WANQUESTIONS

Q1 : Internet c'est quoi ?

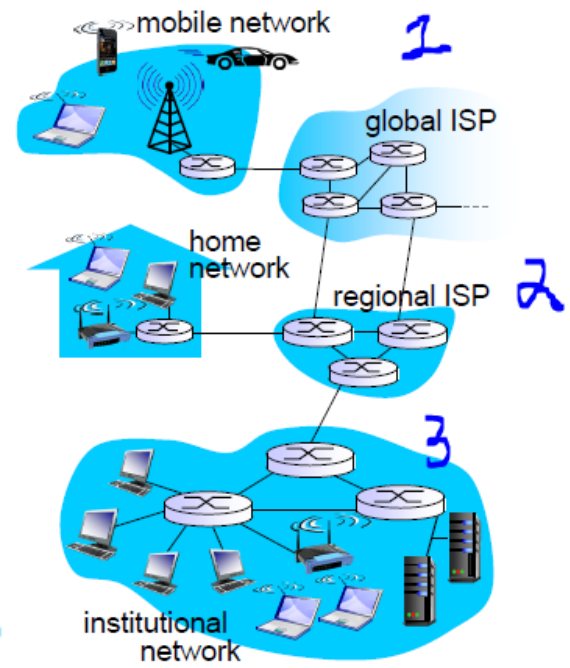
Expliquer l'infrastructure de l'Internet selon les points suivants :
la vue de détail : expliquer le schéma de principe de l'interconnexion de tous les composants ?

- Internet déjà c'est un ensemble d'appareils informatiques interconnectés

→ hôtes = systèmes d'extrémité

→ éxécution d'applications réseau

- liens de communication
  fibre, cuivre, radio, satellite
  taux de transmission: bande passante
- Commutateurs de paquets: transmettre des paquets (morceaux de données)
  routeurs et commutateurs
- Internet: «réseau de réseaux»
  FAI interconnectés
- protocols contrôlent l'envoi, la réception de msgs
  par exemple, TCP, IP, HTTP, Skype, 802.11
- Normes Internet
  RFC: Demande de commentaires
  IETF: Groupe de travail sur l'ingénierie Internet



1) On a un **réseau de mobiles**. Ce réseau permet la connexion de terminaux, réseau d'accès qui lui permet l'accès à un ISP qu'on donne global.

2) Nous avons un **réseau domestique**. Ce sont des réseaux qui sont implémentés sur des bases de LAN & PAN (pas tous). Chez nous la plupart sont

des LAN mais ils en existent des PAN. Ces PAN sont connectés également à des ISP càd qu'il y'a des organismes qui ont mis en place des réseaux (manifestemment des WAN) car ils permettent d'interconnecter des réseaux privés entre eux)

3) On a un **réseau d'entreprise** appeler aussi un **réseau institutionnel** dans lesquels on a des terminaux mobiles (ATTENTION ils ne se connectent pas avec la même logique que le 2). Ce sont des technologies de type LAN mais sans fils → des Wireless.

Donc, on a une série de LAN interconnectés par des routeurs, on reste dans un domaine LAN malgrès qu'il y'a du routage. On a un LAN de service.

ISP régional = un fournisseur d'accès

Les ≠ réseaux sont classés en fonction de leurs fonctionnalités

- Le 2ème & 3ème sont les 2 des architectures LAN mais de taille très différentes : la 2 a une architecture très simple → des terminaux autour d'un access point ou un commutateur intégré au routeur et ensuite une gateway/passerelle vers un réseau extérieur (un WAN avec une étendue supérieure)

Nous avons **2 catégories de réseaux :** les réseaux régionaux et globaux

Internet est un réseau de réseaux → Internet est une interconnexion des ISP

Les protocoles contrôlent l'envoi et la réception des messages (HTTP,IP,TCP,..)

Standards Internet : RFC, IETF

Infrastructure qui fournit des services aux applications.

