

Licence biomédicale



TRAVAUX PRATIQUES

RÉSEAUX INFORMATIQUES HOSPITALIERS

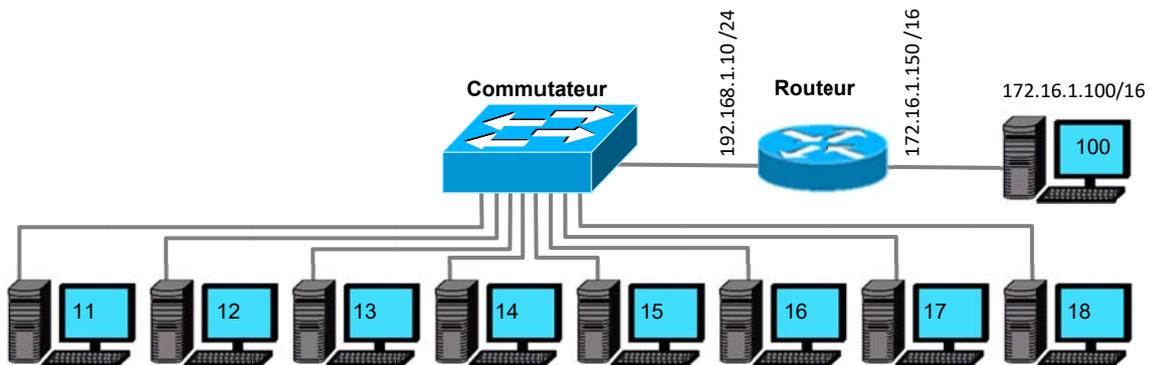
2020

<i>SÉANCE 1</i>	<i>Configuration d'un réseau</i>	<i>1</i>
<i>SÉANCE 2</i>	<i>Analyse de trame – Switch – VLAN – WiFi.....</i>	<i>5</i>
<i>SÉANCE 3</i>	<i>Routage – VPN.....</i>	<i>9</i>
<i>SÉANCE 4</i>	<i>Réseaux de monitoring patient – Dépannage.....</i>	<i>13</i>

SEANCE 1 : CONFIGURATION RÉSEAU

I. Configuration réseau locale

Les 8 postes de notre réseau local sont connectés entre eux et au poste 100 :



1. Définissez en groupe une stratégie d'adressage IP pour chaque poste permettant la communication de tous les équipements entre eux.
Quel est le masque de sous-réseau ?
Quels sont le *NetId* et le *HostId* de votre poste ?
De quelle classe est notre réseau : A, B ou C ?
Combien ce réseau peut-il contenir de postes ?
2. Configurez alors l'interface ethernet (icône connexions réseaux sur le bureau) : **adresse ip, masque, pas de passerelle** (Clic droit sur Ethernet, Propriétés, Protocole internet version 4 (TCP/IPv4))
3. Ouvrez PowerShell  en tant qu'administrateur dans la barre des tâches : clic droit, exécuter en tant qu'administrateur
Vérifiez la configuration en exécutant la commande `ipconfig /all`
Notez et commentez la réponse.
4. Testez la connectivité avec tous les 7 autres pc du réseau par la commande :
`ping [adresse IP du destinataire]` et remplissez le plan d'adressage suivant :
(On peut obtenir l'adresse MAC d'un équipement distant par la commande '`arp -a`' après avoir exécuté un `ping` vers cet équipement)

Nom	Adresse IP	Masque	Adresse MAC	N°Port switch
pc11				
pc12				
pc13				
pc14				
pc15				
pc16				
pc17				
pc18				

5. On va créer 2 sous-réseaux : changez l'adresse IP des postes 15, 16, 17 et 18 en 172.17.1.nn/16
 Testez la connectivité avec un poste de l'autre sous-réseau
 Expliquez pourquoi la connexion n'est pas possible
 Rétablissez la configuration initiale

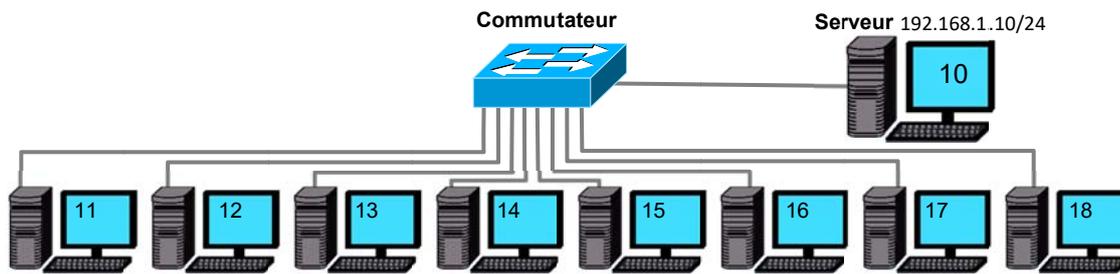
6. Le poste 172.16.1.100 est équipé d'un serveur web http
 Ouvrez le navigateur *Chrome* et tapez son adresse IP dans la barre d'adresse.
 Ça ne devrait pas fonctionner : Il faut renseigner l'adresse IP de la passerelle par défaut sur la configuration IPv4 de votre poste. Testez

