***SI2 Support réseaux des accès utilisateurs***

Le concept de réseau s’est développer dans les année 70.

***Peer to Peer*** → partager des ressources (DD, Imprimantes…)entre différents postes.

Cela à évoluer en ***Client/Serveur*** → centraliser les ressource sur une machine (serveur)→ partage des ressources et les sécurisent, et le client permette de s’y connecter. La sécurité est assuré par des annuaires(inventaires de toutes les ressources d’une entreprises) appelé LDAP→ chez Windows →Active directory.

Les ***SERVICES*** et les protocoles sont deux choses ***IMPORTANTES***.

Le modèle de l’architecture ***OSI*** (***Open Systems Interconnection***) est composé de 7 couches, il a abouti en 1984. Il va permettre de faire communiquer un système par rapport à un autre.

***7-La couche application***

Offre les fonctions de communication à l’utilisateur. Elle est en quelques sorte l’interface utilisateur pour les fonctions de communications. (Messagerie, VM)

***6-La couche présentation***

Traite la mise en forme de l’information. Au-dessus d’elle l’information est codé sous une forme plus appropriée pour son transport. Compression et cryptage sont les rôles de la couches 6.

***5-La couches session***

Elle permet d’ouvrir une session à distance sur un serveur (login/psw). Elle offre des services de synchronisations et de rattrapages d’erreurs.

***4-La couches transport***

Reçoit les données de la couche session et assure leur transport de bout en bout. Elle s’assure que tous ses paquets arrive à destination. Pour améliorer la rapidité de transmission la couche peu créer plusieurs connexions simultanées sur lesquelles elle repartit les paquets.

***3-La couche réseau***

Routage des paquets et gestion de l’adressage IP. Elles s’occupent des pb d’incompatibilités entre couches basses des réseaux traversés.

***2-1- les 2 couches inférieures***, couches liaisons de données et couches physique traitent de la transmission bit par bit des messages sur le support physique de transmission. On ne parle plus de paquets mais de trames.

Dès qu’on passe d’une couche a une autre on encapsule les données de couches qui seront stocker dans un en-tête le « Header ». A l’arrivée on va désancapsuler.

Création du comité 802 l’IEEE en 1980 (chercher la définition).

Sur un réseau local :

Medium (Câble rj45, fibre optique…)

Topologie du réseau (en bus, en étoile, en anneaux…)

Méthode d’accès CSMA/CD non cacophonie sur un réseau → 802.3.

Détecter les collisions sur un réseau, écouter avant d’émettre sa trame. Il écoute en permanence et dès que la voie est libre il envoie sa trame. Si collision→renvoi de la trame.

On peut classer les réseaux en 3 catégorie de distinctes :

-Les réseaux longues distance ***WAN*** Wide Area Network

-Les réseaux interurbains ***MAN*** Métropolitain Are Network

-Les réseau locaux ***LAN*** Local Area Network

Hub = concentrateur

Switch = Le répartiteur

Rj45 = Paire torsadée

Matériel d’interconnexion de base pour un réseau :

***-Le concentrateur*** = HUB → Répéteur multiport il est uniquement capable de faire que du broadcast (diffusion).

***-Le répartiteur*** = Switch → Matériel qui permet d’augmenter la bande passante (Fast Ethernet) table mac/port = enregistrement de l’adresse mc et du port de chaque machine, il apprend dynamiquement les adresses mac. Chaque port va émettre à la vitesse proposer par le switch. Dans un premier temps il fait un broadcast pour découvrir le réseau, puis de l’unicast. Il permet également de faire des VLAN. C’est un regroupement d’utilisateurs communiquant entre eux via le commutateur. Ils vont nous permettre de segmenter le réseau. Les broadcasts correspondent aux VLANs et limite le trafic. Mises-en place d’un niveau de sécurité.

***-Le routeur →*** Grace à ses tables de routages il va orienter le paquet vers le bon réseau. Ils peuvent interconnecter plusieurs réseau.

***-Autres***

Câble de catégorie 5, 6 et 7 constitué de 4 paires torsadés.

 Exemples de protocoles internet : -***IP Internet Protocol*** la couche réseau de la structure.

 -***ARP Address Resolutoin Potocol***: Couhe 2 du modèle OSI.

 -***ICM Internet Control Message Protocol***: Protocol de gestion des messages.

