

RÉSEAUX INFORMATIQUES



Objectifs de l'activité pratique :

Réseau Ethernet :

- câblage point à point, test d'écho ; commandes « mii-tool » et « linkloop »

Commutation Ethernet :

- câblage d'un commutateur
- table de commutation
- notion de segmentation,
- port miroir (WAN)

Routage IP :

- protocoles : LLC, ICMP, ARP ; commandes « ping », « ifconfig » et « netstat »
- paramétrage IP
- configuration d'un routeur

Support d'activité :

Serveur DidaVDI avec routeur, commutateur, câbles RJ45 et VidéoPhone

Ordinateur client sous Debian

Logiciel : WireShark

OBSERVATIONS

NOTE : /

DOCUMENTS RÉPONSES

NOMS : _____ / _____ / _____

GROUPE : _____

DATE : _____

Les réseaux informatiques font partie de notre quotidien depuis de nombreuses années. Ils sont le support de nombreux services (données, voix, vidéo). La théorie des réseaux introduit la notion de couches réseaux. Différents modèles de couches existent (DOD, OSI, ...). Dans un premier temps, le plus important est de connaître la position relative des couches réseaux les plus courantes. Les réseaux locaux (LAN) sont généralement basés sur les couches de protocoles IP et Ethernet.

LA BAIE VDI

Prendre connaissance par une première lecture du dossier relatif à la baie VDI (voir fichier **Baie VDI.PDF** dans le dossier Baie VDI sur le bureau).

À l'aide du dossier technique de la baie VDI.

Retrouver sur la baie VDI les éléments suivants : le serveur, le commutateur (ou switch), le routeur, le panneau de brassage, la set-top-box et le serveur DidaVDI.

Identifier sur le panneau de brassage les différents ports et leurs appartenances (par exemple : R1 est le port 1 du routeur).

APPELER LE PROFESSEUR POUR VALIDER AVANT DE POURSUIVRE

Le professeur met en marche le serveur et active le service HTTP.

Question 1 :

Identifier (sur la baie VDI) et donner les caractéristiques de l'IHM présente sur le serveur.

.....

IDENTIFICATION DES ADRESSES MAC ET IP DU SERVEUR

Dans un réseau Ethernet chaque machine est identifiée par une adresse unique codée sur 6 octets appelée adresse MAC.

À l'aide de l'IHM du serveur et du dossier technique de la baie VDI (pages 17 à 19) :

Question 2 :

Retrouver les adresses MAC et IP du serveur.

@MAC = **00:22:4d**:.....:.....

@IP = **192.168**.....

RÉSEAU ETHERNET POINT À POINT

CÂBLAGE POINT À POINT

Le réseau Ethernet le plus élémentaire est constitué par deux machines reliées à l'aide d'un câble croisé.

À l'aide d'un câble RJ45 croisé, brasser directement un PC client (L013-SIN1 par exemple) sur le serveur (panneau de brassage).

Sur le PC client, vérifier l'état du lien (link) et le débit théorique de la liaison en utilisant la commande :

mii-tool eth0 (à taper dans la console (Shell CLI) « terminal administrateur »).

Question 3 :

Quelle est la signification du nombre « 1000 » renvoyé par la commande « mii-tool » ?

Remarque : voir glossaire du dossier technique page 27.

TEST D'ÉCHO

L'utilitaire **linkloop** permet d'effectuer un test d'écho Ethernet (couche 2) en utilisant les adresses MAC.

À l'aide de l'IHM du serveur, démarrer le service linkloop.

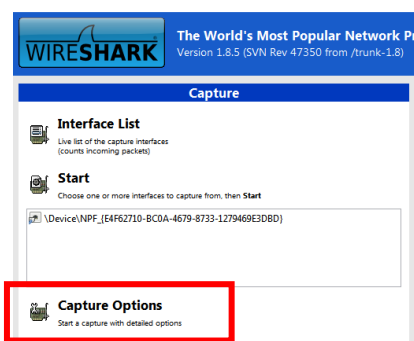
Depuis le PC client effectuer un test d'écho avec la commande linkloop vers l'adresse MAC du serveur trouvée précédemment.

