TP 1: Packet Tracer (Table Mac, Protocole ARP, Ports)

Objectif: Connaitre et apprendre à manipuler Packet Tracer.

What is Cisco Packet Tracer?

> Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Cisco Networking Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.
>
> Packet Tracer can be run on Linux, Microsoft Windows, and macOS. Similar Android and iOS apps are also available. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices. A physical connection between devices is represented by a 'cable' item. Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BGP, to the extents required by the current CCNA curriculum. As of version 5.3, Packet Tracer also supports the Border Gateway Protocol.
>
> In addition to simulating certain aspects of computer networks, Packet Tracer can also be used for collaboration. As of Packet Tracer 5.0, Packet Tracer supports a multi-user system that enables multiple users to connect multiple topologies together over a computer network. Packet Tracer also allows instructors to create activities that students have to complete. Packet Tracer is often used in educational settings as a learning aid. Cisco Systems claims that Packet Tracer is useful for network experimentation.

Durée: 7 200 000 000 000 nanosecondes

Rendu:

- Ce travail demandé est à réaliser en solo. Il doit être démarré durant la séance, à terminer chez soi pour être remis à votre enseignant avant/à la prochaine séance de TP.
- Le dépôt se fait via un espace numérique de travail Moodle dédié
- Lacorrectionestautomatique,respectezstrictementlesconsignes
- Lesréponsesauxquestionsenrougedevrontêtrerenseignéesdanslerendu

Nota Bene:

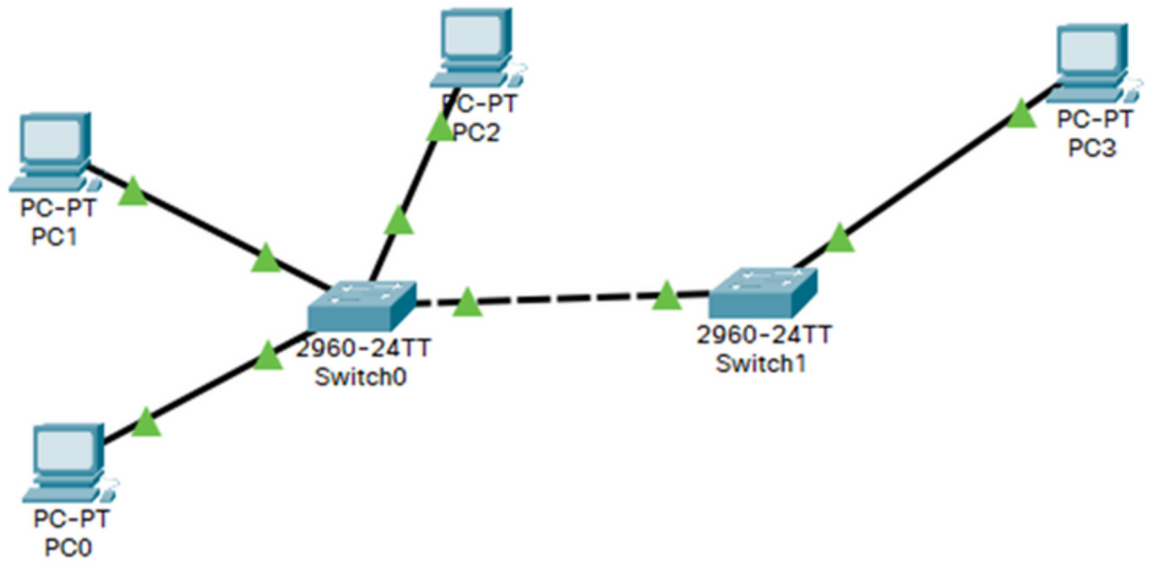
- (2021)UneannexefourniepourlapriseenmaindeCiscoPacketTracer.

[1] https://en.wikipedia.org/wiki/Packet_Tracer

1 Part 1. Commutation

Exercice 1 (Pré-requis).

Reproduire la topologie suivante :



- LesliensentrelesPCetlesswitchsseronten100MFullDuplex
- Lelienentrelesswitchsseraen1GFullDuplex

Configurer en adressage statique les PC en utilisant des adresses privées de classe C de votre choix. Noter les adresses IP & MAC de votre topologie ci-dessous :

- PC0: (IP adresse...) / (Mask...) / (MAC adress...)
- PC1: (IP adresse...) / (Mask...) / (MAC adress...)
- PC2: (IP adresse...) / (Mask...) / (MAC adress...)
- PC3: (IP adresse...) / (Mask...) / (MAC adress...)

Exercice 2 (Table MAC).

Connectez-vous sur les Switch0 et Switch1 en CLI, puis activez le mode "enable" et lancez les commandes:
`clear mac-address-table`
`show mac-address-table.`

1. Que contiennent les tables MAC des switchs ? Cela est due à quoi ?
2. Quelles sont les adresses MACs connues par le switch Switch0?

Testez la connectivité uniquement entre les PC connectés au Switch0 par ping.
`Relancer la commande: show mac-address-table.`

3. Queconstatez-vous?
4. De nouvelles adresses apparaissent-elles? Lesquelles ?
(Les adresses doivent être séparées par une virgule)

5. Pourquoi ?

Lancez la même commande sur le Switch1.

6. De nouvelles adresses sont elles apparues dans la table ? Si oui, lesquelles ?

7. Est-ce normal? Expliquez

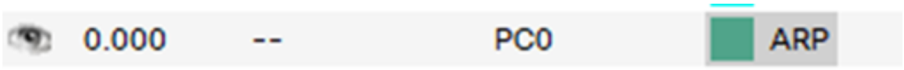
Testez la connectivité depuis un des PCs connectés sur le Switch0 vers le client connecté au Switch1 par un ping et vérifiez l'état de la table MAC du Switch1. Lancez encore la même commande sur le Switch1, que constatez-vous ?

8. Y a t'il eu un changement table dans la table ? Si oui, lesquelles?

Exercice 3 (Protocole ARP).
Sur tous les PC clients, videz la table ARP en utilisant la commande: arp -d depuis le «command prompt»
Passez votre logiciel en mode simulation et sélectionnez les protocoles ARP et ICMP. Lancez un ping depuis ce PC vers une destination de votre choix et lancez la simulation avec le bouton «play» (vous pouvez modifier la vitesse de transition entre les étapes avec le curseur)

1. Quel est le type du premier message émis depuis votre PC vers le switch?

2. Pourquoi ce premier paquet émis n'est pas un paquet ICMP ?



Consultez le détail de la requête ARP émise par le PC en cliquant sur la ligne adéquate dans l'«event list».
Une nouvelle fenêtre vous permet de consulter la construction de cette trame sur le modèle OSI ainsi que le contenu des différents entêtes.

3. Quel est l'adresse MAC destination de cette requête ?

4. Que signifie l'adresse MAC de destination de cette requête ?

Connectez-vous sur les switchs et tapez la commande: show arp

- Que constatez-vous ? Quelles informations vous sont rendues ? Est-ce normal ?

Exercice 4 (Port Security).
Gardez la topologie précédente et désactivez tous les ports inutilisés sur Switch1 et Switch2 (Afin que cela empêche les hôtes non autorisées de se connecter au réseau)
Configurez la sécurité des ports sur les interfaces utilisées pour connecter les machines sur le Switch1 et Switch2. N'autorisez bien sûr que l'adresse MAC du PC connecté au port.

1. Quelles sont les commandes utilisées ?

Utilisez une commande "show port-security" pour vérifier l'adresse MAC sur le PC2

2. Quelle est la syntaxe de la commande utilisée ?