 -***TCP Transmission Control Protocol*** transport fiable avec accusé de réception

 -***UDP User Datagram Protocol*** non fiable

 Synthèse entre les différents câbles cat 6, 7 et fibre optique

***Synthèse des différents câbles Ethernet et fibre optique***

***Câble RJ45 cat 6***

La catégorie 6 des cordons RJ45 peut transmettre des données avec des débits pouvant aller jusqu'à 1 Gbit/s sur des longueurs de 100 mètres maximum.

Ce type de câble peut permettre l'utilisation du Gigabit Ethernet.
De nos jours, la catégorie 6 devient la norme des réseaux d'entreprises.

***Câble RJ45 cat 6a***
La catégorie 6a permet, de transporter des données avec des débits qui peuvent aller jusqu'à 10 Gbits/s.

Le câble de catégorie 6a est utilisé dans des réseaux avec liaisons Ethernet en mode full-duplex.

***Câble RJ45 cat 7***
La catégorie 7, permet la transmission de données à des débit de 10 Gbits/s.

Ils sont utilisés pour des réalisations de réseaux informatiques Ethernet qui ont besoin de très haut débits. Le câble de catégorie 7 possède quatre paires torsadées qui sont blindées individuellement. Ce type de câble est donc doté des meilleures performances possibles pour un câble. il permet l’acheminement d’un signal de télévision modulé en bande VHF ou UHF.

***Câble de cat 7a***

La catégorie 7a permet un débit allant jusqu'à 10 Gbit/s. Par contre, le connecteur RJ45 n'est pas reconnu, créant les mêmes difficultés que la catégorie 7 pour connecter les équipements.

***La fibre optique***

Le record actuel de transmission a été établie en laboratoire par NEC et Corning en septembre 2012, le débit record est de 1 pétabit/s soit 125 000 giga-octets/s sur une distance de 52,4 km.

***Notion de protocole :***

C’est un mode opératoire qui doit être commun à tous les éléments qui désirent communiquer entre eux.

Il n’y pas de communication possible sans avoir recours à un protocole.

Un protocole doit être adapté au type

***←Tcp-ip***

***Protocole applicatif***: protocole de haut niveau, destinés à permettre le dialogue entre applications serveur et clients.

Exemple : -HTTP

 -POP

 -FTP

 -SMTP

***La couche de transport***

/ Protocole orientés transports de données

UDP(User Datagram Protocol) est dit « sans connexion » et « TCP » est dit « avec connexion ». Ces protocoles permettent à la couches 4 de transporter leur donné.

Le TCP nécessite un accusé de réception.

UDP Utilise la communication sans connexion.

***La couche Internet***

Ce sont des protocoles de haut niveau de la couche réseau.

IP → permet un routage des informations entre réseaux c’est ici que l’adresse IP est utilisé.

ICMP → est un protocole de « contrôle » il met à dispotion des outils de dépistage d’erreurs et de signalisation.

On trouve également dans cette couche les protocoles :

ARP(MAC →IP)et

RARP(IP→MAC)

ARP est donc chargé de l’obtention de l’adresse matérielle des hôte TCP-IP sur des réseaux supportant la diffusion.

ARP recherche toujours dans la mémoire cache ARP une correspondance d’adresse ip. Elle a recours à une diffusion locale.

***La couche réseau***

Protocole de plus bas niveau sur le réseau, il assure la bonne gestion du médium (détection de collision) et permet l’acheminement des informations (trames) entre émetteur et destinataire au niveau des adresses MAC.(Medium Access Contrôle)

***La couche transport***

***IP*** est un protocole sans connexion charger particulièrement d’adresser et de router les paquets entre hôtes IP.

***IP*** est sans connexion car in il n’établit pas de session avant l’échange de donnée

***IP*** n’est donc pas fiable car il ne peut pas garantir la livraison. Il effectue toujours une tentative « Besse effort » pour livrer le paquet.

Pendant le parcours le paquet peut être perdu, retarder.

***IP*** ne nécessite pas d’accusé de réception des données

L’émetteur et le récepteur ne sont pas tenus au courant de la perte de paquet.

Cet accusé réception est du ressort du protocole de transport TCP.

TCP → service fiable de livraison fondé sur le mode connecté.

Les données TCP sont transmises par segment et une session doit être établit avant que les hôtes puissent échanger des données.

Pour chaque segment envoyé à l’hôte récepteur doivent renvoyer un ACK. Si l’émetteur ne reçoit pas de ACK les données sont retransmises.

TCP fabrique donc des paquets qui seront routés par IP et TCP numérote chaque paquet. Ce numéro permettra de remettre les paquets dans le bon ordre si ceux-ci sont arrivés dans le désordre.

Ce numéro correspond au ACK du paquet.