linkloop 00:22:4d:xx:xx:xx

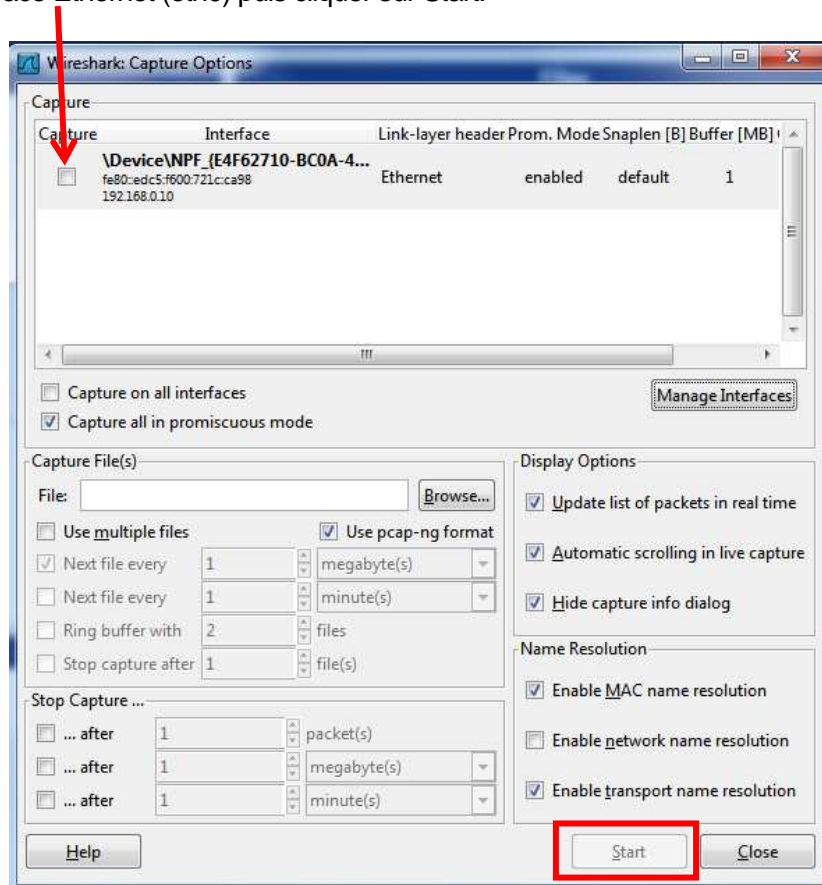
Sur le poste client, lancer le logiciel de capture et d'analyse réseaux « **Wireshark** » en utilisant la commande ci-dessous :

sudo wireshark

Cliquer sur **Capture Options**



Sélectionner l'interface Ethernet (eth0) puis cliquer sur Start.



Relancer un test d'écho comme précédemment.

linkloop 00:22:4d:xx:xx:xx

Dans WireShark, arrêter la capture sur l'interface Ethernet (Capture/Stop ou Ctrl+E).

Dans WireShark, appliquer un filtrage des paquets contenant l'adresse MAC du serveur (Filter).

eth.addr==00:22:4d:xx:xx:xx

Dans WireShark, la zone du haut donne la liste des paquets, après filtrage. Il doit rester deux paquets : le paquet émis depuis le PC client vers le serveur et le paquet renvoyé depuis le serveur vers le PC client.

À partir de ces deux paquets :

Question 4 :

Compléter le diagramme de séquence page suivante.

CÂBLAGE AVEC LE COMMUTATEUR (SWITCH)

À l'aide de câbles RJ45 droits :

Brasser le serveur DidaVDI sur le commutateur.
Brasser un PC client sur le commutateur (L013-SIN1 par exemple).

Sur le commutateur, vérifier les liens symbolisés par l'allumage des LEDs correspondantes.

Question 6 :

Compléter le tableau ci-dessous :

État de la LED (Éteinte/clignotante)	Éteinte	Clignotante
État du lien (up/down)

COMMUTATION ETHERNET

TABLE DE COMMUTATION

Sur le PC client, lancer le navigateur internet. Connectez-vous à l'interface web du commutateur avec l'adresse : **http://192.168.1.250**

Authentifiez-vous avec le nom d'utilisateur « **Cisco** » et le mot de passe « **password** ».