7. Partage de fichiers *Windows*
 Sous C:\ créez un dossier nommé partage15 (pour le poste 15 par exemple) ; dans ce dossier, créez un document texte.txt contenant votre nom ou ce que vous voulez.
 Effectuez un clic droit sur le dossier, sélectionnez « propriétés » puis l'onglet « partage »
 Activez le bouton '*partager*', dans le champ vide tapez '*tout le monde*', puis cliquez '*ajouter*'
 Validez en cliquant sur '*partager*'
 Vos collègues devraient maintenant pouvoir lire votre fichier partagé. Vérifiez l'accès au fichier partagé d'un autre poste. Supprimez votre dossier partagé

8. A retenir

- Pour que 2 équipements puissent communiquer entre eux sans passerelle, il faut que la partie **NetId** (correspond aux 255 du masque) de leur adresse IP soit la même.
- La commande **ipconfig /all** affiche la configuration réseau complète du poste
- La commande **ping** (suivie d'une adresse IP) teste la connectivité avec un équipement distant
- La commande **arp -a** affiche les correspondances des adresses IP et MAC récemment utilisées

II. Configuration réseau automatique : serveur DHCP



Observez la configuration DHCP sur le serveur : Etendue, bail, ...

1. Configurez votre poste connexion réseau Ethernet afin d'obtenir une adresse IP automatiquement et testez votre configuration par la commande `ipconfig /all`
Listez les paramètres réseau configurés automatiquement sur votre poste.
2. Résiliez le bail DHCP par la commande `ipconfig /release`, notez votre adresse MAC puis configurez le serveur DHCP afin qu'il délivre à votre machine toujours la même adresse IP (192.168.1.xx).
Lorsque tout le groupe a terminé les réservations, sollicitez un nouveau bail avec `ipconfig /renew` et testez votre configuration avec : `ipconfig /all`.
3. Comparez les avantages/inconvénients par rapport à la configuration en IP locale vue précédemment

III. Serveur DNS

Pour la navigation sur Internet on utilise généralement des noms plus parlants que l'adresse IP: par exemple `snf.com` au lieu de `90.84.59.155`.

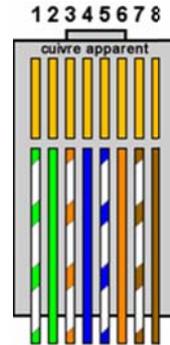
Lorsqu'un équipement recherche l'adresse IP d'un équipement, il consulte tout d'abord son fichier '*Host*' interne ; s'il ne trouve pas la réponse il interroge son serveur DNS plus complet qui lui-même peut interroger un autre serveur DNS...

1. Configurez le serveur DNS afin d'y ajouter le nom de votre poste (poste11 par exemple) en zone de recherche directe. Testez en tapant `ping postexx`.
2. Chaque machine mémorise les associations @IP/Nom de domaine pendant un certain temps.
Commentez la réponse à la commande `ipconfig /displaydns`
Recommencez après avoir exécuté `ipconfig /flushdns`

IV. Câblage d'un cordon RJ45

Vous câblerez un cordon Ethernet droit 100 Base T. Des câbles nus, connecteurs, cutters, pinces coupantes et 2 pinces à sertir spécifique se trouvent dans la salle. La méthode est la suivante :

- Dénuder la gaine extérieure sur 1,5 cm à l'aide d'un cutter
- Positionner les conducteurs (sans les dénuder !) dans le bon ordre et couper le surplus de façon à ce que la gaine pénètre de 5mm dans l'embout, les conducteurs doivent atteindre l'extrémité de l'embout.
 - Sertir l'ensemble avec la pince dédiée
 - Après avoir vérifié que les 2 embouts sont bien sertis, vérifiez le bon fonctionnement de votre cordon avec le testeur *Fluke*



1	TD+	Blanc/Vert
2	TD-	Vert
3	RD+	Blanc/Orange
4	nu	Bleu
5	nu	Blanc/bleu
6	RD-	Orange
7	nu	Blanc/Marron
8	nu	Marron

1. Analyse de trames – Encapsulation

Configurez votre poste en *dhcp*, pour l'analyse de trames vous utiliserez le logiciel Wireshark, une notice simple se trouve sur votre poste de travail