Les port TCP constituent un emplacement physique pour la livraison des messages. (RFC 1700) IANA(iana welknown port)

UDP

Fournit un service de datagramme sans connexion et avec une livraison de type (remise au mieux) Bess Effort, non fiable.

UDP est utilisé pour des application ne nécessitant pas d’accusé réception et transmettant des petites quantités d’informations.

Ex : services de Nom NetBIOS, SNMP

UDP (unreliable packet delivery) utilisé pour le streaming.

Udp et TCP utilisent la notion de Socket

Un socket est un couple d’adresse ip + n°

Netstat

Le socket est un canal de communication indispensable pour faire communiquer 2 machines entre elle.

***Adressage ip***

C’est la possibilité d’identifié un poste sur un réseau. Composé en 2 partie, une partie qui identifie le réseau et l’autre la machine.

Deux format d’adressage IP : -Le format binaire

 -Le format décimal point

Chaque adresse est codée en 32 bits composé de 4octets de 8bits (IPV4).

Chaque octet représente une valeur décimal comprise entre 0 et 255.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 2^7 | 2^6 | 2^5 | 2^4 | 2^ 3 | 2^2 | 2^1 | 2^0 |
| Poids | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| Binaire | 1000 0000 | 0100 0000 | 0010 0000 | 0001 0000 | 0000 1000 | 0000 0100 | 0000 0010 | 0000 0001 |

Exemple :

192.168.43.185

192.168.10.16 1100 0000(128+64) 101010000(128+32+8) 00001010 (8+2) 0001 0000(16)

172.16.34.100 1010 1100 (128+32+8+4) 0001 0000 (16) 0100 0010(32+2) 0110 0100 (64+32+4)

10.0.0.224 00001010 0000 0000 0000 0000 1110 0000

Il existe différente classe d’adresse IP.

La communauté internet définit 5 classes dont les principales sont les suivantes :

|  |  |  |  |
| --- | --- | --- | --- |
| Octet 4 | Octet 3 | Octet 2 | Octet 1 |
| Octet 4 | Octet 3 | Octet 2 | Octet 1 |
| Octet 4 | Octet 3 | Octet 2 | Octet 1 |

CLASSE A : 0 (7BITS RESEAU/24 HOTE)

CLASSE B : 10 (14BITS RESEAU/8 HOTE)

CLASSE C : 110 (21BITS RESEAU/16 HOTE)

CLASSE D : 1110 (28BITS RESEAU)

|  |
| --- |
|  |
| Classe | Réseaux Privés |
| A | 10.0.0.0 |
| B | 172.16.0.0 à 172.31.0.0 |
| C | 192.168.0.0 à 192.168.255.0 |

Adresse DU RESEAU

|  |
| --- |
|  |

ADRESSE DE L’HOTE

Adresse privée (non visible sur le net)

Adresse public (routable, visible sur le net)

IPV6 a été créé pour faire face une pénurie d’adresse public.

Adresse finissant par ***0*** représente le ***réseau***

***Broadcast*** → diffusion

***Unicast*** → point à point

***0000*** HOTE INCONNU

***0001*** PREMIER HOTE SUR LE RESEAU

***255.255.255.255*** TOUS LES RESEAUX

***Masque de sous réseau***

|  |  |  |
| --- | --- | --- |
| ***CLASSE*** | ***Masque de sous réseau*** | ***Nb octets pour l’hôte*** |
| ***A*** | 255.0.0.0 | 3 |
| ***B*** | 255.255.0.0 | 2 |
| ***C*** | 255.255.255.0 | 1 |

Adresse 32bits bloque ou masque une partie de l’adresse IP. Permet de savoir si une adresse est sur un réseau local ou distant. Par défaut de base mais peuvent être personnalisé. LE masque permet de déterminer si un paquet est destiné à un hôte local ou distant.

Adressage CIDR (classless inter-domain Routing)

Adressage sans classe

Plutôt que de noter adresse/masque

Adresse/préfixe

Ex : 192.168.0.1/24

***EXERCICE***:

80.129.202.65/19

255 255 224(128+64+32) 0

***ET***

1111 1111 1111 1111 1110 0000 0000 0000

80. 129. 202. 65

0101 0000 1000 0001 1100 1010 0100 0001

0101 0000 1000 0001 1100 0000 0000 0000

80. 129. 192. 0

***Les sous réseaux***

172. 16. 78. 250

1010 1100 0001 0000 01001110 111 1010

255. 255. 254. 0

1111 1111 1111 1111 1111 1110 0000 0000

1010 1100 0001 0000 0100 1110 0000 0000

2^7 sous réseaux = 128

510 par sous réseaux

172.16.78.1 premier adresse

193.1.1.0/24 25 HOTES ET 6 SOUS RESEAUX

255. 255. 255. 224

1111 1111 1111 1111 1111 1111 1110 0000

(2^5) -2 = 30 machines et 8 sous réseaux (2^3=8)

193.1.10.0/24

Définir 10 sous réseaux

Nb hôte par sous réseaux ?