Naviguer dans le menu « MAC Address Tables > Dynamic Adresses » et observer la table Adresses MAC/ports de votre commutateur.

NOTION DE SEGMENTATION

Brasser un second PC client (L013-SIN2 par exemple), sur le commutateur.

Sur le second PC client lancer une capture WireShark.

Sur le premier PC Client, effectuer un test d'echo linkloop vers l'adresse MAC du serveur DidaVDI.

Sur le second PC Client, arrêter la capture WireShark puis appliquer un filtrage des paquets contenant l'adresse MAC du serveur DidaVDI.

Question 7 :

Expliquer pourquoi le second PC Client ne voit pas l'échange entre le premier PC Client et le serveur DidaVDI.

.....
.....

PORT MIROIR

Comme vous venez de le constater, une machine connectée sur un port du commutateur ne voit pas les échanges entre deux autres machines connectés sur deux autres ports du même commutateur. Pour analyser l'ensemble des échanges dans un réseau Ethernet, il est souvent utile de disposer d'un port permettant de voir l'ensemble des échanges qui ont lieu au sein d'un commutateur. Un port configuré de cette manière s'appelle **un port miroir**.

Le port repéré M du commutateur est configuré en port miroir.

Brasser le second PC client sur le port miroir du commutateur.

Réaliser de nouveau un test d'écho et une capture avec WireShark comme pour la notion de segmentation et vérifier que le second PC Client voit l'échange entre le premier PC client et le serveur DidaVDI.

ROUTAGE IP

Les adresses physiques sont uniques et non modifiables. La taille des réseaux actuels nécessite un adressage plus souple : l'adressage logique. **Les adresses logiques (adresses IP)** sont paramétrables par l'utilisateur.

ICMP : PING

Vous avez précédemment effectué des tests d'écho au niveau **liaison de données (couche 2)** avec le protocole **LLC** en utilisant l'utilitaire « **linkloop** » et les **adresses physiques (adresses MAC)**. Il est également possible d'effectuer des tests d'écho au niveau **réseau (couche 3)** avec le protocole **ICMP** (Internet Control Message Protocol) en utilisant l'utilitaire « **ping** » et les **adresses logiques (adresses IP)**.

Depuis un PC client, effectuer un test d'écho de niveau réseau (couche 3) avec le serveur DidaVDI en utilisant une requête d'écho ICMP.

Appuyer sur les touches Ctrl+C pour arrêter.

Sur un PC client, lancer le logiciel de capture et d'analyse réseaux « WireShark » puis lancer une capture sur l'interface Ethernet.

Sur un deuxième PC Client, relancer un test d'écho comme précédemment.

Arrêter la capture dans WireShark et appliquer un filtrage des paquets ICMP.

Question 8 :

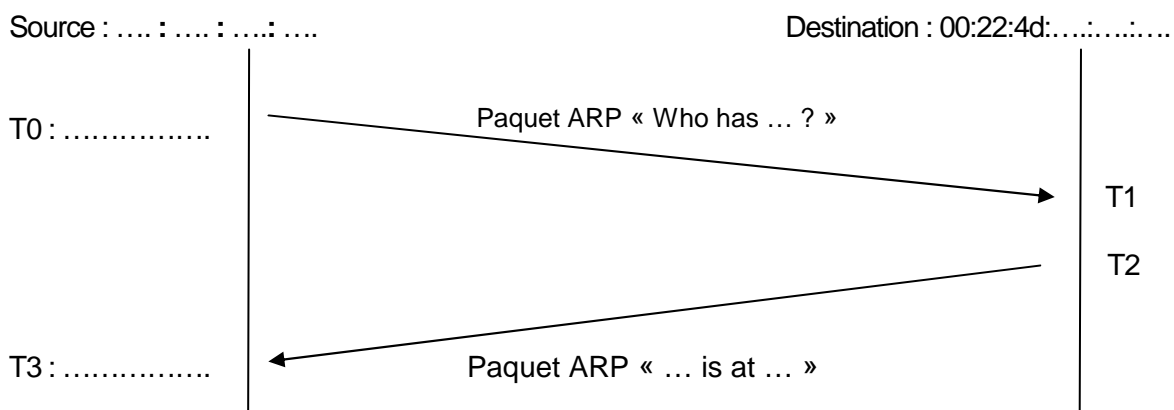
Compléter le diagramme de séquence page suivante.