1. Etude des trames dhcp

Exécutez Wireshark, puis lancez une capture

Dans une fenêtre « invite de commande », tapez `ipconfig /release` puis `ipconfig /renew`

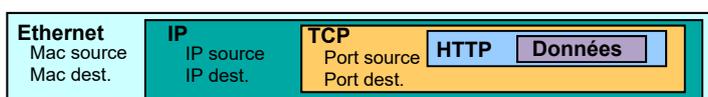
Identifiez les trames DHCP (on peut utiliser un filtre du type : *bootp*)

Quelles sont les 4 phases d'une transaction dhcp ?

Commentez les trames encapsulées et les informations échangées : adresses MAC, IP...

Dessinez le diagramme d'encapsulation

d'une trame DHCP. Exemple pour http :



2. Trames http

Le protocole http permet le fonctionnement des navigateurs web

Nous disposons d'un serveur web d'adresse IP 172.16.1.100 situé derrière un routeur.

Exécutez Wireshark, puis connectez-vous à ce serveur avec Chrome, stoppez la capture puis analysez et commentez les trames échangées (Vous pourrez utiliser le filtre `ip.addr==votre adresse ip` ou le filtre `http`).

Vérifiez le diagramme d'encapsulation d'une trame http

Quelle information importante est contenue dans la couche *tcp* ? Quel est le numéro de port standard d'un serveur HTTP ? , de votre poste client ?

3. Trames ftp

FTP est le protocole de transfert de fichier très utilisé sur Internet

Exécutez Wireshark sur votre poste, puis lancez une capture (filtre=*ftp*)

Connectez-vous au serveur FTP par la commande `ftp 192.168.1.10` (login *imb*, mot de passe *tsh*).

Vérifiez le fonctionnement du client ftp en accédant aux fichiers du serveur (ls = liste les fichiers, get=copie de fichier serveur→local, put=copie de fichier local→serveur, bye=ferme la session ftp)

Commentez les trames et les informations échangées : Le mot de passe est-il visible ?

Dessinez le diagramme d'encapsulation d'une trame ftp

Quel est le numéro de port standard d'un serveur ftp ?

4. Trames arp

Pour qu'un poste A puisse envoyer des données à un poste B, l'adresse mac de B doit être connue de A. Le poste A recherche tout d'abord dans son cache *arp* l'adresse *mac* correspondant à l'adresse IP visée (le cache *arp* est actualisé dynamiquement)

En cas d'échec, il envoie une requête *arp* broadcast pour que B lui retourne son adresse *mac*

Videz le cache ARP de votre poste par la commande `arp -d *`, lancez une capture, effectuez un *ping* vers un poste quelconque, stoppez la capture, observez et commentez les trames *arp* (filtre=*arp*)

II. Commutateur (ou Switch)



1. Filtrage des trames

Exécutez Wireshark, lancez une capture puis effectuez des 'ping' vers les autres postes.

Vous devriez observer vos 'ping' et leurs réponses mais pas ceux exécutés sur les autres postes

Comment le commutateur peut-il savoir vers quel port acheminer le 'ping' ? Effectuez des propositions

2. Mesure du débit utile

Pour mesurer le débit utile des données entre 2 postes à travers le commutateur, on peut utiliser l'outil `ttcp`. Dans le répertoire `ttcp` sur le bureau cliquez 'droit' sur `TtcpEmit.bat` puis sur modifier. Dans le fichier, modifiez l'adresse IP pour qu'elle corresponde à celle de votre voisin.

Demandez à votre voisin (ou vous-même) de lancer d'abord `ttcpReceive.bat`, puis lancez `ttcp Emit` sur l'autre poste. Après quelques secondes, des données apparaissent et vous renseignent sur la rapidité de la connexion, notez le débit moyen en kB/s (k octets/s) que vous convertirez en bit/s (1kB=1024 octets) et exprimerez en % de la bande passante de la liaison (100 Mbits/s).

3. Trames broadcast dans un commutateur

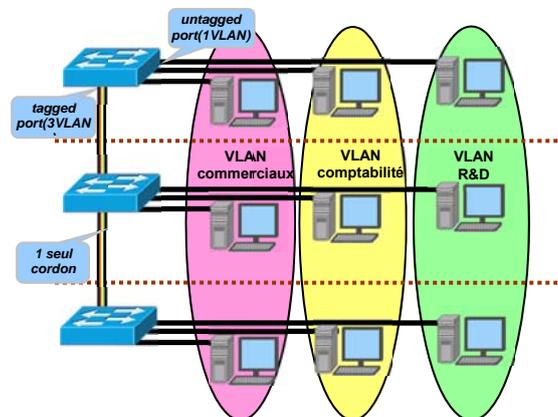
Effacez la table ARP de votre poste (`arp -d *`), exécutez quelques `ping` (en même temps que vos collègues) et lancez une capture. Des trames provenant d'autres postes et ne vous étant pas destinées à priori ont-elles pourtant transité jusqu'à vous ? Quel type de trames ? Qu'est-ce qu'une adresse MAC Broadcast ?