2^4 = 16

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sous/réseau | Sous réseau en binaire | Adresse s/r en décimal point | 1 hôte | Dernier hôte | Adresse broadcast |
| 193.1.10.0 à193.1.10.15 | 0000 | 193.1.10.0 | 193.1.10.1 | 193.10.1.14 | 193.1.10.15 |
| 193.1.10.16 à 193.1.10.31 | 0001 | 193.1.10.16 | 193.1.10.17 | 193.1.10.30 | 193.1.10.31 |
| 193.1.10.32 à193.1.10.47 | 0010 | 193.1.10.32 | 193.1.10.33 | 193.1.10.46 | 193.1.10.47 |
| 193.1.10.48à193.1.10.63 | 0011 | 193.1.10.48 | 193.1.10.49 | 193.1.10.62 | 193.1.10.63 |

193 .1 .10 .0

1000 0001 0000 0001 0000 1010 0000 0000

255 .255 .255 .240

1111 1111 1111 1111 1111 1111 1111 0000

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Site ou liaison | Adresse réseau | Masque de sous-réseau | Masque sous réseaux | Nombre hôtes | Pas de |
| Marseille | 195.10.228.0 | 255.255.255.128 | 1000 0000 | 126  | 128 |
| Salon | 195.10.228.128 | 255.255.255.224  | 1110 0000 | 30 | 32 |
| Aix | 195.10.228.160 | 255.255.255.224 | 1110 0000 | 30 | 32 |
| Arles | 195.10.228.192 | 255.255.255.224 | 1110 0000 | 30 | 32 |

*12/10/2018* :

192.168.110.0 / 24 (255.255.255.0)

→ Créer 16 sous réseaux et déterminer le nombre de machine par sous réseaux.

192 .168 .110 .0

1100 0000 1010 1000 0110 1110 0000 0000

255 .255 .255 .0

1111 1111 1111 1111 1111 1111 0000 0000

1100 000 1010 1000 01101110 0000 0000

2^4 -2 = 16-2 = 14IP

Le Pas est de 16. Donc le masque de sous réseau et le suivant :

1111 1111 1111 1111 1111 1111 1111 0000

Et 14 machines par sous réseaux.

NEW → 255.255.255.240

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| N° S/R | Sous/réseau | Sous réseau en binaire | Adresse s/r en décimal point | 1 hôte | Dernier hôte | Adresse broadcast |
| 1 | 192.168.110.0A 192.168.110.15 | 0000 | 192.168.110.0 | 192.168.110.1 | 192.168.110.14 | 192.168.110.15 |
| 2 | 192 .168.110.16 A 192.168.110.31 | 0001 | 192 .168.110.16 | 192 .168.110.17 | 192 .168.110.30 | 192 .168.110.31 |
| 3 | 192 .168.110.32 A 192.168.110.47 | 0010 | 192 .168.110.32 | 192 .168.110.33 | 192 .168.110.46 | 192 .168.110.47 |
| 4 | 192 .168.110.48 A 192 .168.110.63 | 0011 | 192 .168.110.48 | 192 .168.110.49 | 192 .168.110.62 | 192 .168.110.63 |

172.16.0.0/16 (255.255.0.0)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| N° S/R | Sous/réseau | Sous réseau en binaire | Adresse s/r en décimal point | Masque de S/R | 1 hôte | Dernier hôte | Adresse broadcast |
| 1 | 172.16.0.0A 172.16.15.0 | 0000 | 172.16.0.0 | 255.255.240.0 | 172.16.0.1 | 172.16.15.254 | 172.16.15.255 |
| 2 | 172.16.16.0 A 172.16.31.0 | 0001 | 172.16.16.0 | 255.255.240.0 | 172.16.16.1 | 172.16.31.254 | 172.16.31.255 |
| 3 | 172.16.32.0 A 172.16.47.0 | 0010 | 172.16.0.32.0 | 255.255.240.0 | 172.16.32.1 | 172.16.47.254 | 172.16.47.255 |
| 4 | 172.16.48.0 A 172.16.63.0 | 0011 | 172.16.48.0. | 255.255.240.0 | 172.16.48.1 | 172.16.63.254 | 172.16.63.254 |

→ Créer 12 sous réseaux.