INTÉRÊT DE ARP

Dans la capture WireShark précédente, appliquer un filtrage sur les paquets ICMP ou ARP (si vous ne voyez pas les requêtes ARP, vider le cache juste avant de faire le ping avec la ligne de commande suivante : `arp -d 192.168.1.100 ; ping 192.168.1.100`).

Question 10 :

Compléter le diagramme de séquence montrant l'échange ARP qui précède l'échange ICMP.



La requête ARP « Who has ... ? » n'est pas effectuée systématiquement, pour optimiser les performances les systèmes d'exploitation disposent d'un tampon ARP (ARP cache).

Visualiser le contenu du tampon ARP de votre PC Client avec la commande :

arp -a

CAS CONCRET D'UTILISATION DE ARP

Il existe de nombreux périphériques réseaux ne disposant pas de capacité d'affichage locale, par exemple une caméra réseau. Si l'interface réseau d'un tel périphérique est paramétrée en DHCP, il n'y a aucun moyen pour afficher son adresse IP obtenue via DHCP. Une solution est alors de visualiser le bail DHCP sur le serveur qui l'a délivré. Une autre solution consiste à utiliser ICMP et ARP.

Connecter un VidéoPhone paramétré en DHCP sur un port du commutateur.

Question 11 :

Noter l'adresse MAC du VidéoPhone (voir étiquette au dos du VidéoPhone).

@MAC = **00:0b:82**:.....:.....

Depuis un PC Client, effectuer une requête d'écho ICMP en « broadcast » (adresse de diffusion) sur le réseau « **192.168.1.0/24** », avec la commande : **ping -b @diffusion**.

Laisser tourner une minute puis arrêter avec les touches « **Ctrl+C** ».

Visualiser le contenu du tampon ARP de votre PC Client et relever l'adresse IP correspondante à l'adresse MAC du VideoPhone.

@IP =

PARAMÉTRAGE IP

Les principaux paramètres IP d'une machine sont :

- son adresse IP
- le masque de sous-réseau
- l'adresse IP de la passerelle

Sous LINUX, le paramétrage IP de la machine peut être réalisé via l'environnement graphique (GUI) ou à travers l'interpréteur de commande (CLI). Afin d'illustrer les deux méthodes, vous allez utiliser l'interpréteur de commande pour la lecture des paramètres IP, et l'interface graphique pour l'écriture de nouveaux paramètres IP.

LECTURE DES PARAMÈTRES IP

Brasser un troisième PC client (L013-SIN3 par exemple) sur un port normal (pas le port miroir) du commutateur.

Sur le second PC Client, vérifier les paramètres IP de l'interface eth0 obtenus via DHCP en utilisant la commande : **ifconfig eth0**

Question 12 :

Compléter le tableau ci-dessous :

Adresse IP
Masque de sous-réseau

Question 13 :

Calculer ci-dessous l'adresse du sous-réseau en effectuant un ET logique (bit à bit) entre l'adresse IP de la machine et son masque de sous-réseau.

@masque de sous-réseau =

Sur le troisième PC Client, visualiser la table de routage en tapant la commande : **netstat -ar**


Question 14 :

Noter l'adresse IP de la passerelle (routeur) obtenue via DHCP :

@passerelle =:.....:.....

ÉCRITURE DES PARAMÈTRES IP

Sur le troisième PC Client, dans la barre « GNOME » en haut à droite, effectuer un clic droit

sur l'icône : 

Dans la liste déroulante sélectionner « Modification des connexions », et dans la fenêtre « Connexions réseaux », sélectionner l'onglet « Filaire » puis « Wired connection 1 ou eth0 », puis cliquer sur « Modifier ».

Cliquer sur l'onglet « Paramètres IPv4 », puis dans la liste déroulante « Méthode », choisir « Manuel ». Enfin, dans le tableau « Adresses », cliquer sur « Ajouter », et compléter les champs d'après le tableau ci-dessous :

Adresse	Masque de sous réseau	Passerelle
192.168.0.213	255.255.255.0	192.168.0.251

Question 15 :

Calculer l'adresse du sous-réseau en effectuant un ET logique (bit à bit) entre l'adresse IP de la machine et son masque de sous-réseau.