4. Utilisation des VLAN

Les commutateurs permettent de fractionner un réseau en plusieurs **sous-réseaux isolés** appelés VLAN qui transitent par les mêmes commutateurs et les mêmes cordons RJ45 ('tagged link') mais restent complètement isolés entre eux.

Intérêts :

- Economie de commutateurs et cordons
- Sécurité : création de sous réseaux isolés
- Réduction de la taille du domaine de broadcast donc augmentation de la bande passante
- Grande souplesse de configuration à distance



Lorsque vous serez tous arrivés à ce point, prévenez

l'enseignant pour qu'il fractionne le réseau en 2 VLAN puis, à l'aide de 'ping', déterminez la constitution des VLAN A et B

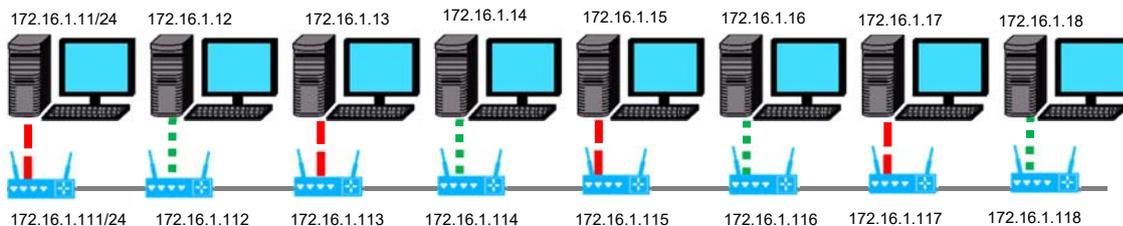
5. Mise en œuvre de VLAN avec le commutateur CISCO RV110W

Vous allez constituer un réseau local de 8 postes fractionné en 3 VLAN :

Le VLAN1 (VLAN par défaut) et indispensable

Le **VLAN3** auquel appartiendront les postes 11, 13, 15 et 17

le **VLAN4** auquel appartiendront les postes 12, 14, 16 et 18



Configurez votre poste conformément au schéma ci-dessus

Reliez le port 1 du commutateur à votre poste (port d'administration)

Reliez le port 3 au commutateur suivant à droite et le port 4 au commutateur suivant à gauche

Connectez-vous au commutateur, son adresse ip est inscrite sur le boîtier.(login=cisco, pass=cisco)

Configurez les VLAN dans le menu *Networking > LAN > VLAN Membership*

Pour un VLAN donné, chaque port peut recevoir l'attribut Default, Untagged, Tagged ou Excluded :

Le port 1 véhiculera uniquement le VLAN1 (administration)

Les ports 3 et 4 véhiculeront les 2 VLAN 3 et 4 taggés

Le port 2 (utilisation) véhiculera uniquement votre VLAN non *taggé* (3 ou 4 selon la parité de votre poste)



Reliez votre poste au port 2, exécutez des commandes *ping* sur d'autres postes du même VLAN et de l'autre, puis lancez *WireShark* et capturez les trames. Des trames de l'autre VLAN, et plus particulièrement les trames broadcast sont-elles véhiculées jusqu'à votre poste ?

Rétablissez la configuration initiale du commutateur : menu administration>Backup- Restore Settings

Puis : Locate & select the upload file : RV110_startup.cfg

Start to Upload

III. WiFi

L'intérêt du WiFi est la **mobilité**, les risques sont la **vulnérabilité** des données et la **fiabilité**



1. Configuration

Désactivez l'interface filaire de votre poste (clic droit puis désactiver)

et activez l'interface sans fil que vous configurerez avec une adresse ip 172.16.1.n°poste/16

En cliquant sur l'icône , trouvez le SSID (diffusé) du réseau vous paraissant probable, la clé wpa2 est 'TPnetwork'

Testez la connectivité entre postes.

2. Vitesse de transfert en mode g

Organisez-vous en groupes de 2 postes (1 émetteur + 1 récepteur) et mesurez la vitesse de transfert en bps avec l'outil tcp (déjà utilisé) en simultané puis indépendamment.