2^4=16-2=14ip → NEW → 255.255.240.0

2^12 =4096 – 2 + 4094 machines par sous réseaux.

171.16.0.0 /16 (255.255.0.0)

NEW → 255.255.255.240 2^4=16-2=14 hôtes

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| N° S/R | Sous/réseau | Sous réseau en binaire | Adresse s/r en décimal point | Masque de S/R | 1 hôte | Dernier hôte | Adresse broadcast |
| 1 | 171.16.0.0A 171.16.0.15 | 0000 | 171.16.0.0 | 255.255.255.240 | 171.16.0.1 | 171.16.0.14 | 172.16.0.15 |
| 2 | 172.16.0.16 A 172.16.0.31 | 0001 | 172.16.16.0 | 255.255.255.240 | 172.16.16.1 | 172.16.16.30 | 172.16.16.31 |
| 3 | 172.16.0.32 A 172.16.0.47 | 0010 | 172.16.0.0.32 | 255.255.255.240 |  |  |  |
| 4 | 172.16.0.48 A 172.16.0.63 | 0011 | 172.16.0.48 | 255.255.255.240 |  |  |  |

172.16.78.0/16 (255.255.0.0)

NEW→255.255.255.224

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| N° S/R | Sous/réseau | Sous réseau en binaire | Adresse s/r en décimal point | Masque de S/R | 1 hôte | Dernier hôte | Adresse broadcast |
| 1 | 172.16.78.0 A172.16.78.31 | 0000 | 172.16.78.0 | 255.255.255.224 | 172.16.78.1 | 172.16.78.30 | 172.16.78.31 |
| 2 | 172.16.78.32 A172.16.78.63 | 0001 | 172.16.78.32 | 255.255.255.224 | 172.16.78.33 | 172.16.78.62 | 172.16.78.63 |
| 3 | 172.16.78.64 | 0010 |  |  |  |  |  |
| 4 |  | 0011 |  |  |  |  |  |

214.123.155.0 /24 (255.255.255.255)

2^1

NEW→255.255.255.128

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| N° S/R | Sous/réseau | Sous réseau en binaire | Adresse s/r en décimal point | Masque de S/R | 1 hôte | Dernier hôte | Adresse broadcast |
| 1 | 214.123.155.0 A 214.123.155.127 | 0000 | 214.123.155.0  | 255.255.255.128 | 214.123.155.0 | 214.123.155.126 | 214.123.155.128 |
| 2 | 214.123.155.128A214.123.155.255 | 0001 | 214.123.155.128 | 255.255.255.128 | 214.123.155.128 | 214.123.155.254 | 214.123.155.255 |

***Support des services et des serveurs :***

***DHCP =*** Récupération d’une adresse IP automatique

Le protocole DHCP permet de centraliser sur un serveur et de distribuer les paramètres TCP/IP nécessaires aux stations qui feront la demande :

 -L’adresse IP/Masque de S/R

 -La passerelle par défaut

 -L’adresse des serveurs DNS

 -Etc…

La recherche d’un serveur DHCP se fera à l’aide d’une diffusion (broadcast).

Principe de fonctionnement D.O.R.A

* DHCP Discover est une trame de Niv 2 du modèle OSI. La diffusion est effectuée à l’aide du protocole UDP. Port 67 en tant que client BOOTP.
* DHCP Offer → offre d’adresse ip, envoyer la proposition dans une trame à l’adresse mac du client. A l’intérieur de la trame adresse → ip proposé, masque, durée du bail, adresse ip du serveur qui a fait la proposition et éventuellement DNS et Passerelle
* DHCP Request c’est l’acceptation d’une proposition. Le client répond à l’offre par broadcast. Cela permet d’informer les autres serveurs des choix faits par le client (adresse ip/masque…)
* DHCP ACK C’est une confirmation du fonctionnement de l’adresse ip. Information visible ipconfig /all
* DHCP NACK expiration du bail →retrait des paramètre tcp/ip par le serveur

Le client doit donc recommencer toute la procédure pour obtenir une adresse ip.

Les serveurs n’ont pas le droit d’avoir des adresse ip dynamique (DHCP)

169.254 APIPA adresse private internet =adresse privée proposé mais aucuns serveurs de contactable

Commandes utiles : Net stop dhcp server

 Net start dhcp server

09/11/2018 :

***L’Agent relais DHCP :***

 Agent relais DHCP Les clients DHCP reçoivent leur config TCP-IP par broadcast.

