, 1 commutateur (switch), et 4 ordinateurs personnels (PC). Les divers dispositifs communiquent entre eux via des connexions Ethernet à l'aide de câbles droits en cuivre.

→ Déterminer le nombre de machines que l'on peut brancher sur ce réseau ?

Pour déterminer le nombre de dispositifs que l'on peut connecter au réseau source, il est nécessaire de considérer les adresses IP déjà en cours d'utilisation. Les serveurs ont, au total, déjà reçu 5 adresses IP. Étant donné que le réseau peut fournir jusqu'à 256 adresses IP, nous soustrayons 4 de ce nombre pour obtenir la capacité d'accueil en machines. Ainsi, $256 - 4$ équivaut à 252. Par conséquent, il est possible de connecter jusqu'à 252 machines sur ce réseau

Job 14: Conversion les donnée

- 145.32.59.24 = 10010001.00100000.00111011.00011000
- 200.42.129.16 = 11001000.00101010.10000001.00010000
- 14.82.19.54 = 00001110.01010010.00010011.00110110

Job 15: Synthèse

→ Qu'est-ce que le routage ?

Le routage est le processus de transmission de données d'un point à un autre sur un réseau, à l'aide de routeurs pour déterminer le meilleur chemin pour transmettre ces données. Ceci est crucial pour diffuser des informations sur Internet.

→ Qu'est-ce qu'une passerelle ?

Les passerelles sont un élément important pour permettre la communication entre différents réseaux informatiques en assurant la compatibilité et la conversion des données, en plus de jouer un rôle de sécurité et de routage dans certains cas.

→ Qu'est-ce qu'un VPN ?

Un VPN, ou réseau privé virtuel, est un outil de sécurité en ligne qui crée une connexion sécurisée et cryptée entre votre appareil et un serveur distant. Cela protège votre confidentialité en ligne en masquant votre emplacement et en cryptant votre trafic Internet, protège vos données, permet l'accès à distance aux ressources de l'entreprise et aide à contourner la censure et les restrictions de géolocalisation.

→ Qu'est-ce que le DNS ?

Le DNS est un élément fondamental de l'infrastructure Internet car il simplifie l'accès aux sites Web en utilisant des noms de domaine au lieu d'adresses IP. Il joue un rôle essentiel en rendant Internet convivial et accessible aux utilisateurs.