Concluez en comparant avec les vitesses obtenues en filaire (séance précédente)

3. Vitesse de transfert en mode n

Demandez à l'enseignant de commuter le point d'accès en mode n, puis reprenez la mesure de vitesse précédente.

4. Vitesse de transfert en éloignement

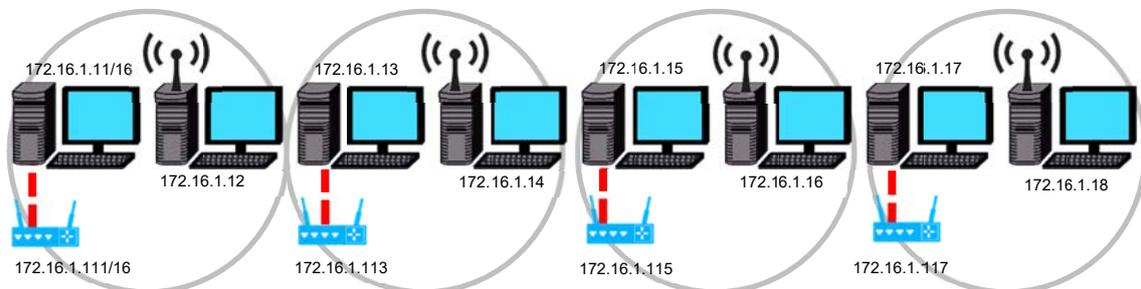
Lorsque le point d'accès est éloigné (30m), reprenez la mesure de vitesse précédente

5. Configuration du point d'accès

On veut réaliser 4 réseaux Wifi différents dans le même lieu.

Organisez-vous en groupes de 2 PC et connectez le point d'accès Cisco sur le PC de numéro impair (sur ce PC vous désactivez le WiFi et activez l'interface filaire.)

Configurez vos PC en 172.16.1.n°poste /16:



Configurez le point d'accès avec un SSID imb11, imb13, imb15 ou imb17 sans sécurité

Configurez le PC de numéro pair en WiFi, avec le bon SSID et l'adresse IP indiquée.

Quelle sont les différences entre la configuration d'un point d'accès et celle d'un pont ?

Rétablissez la configuration initiale du point d'accès : menu administration>Backup- Restore Settings

Puis : Locate & select the upload file :

6. Sécurité/confidentialité

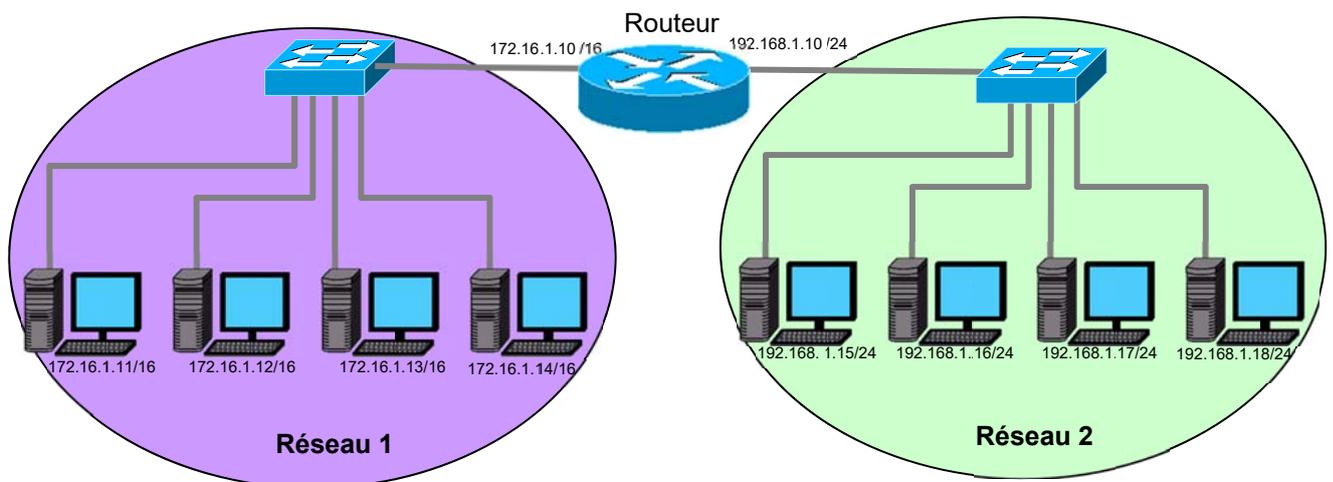
Le réseau Wifi que nous avons configuré pourrait-être facilement observé et pénétré à distance.

Listez et classez les solutions de protection par ordre d'efficacité que vous avez pu observer en parcourant les menus.