Dans le cas de l’existence d’un routeur reliant plusieurs segments réseaux les diffusions seront stoppées par le routeur, il faudra envisager la présence d’un serveur DHCP par segment.

Cette contrainte peut être détournée en faisant jouer le rôle d’agent relais DHCP à un serveur ou un routeur.

***Fonctionnement du relais DHCP :***

* Le client envoi la diffusion DHCP Discover
* Le relais DHCP intercepte la requête et modifie l’entête ip afin de l’envoyer en unicast à destination d’un serveur DHCP présent de l’autre côté du réseau pour que le paquet puisse traverser le routeur.
* Le serveur DHCP puise dans l’étendue correspondant au réseau appartenant à l’agent relai DHCP et envoi une requête DHCP offer en unicast au relais DHCP.
* Le relais DHCP diffuse alors en broadcast le DHCP offer.
* Le relais DHCP envoie à son tour une requête DHCP request toujours en broadcast.
* Le relais DHCP retourne cette requête en unicast au serveur dhcp et recevra un dhcp ack du serveur.
* Le relais envoi ensuite en broadcast l’ack afin que le client puisse en prendre connaissance.

Ip helper-address X.X.X.X

Show ip interface brief

***Ajouter le rôle*** :

* Service de stratégie et accès réseau
	+ Service routage et accès distant
		- Configuration et Activation du routage
		- Ajout du nouveau protocole (agent relais DHCP)
		- Choisir l’interface d’écoute
		- Indiquer l’adresse du serveur DHCP à contacter

Service → service routage → service intervient

***Activer le routage*** :

* Routage et accès distant → clique droite configurer et activer le routage (il monte les routes directement connecter.
* Configuration → configuration personnalisée
* Cocher « Routage réseau »
* Sélectionner « Agent relais DHCP »

1 – Ajouter une carte réseau

2 – Ajout d’un rôle : rôle → Service de stratégie et accès réseau (suivant, suivant, service de routage et accès distant, suivant, installation)

***Création des étendues*** :

1 – Nouvelle étendu : définition de la plage → définition des exclusion (1-10) → non → suivant → Clique droit : « activer » → Option d’étendu : 003 (ex : 172.16.78.254)

Clique droit → Activer/Désactiver le routage → console suivante : « Routage réseau »

Clique droit → Nouveau Protocole de routage → Agent de relais DHCP

7/12/2018 :

***Le DNS (Domain Name System)***

* Evolution du NetBios toutefois les deux cohabitent.
* DNS ( systèmes de nom de domaine) → surf sur internet et même en local (maintenant pour faire fonctionner les application) ensuite sera en communication vers d’autre DNS externe.
* Résolution de nom : service permettant de traduire un nom de domaine en adresse ip de machine portant ce nom.
* Nom pleinement qualifier représente l’url.

Certaine apk utilise le nom des machines = Sony

Alors que d’autres les noms d’internet ou d’hôtes comme : sony.jf-formation.fr

***Trois étapes :***

* Consultation du cache DNS
* Serveur WINS → il fait uniquement de la résolution NetBios.
* Consultations du fichier LMHOSTS (Lan Manager Hosts) : il permet de faire un Mappage statique (nbtstat -r et nbstat -R pour vider le cache)

Dans le monde NetBios deux solutions de résolutions possibles :

* Serveur WINS ou fichier LMHOSTS

Pour internet il existe deux solutions similaires :

* Serveur DNS ou fichier host : possible d’effectuer un ping avec FQDN (Full qualified domain name) plutôt que l’adresse ip

Exemple : commande ping à tester : ping sony ; ping

Définition : Le réseau internet de part sa taille est composé d’une racine (le sommet) et de 13 serveurs qui gèrent la racine de l’internet.

Ces 13 serveurs racines ont une connaissance exacte des serveurs gérant le niveau inférieur, que l’on appelle le premier niveau.

Racines (TLD) Top level domain ou GTLD des générique.

ccTLD : country code Top Level Domain environ 250

Organisme qui gère internet ICANN, l’afnic et internic en France.

Mécanisme de délégation d’une zone

Les màj DNS sont basé sur la délégation de zones.

Les types de requêtes :

Les requêtes récursive (en local) : Le serveur ayant reçu cette requête s’engage à résoudre le nom recherché à la place du client.