@masque de sous-réseau =:.....:.....

Question 16 :

Comparer l'adresse de sous-réseau obtenue avec celle calculée précédemment (lecture des paramètres IP).

.....

Essayer d'effectuer un test d'écho de niveau réseau (couche 3) vers le serveur DidaVDI.

ROUTAGE IP

Le commutateur ne travaille qu'au niveau liaison de données (couche 2). La communication IP entre sous-réseaux différents nécessite l'emploi d'un **routeur**, qui lui travaille au **niveau réseau** (couche 3), autrement dit, au niveau du protocole IP.

Brancher un port LAN du routeur sur le commutateur.

Brancher le premier PC Client (L013-SIN1 en DHCP dans le sous-réseau 192.168.1.0/24) sur le commutateur.

Brancher le troisième PC Client (L013-SIN3 en IP statique 192.168.0.213/24) sur le port WAN.

Les adresses IP de passerelles définies par les sous-réseaux 192.168.0.0/24 et 192.168.1.0/24 sont respectivement 192.168.0.251 et 192.168.1.251. Il faut affecter ces adresses IP respectivement aux ports WAN et LAN de votre routeur.

APPELER LE PROFESSEUR POUR VALIDER AVANT DE POURSUIVRE**Le professeur réinitialise le routeur dans sa configuration par défaut :**

Appuyer sur le bouton reset jusqu'à ce que la LED « Test » clignote (environ 10 s)
Laisser le routeur redémarrer (environ 1 min)

Dans la configuration usine, l'adresse IP du routeur est 192.168.1.1

Depuis le premier PC Client (L013-SIN1 en DHCP dans le sous-réseau 192.168.1.0/24), effectuer un test d'écho de niveau réseau (couche 3) vers le routeur.

Connectez-vous à l'interface http du routeur.

Authentifiez-vous avec l'utilisateur « **admin** » et le mot de passe « **password** ».

Pour éviter tout conflit avec le service DHCP du serveur DidaVDI, désactiver le service DHCP du routeur :
Network Configuration > LAN Setting > LAN Setup >, dans la section « DHCP », activer « Disable DHCP Server » et valider par « Apply ».

Sur la même page, dans la section « LAN TCP/IP Setup », modifier l'adresse IP du routeur à « 192.168.1.251 » et valider par « Apply ».

Reconnectez-vous sur l'interface http du routeur.

Cliquer sur « Network Configuration > WAN Setting > Broadband ISP Settings », dans la section « Internet (IP) Address » compléter les champs comme ci-dessous :

IP Address : **192.168.0.251**

IP Subnet Mask : **255.255.255.0**

Gateway IP Address : **192.168.0.251**

Cliquer sur « Network Configuration > WAN Setting > WAN Mode », dans la section « Use NAT or Classical Routing between WAN & LAN interfaces ? », activer « Classical Routing » et valider par « Apply ».

Cliquer sur « Security > Firewall > Attack Checks », dans la section « WAN Security Checks », activer « Respond to ping on Internet Ports » et valider par « Apply ».

Cliquer sur « Security > Firewall > LAN WAN Rules », dans la section « Inbound Services », cliquer « Add ... » et compléter comme ci-dessous puis valider par « Apply ».

Service	ANY
Action	ALLOW ALWAYS
Select Schedule	Schedule 1
Send to LAN Server	Single Address
Translate to port Number	
WAN Destination IP Address	Broadband
LAN Users	Any
WAN Users	Any
Log	Never
Bandwith Profile	NONE

Redémarrer le routeur, en cliquant sur « Monitoring > diagnostics », et cliquer sur « reboot ».

Depuis le premier PC Client (en DHCP dans le sous-réseau 192.168.1.0/24), effectuer un test d'écho de niveau réseau vers le second PC Client (paramétré en 192.168.0.201).

Question 17 :

Noter ci-dessous vos remarques.

.....

Depuis le second PC Client (paramétré en 192.168.0.201), effectuer un test d'écho de niveau réseau vers le premier PC Client (en DHCP dans le sous-réseau 192.168.1.0/24).

Question 18 :

Noter ci-dessous vos remarques.

.....