I. Routage simple (niveau 3 OSI)

Deux équipements ayant des adresses IP dont la partie Net Id sont différents (par exemple **192.168.1.12/24** et **192.168.2.18/24**) ne peuvent communiquer que par l'intermédiaire d'un **routeur ou passerelle**. Un routeur possède donc au moins 2 interfaces réseau. Lorsqu'un routeur n'a aucune interface réseau correspondant à l'adresse IP demandée, il peut transmettre la trame à un autre routeur et ainsi de suite : c'est le principe du routage sur Internet.

1. Organisez les adresses IP des postes conformément au schéma ci-dessous sans passerelle



2. Connectivité et analyse de la table de routage locale

- a) En exécutant la commande `'route print'`, analysez la table de routage locale de votre poste.
- b) **127.0.0.1** est l'adresse IP de **loopback** (rebouclage) ou **localhost** présente sur chaque poste ; testez la commande `ping 127.0.0.1` ou `ping localhost`
- c) Testez la connectivité avec l'autre réseau

3. Configurez votre poste de façon à assurer une connectivité avec l'autre réseau.

- a) Quel changement cela apporte-t-il à la table de routage ? Que représente l'adresse **0.0.0.0** ?
- b) Testez la connectivité avec l'autre réseau. Concluez.
- c) Capturez avec *Wireshark* une trame de votre commande `ping` (filtre `=icmp`), commentez les adresses IP et MAC contenues dans la trame émise. L'adresse MAC destinataire de la trame capturée est-elle celle du poste distant ? A qui appartient cette adresse MAC (pour vous aider tapez `arp -a`) ? Les trames broadcast franchissent-elles les routeurs ?

4. La commande **tracert** permet de visualiser tous les routeurs traversés pour joindre un destinataire.

Exécutez la commande `tracert adresse IP` avec une adresse IP de l'autre réseau, commentez les résultats. Quelle est l'utilité de la commande `'tracert'` par rapport à la commande `'ping'` ?

II. Tunnel VPN

THÉORIE

Définition

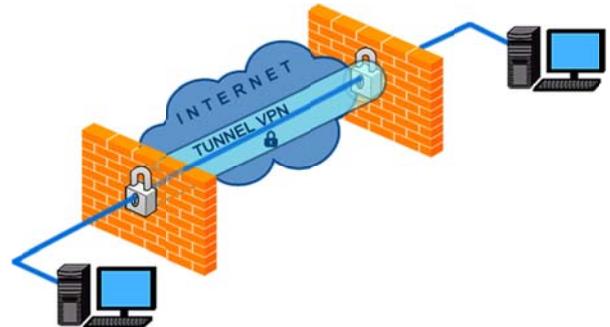
Un réseau privé virtuel, abrégé VPN – Virtual Private Network, est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic Internet

Problématique

S'il est bien sûr possible d'initier une connexion à partir d'un intranet vers Internet, à priori il est impossible d'initier une connexion vers un poste d'un intranet distant.

VPN

Un tunnel isolé préconfiguré (Protocole Ipsec) est utilisé vers l'intranet distant. L'adresse ip destination du datagramme IP (ESP) est publique (adresse WAN du routeur), à l'intérieur de ce datagramme est encapsulé un autre datagramme dont l'adresse ip destination est cette fois privée (adresse LAN). Les données de ce datagramme sont cryptées.

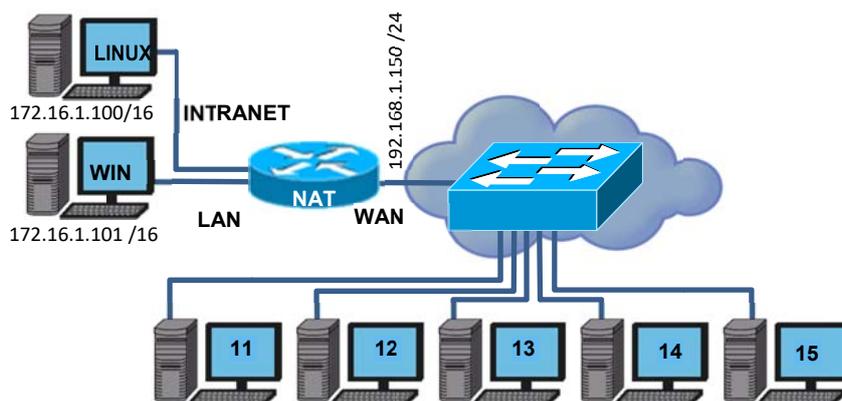


PRATIQUE

Un poste WINDOWS et un poste LINUX sont placés dans un réseau local intranet 172.16.0.0/16