 Ce type de requête doit absolument aboutir à :

 Une réponse positive dans le cas ou le serveur a réussi à résoudre le nom, négative dans le cas contraire.

Les requêtes Itérative : lorsqu’un serveur reçoit une requête itérative , il répond au client(généralement un autre serveur dns) soir par l’adresse i du nom recherché soir par l’adresse ip d’un serveur pouvant aider à résoudre ce nom.

Généralement un client utilisera une requête récursive vers un serveur DNS local puis ce dernier utilise des requêtes itératives afin de résoudre le nom du client.

UDP 53

9.9.9.9

Commandes de bases :

* Ipconfig /displaydns
* Ipconfig /flushdns (vidage du cache)
* Ipconfig /registerdns (pour enregistrer la zone inversée)

Autres commandes :

* Permettent de démarrer et arrêter le client DNS
* Net stop dnscache
* Nat start dnscache
* Net stop dns
* Net start dns
* Utilitaire NSLOOKUP :

Permet de tester le fonctionnement d’un serveur dns

 C:\>nslookup -option ordinateur\_à\_chercher Serveur\_dns\_à\_utiliser

* Utilitaire TCP-IP :Tracert et ping

C:\tracert sony.jf-formation.fr

Deux zones à créer pour un dns pour que le serveur dns ai autorité.

Les principales types de zones :

* Zone principale standard : fichier texte en .dns le serveur possède un accès en lecture écriture.
* Zone secondaire standard : copie en lecture seul du fichier.
* Zone Inversée : utilisé pour retrouver le nom d’hôte à partir de l’adresse ip. (ex : ping -a).

Enregistrement type a pour les machines dans la zone de recherche directe.

NS → serveur de noms : grâce à lui que l’on peut faire de la délégation.

Autres Zones :

* Enregistrement de type SRV pour identifier les serveurs.
* Enregistrement de type MX pour les serveurs de messagerie.

Pointeur PTR équivalent de A ptr pointe sur A qui pointe(mappe) sur PTR.

Pour qu’un serveur soit opérationnel il faut 3 élément de bases :

* SOA
* NS
* A

Ne pas oublier le suffixe dns sur le poste et le serveur : Il faut bien modifier dans les propriétés du serveur le nom de l’ordinateur puis dans autre déclarer la zone dans laquelle on va déclarer la machine.

* ***Serveurs DNS secondaire : tolérance de pannes***

Source de nom (SOA) Source of Authority :

* Chaque dns en possède ;
* Premier enregistrement lors de la création d’une zone ;
* Il gère le mécanisme de transfert de zone ;
* N° de série : utiliser pour gérer les transfert de zone ;
* Serveur Principal ;
* Intervalle d’actualisation ;
* Durée de vie maximale.
* Transfert de zone IXFR (I : Incrémentiel) : seule les modifications seront transférées dans le secondaire.
* Transfert de zone :
	+ Options de paramétrages :
		- Vers n’importe quel serveur ;
		- Uniquement vers les serveurs listés dans l’onglet Serveur de Nom (la plus pro) ;
		- Uniquement vers les serveurs suivants : avec adresse ip listée.
1. Installer service DNS ;
2. Deuxième serveur doit pointer sur le serveur 1 ;
3. Modifier le nom et la zone ;
4. Paramétrer les zone direct et inversée en secondaire avec un serveur dns maître.
5. Retour sur le srv principal pour direct et inversé : clique droit SOA → transfert de zone → cocher uniquement vers les serveurs suivant → entrer l’adresse ip du serveur secondaire.
6. Retour sur le secondaire et actualiser.
7. Modifier le dns auxiliaire sur le poste client.
* ***Délégations et redirecteurs :***

Création d’un domaine et d’un sous domaine.

 Js-formation.fr : comme premier espace de nom

 Enfant.js-formation.fr : comme second espace de nom

Un seul serveur autorisé pour la résolution des noms.

Paramétrer 2 DNS :

1. Installer 2 serveurs ;
2. Mettre une ip serveur et dns fixe pour chacun ;
3. Installer 2 machines win 10 une pour chaque DNS ;
4. Mettre une zone pour chaque serveur que l’on rentre également sur chaque machine ;
5. Créer les zones dans les paramètres DNS ;
6. Faire une ipconfig /registerdns sur le serveur et le poste ;
7. Sur serveur 1 paramétrer une nouvelle délégation pour chaque zone avec l’ip du serveur 2 ;
8. Créer une redirection vers le serveur 1 sur le serveur 2 ;

# VLAN et Commutateurs (Switch)

*18/01/2019 :*

Segmenter le réseau en sous réseau pour assurer une sécurité. Association de groupe d’utilisateur par VLAN. Le commutateur segmente les domaines de collision, et maintient un seul domaine de diffusion. Création de domaines de diffusion indépendant les uns des autres. Une trame de diffusion (broadcast) émise par une carte réseau associée à un VLAN sera transmise à toutes les cartes réseau composant ce VLAN et uniquement à celui-ci.