Vous vous organiserez en binômes ou trinômes sur les 5 postes 11, 12, 13, 14, 15

Votre poste est censé se trouver sur internet, le but est d'accéder aux 2 postes intranet situés derrière un routeur NAT



1. Test de connexion sans VPN

Configurez votre poste en 192.168.1.xx/24 avec la passerelle 192.168.1.150

Testez la connexion avec les 2 postes intranet avec des commandes ping

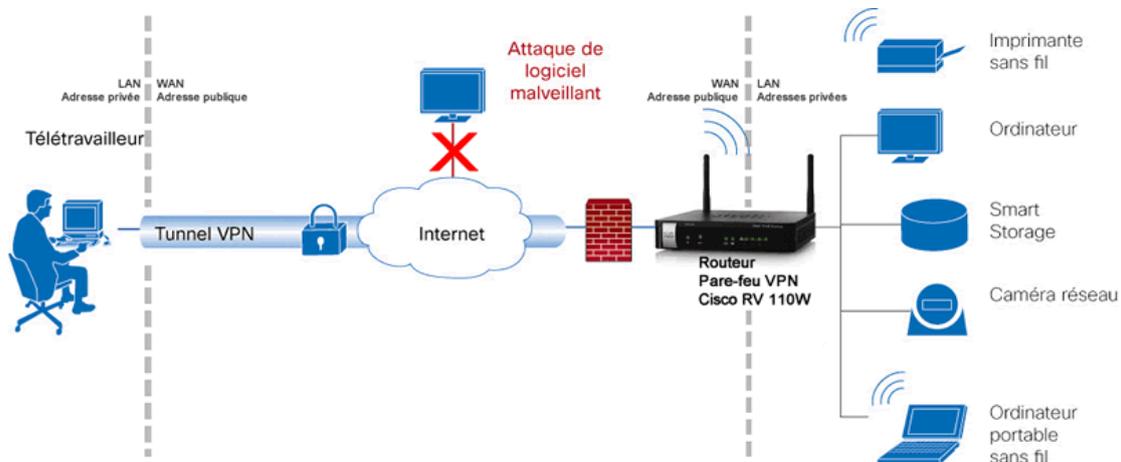
Pourquoi la connexion est-elle impossible ?

Quelle est la différence avec la partie I. dans laquelle la connexion était possible à travers le routeur ?

Exécutez WIRESHARK avec le filtre *icmp* avant votre *ping*. Commentez les trames capturées

2. Préparation du VPN

Cisco propose un utilitaire très simple : QUICKVPN pour créer un VPN avec le routeur NAT RV110W
Pour la sécurité et le cryptage du VPN, il faut utiliser un certificat confidentiel et crypté qui contient une clé publique(symétrique), les informations d'utilisateur et la méthode de cryptage.



Copiez le certificat RV110W_client.pem présent sur votre bureau dans le répertoire :

C:\Program Files (x86)\Cisco Small Business\QuickVPN Client

Exécutez VPNClient dans Cisco Small Business, le login est vpn11, le mot de passe est passvpn11 pour le poste 11 par exemple. Connectez-vous avec le bouton *Connect*



3. Utilisation du VPN

Tests ping

Effectuez des commandes *ping* vers les postes LINUX et WINDOWS

Effectuez des captures de trame, et commentez le contenu des trames *ping* notamment le datagramme *ESP* propre aux VPN IPSEC

Connexion au poste WINDOWS

Dans l'explorateur WINDOWS de votre poste, entrez \\172.16.1.101, vous devriez accéder au contenu partagé de ce poste.

Connexion au poste LINUX

- Connexion au serveur web

Exécutez WIRESHARK avec le filtre *http*,

Entrez l'adresse du poste linux dans le navigateur chrome et vérifiez le bon fonctionnement

Arrêtez la capture et vérifiez que le contenu des trames est bien crypté

Représentez le diagramme d'encapsulation

- Connexion à travers le terminal ssh *putty*

Putty est un petit utilitaire qui permet d'utiliser une machine à distance

Exécutez *putty* et entrez l'adresse IP du poste LINUX

Connectez-vous avec le login *pi* et le mot de passe *raspberry*

Vous êtes sur la console de la machine linux, vous pouvez lister les fichiers (commande *ls*),

effectuer des *ping*, exécuter des programmes, arrêter la machine...

- Supprimez le certificat RV110W_client.pem du répertoire :
C:\Program Files (x86)\Cisco Small Business\QuickVPN Client

4. Bilan à retenir

Les vpn permettent une extension sécurisée et cryptée d'un réseau local intranet à travers internet

I. Réseaux de monitoring

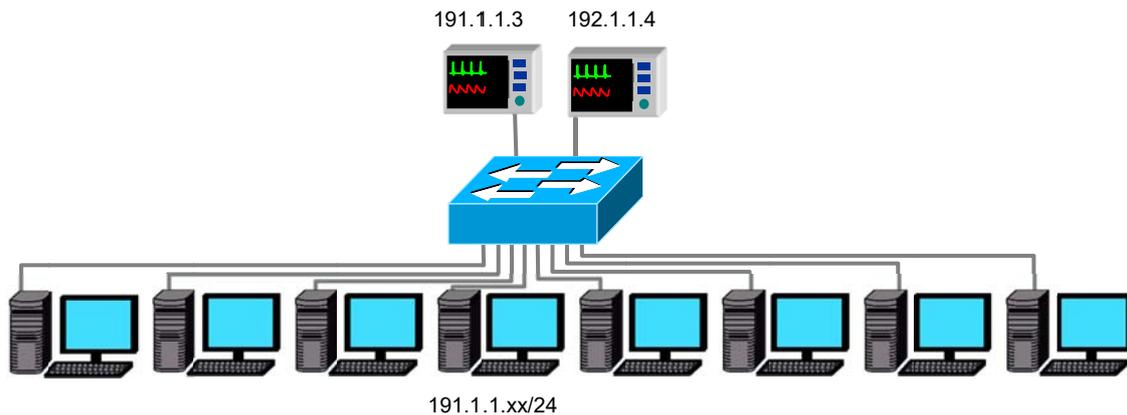
Transmission multicast

Une émission *multicast* consiste à diffuser un seul datagramme destiné à plusieurs destinataires. L'intérêt concerne la visioconférence et pour nous le monitoring patient en réanimation par exemple : une alarme sur un moniteur peut-être diffusée sur tous les moniteurs dans toutes les chambres sans l'aide d'une centrale. Une infirmière peut également observer les données patient d'une autre chambre, c'est la fonction '**bed to bed**'

Le protocole utilisé ne peut pas être TCP car il ne peut y avoir d'accusés de réception : **UDP** est utilisé. Selon la norme, l'adresse IP destination d'une diffusion *multicast* commence par un octet supérieur à **224**

En pratique le *multicast* pourrait facilement « inonder » les réseaux comme des trames *broadcast*, les commutateurs et routeurs peuvent ne propager les trames multicast qu'aux interfaces ayant reçu une demande d'abonnement IGMP, c'est l'**IGMP snooping**

Configurez l'adresse IP de votre poste en 191.1.1.N°poste /16



1. Lancez une analyse de trame, voit-on des trames provenant des moniteurs ? On peut utiliser un filtre d'affichage du type `ip.addr==192.168.1.3 || ip.addr==192.168.1.4`, (|| représente le 'ou logique')
2. Pour observer l'*IGMP snooping*, lancez une nouvelle capture puis exécutez le programme '*monitorage*'. Stoppez la capture et identifiez les trames IGMP. Les données provenant des chambres 214 et 215 sont-elles toujours absentes ?
3. A quelle classe appartient l'adresse IP destination ? Quel est l'intérêt d'utiliser un tel protocole en réseau de monitoring

Classe IP v4	1 ^{er} octet	2 ^{ème} octet	3 ^{ème} octet	4 ^{ème} octet
A	Net Id		Host Id	
	0 à 127			
B	Net Id		Host Id	
	128 à 191			
C	Net Id			Host Id
	192 à 223			
D	Multicast			
	224 à 239			

4. Les trames Multicast sont dirigées vers plusieurs destinataires, pour ne pas les confondre avec les trames MAC Broadcast (ff:ff:ff:ff:ff:ff), une adresse MAC spéciale Multicast est utilisée, quelle est cette adresse ?
5. En observant les captures *wireshark*, déterminez le nombre de paquets par seconde provenant d'un seul moniteur ainsi que la taille maximale d'un paquet. Déterminez alors le nombre maximal de moniteurs patient ne surchargeant pas le réseau : On estime que la congestion commence à 20% de la bande passante (10 Mbits/s ici).

Pause 10 minutes

II. Dépannage réseau

Dans le schéma suivant, le routeur, le poste 18 et le poste 100 sont correctement configurés.

Vous devriez en théorie pouvoir vous connecter à tous les postes avec des commandes *ping*, ... ça n'est pas le cas, il y en a 5 erreurs de configuration.

Déterminez toutes les causes probables de dysfonctionnement, et proposez une correction

Pour chaque erreur que vous pensez avoir trouvée, demandez confirmation à l'enseignant et gardez vos réflexions et solutions **confidentielles** avec vos collègues.