1. Les Avantages

 -réduction des messages de diffusion (notamment les requêtes ARP) limités à l’intérieur d’un VLAN. Ainsi les broadcast d’un serveur peuvent être limités au clients de se serveur.

 -Création de groupe de travail indépendant de l’infrastructure physique.

 -Augmentation de la sécurité parce qu’on a isoler les utilisateur dans leur domaines. Cependant on pourra toujours faire des ACL pour joindre les VLANs.

1. Les niveau des VLANs

Les VLANs permettent de séparer logiquement des ordinateurs branchés physiquement sur un switch.

Il existe différent niveau de VLANs :

 -Le niveau 1 étant basé sur les ports : Dépendant de la localisation.

 -Le niveau 2 sur les adresses MAC : VLAN indépendant de la localisation.

 -Le niveau 3 sur les adresses IP et sous réseaux.

1. Les différentes méthodes de créer un VLAN

Affecte chaque port des commutateur à un VLAN.

L’appartenance d’une carte réseau à un VLAN est alors déterminé par sa connexion à un port du commutateur

Les ports sont affectés statiquement à un VLAN.

Mode Access sur packet tracer.

1. Le protocole 802.1Q et mode Trunk

Un commutateur gère plusieurs VLANs et un VLAN peut être géré par plusieurs commutateurs.

Trame circulant entre les commutateurs = Marquage de la trame (tag) + identifiant du VLAN.

Le protocole 802.1Q marque les trames en modifiant l’en-tête MAC de la trame.

Il ajoute un identifiant de VLAN dans l’entête qui permet rapidement au commutateur d’associer la trame à un VLAN sans consulter les tables.

Mode trunk

Lorsque les VLANs sont répartis sur plusieurs commutateurs un lien particulier est mis en place entre les commutateurs.

La norme 802.1Q norme standard d’encapsulation (mode trunk).

1. Fonctionnement d’un commutateur

L’initialisation d’un switch Cisco s’effectue en 3 temps :

1. Vérification des différents éléments matériels par le programmes POST,
2. Recherche et chargement de l’IOS, on parle de fichier contenant l’IOS,
3. Recherche de la configuration de démarrage.

**(Start-Up configuration)** et chargement de cette configuration dans la RAM **(Running Configuration)**

Lors de l’étape N°3, Si aucun fichier de configuration n’est trouvé, le switch se met en mode SETUP.

1. Sources de configuration

-Le port console (source locale). Indispensable si le switch n’a pas de protocole IP configuré.

-Un terminal Asynchrone (source distante : pas SSH ou telnet et locale).

-Par le protocole IP.

-Par des serveurs TFTP qui permettent de télécharger un fichier de configuration sur le switch.

-Par des stations d’administration de réseau : au moyen d’une station SNMP comme Cisco Works ou HP Open View.

1/2/2019 :

Un vlan peut être assimilé a un domaine de broadcast.

Chaque Vlan comprend son propre sous réseau.

Sans équipement de niveau 3 impossible de communiquer entre VLAN.

Protocole ISL chez cisco équivalent du 802.1Q.

Lorsque 2 vlans veulent communiquer entre eux il faut qu’ils passent par une passerelle commune sur le routeur ou switch de niveau 3.

Trunk entre routeur-commutateur (switch). Cette connexion comprend plusieurs liens logiques : Un trafic Vlan par sous-interface, sur une liaison physique : un câble droit connectant une interface du routeur à une interface d’un commutateur.

Inter-vlan on stick.

Trafic de vlan supporté par une sous interface du routeur. Attribution d’une adresse IP pour chaque sous interface et précisé l’encapsulation utilisé par vlan.

Les hôtes peuvent communiquer entre eux même s’ils ne sont pas sur le même vlan.

Envoi d’une trame pour destination d’un sous réseau différent le switch encapsule et l’envoi a la passerelle par défaut.

Apres avoir traversé le trunk traitée au niveau routeur. Il désencapsule puis réencapsule.

Faire un ip helper pour faire un relais ;

Agrégation de route :

Regarder ce qui est commun entre les sous réseau et nous donne le sur réseau pour simplifier la table de routage.