Infrastructure qui fournit une interface de programmation aux applications.

la vue "service" : l'infrastructure offre ses services à qui / quoi et comment ? (voir comment)

Infrastructure qui fournit des services aux applications:
Web, VoIP, email, jeux, e-commerce, réseaux sociaux,...
fournit une interface de programmation aux applications
hooks qui permettent d'envoyer et de recevoir des programmes d'application

pour se «connecter» à Internet
▌offre des options de service, analogues au service postal

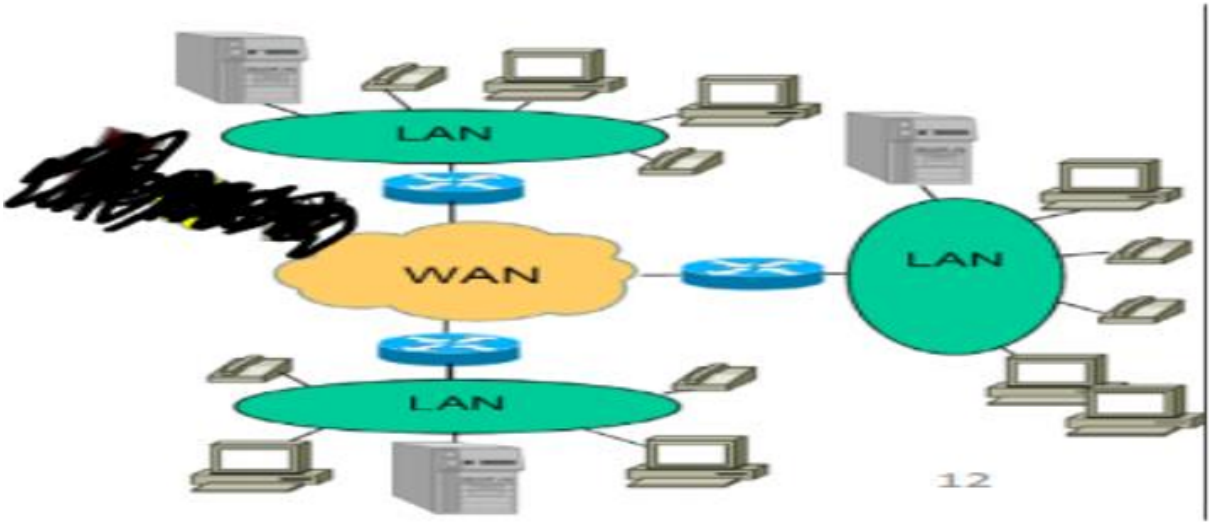
▌les relations entre Internet, les réseaux WAN et les réseaux LAN : quels sont les acteurs et quels sont les principes d'organisation ? (finir → pas complet)

Le LAN permet l'interconnexion des terminaux et le WAN l'interconnexion des LAN

Q2 : Concepts WAN

expliquer le but et le fonctionnement des wan

objectifs des WAN : expliquer à partir d'un schéma topologique de réseau d'entreprise ?



Un WAN signifie Wide Area Network,en français on peut le traduire par réseau étendu. C'est une association de plusieurs LAN. Supposons 3 LAN : le "branchement" des 3 LAN forme un WAN. Nous pourrons l'utiliser pour obtenir un seul réseau virtuel dans 2 endroits géographiquement ≠.

On peut voir qu'il est nécessaire pour se connecter au-delà des limites du réseau local,sur une zone géographique plus grande.

Les topologies WAN sont décrites à l'aide d'une topologie logique : Point-à-point, Hub and spoke, Dual-home, Fully Meshed et Partially Meshed.

Une connexion à une seule entreprise est lorsqu'une organisation se connecte à un seul fournisseur de services. Une connexion à deux transporteurs assure la redondance et augmente la disponibilité du réseau

fonctionnement ?

Le fonctionnement du WAN se fait principalement sur la couche 1 et 2

La couche 1 décrit les connexions physiques entre les réseaux d'entreprise et les réseaux de fournisseur de service. Des termes spécifiques sont utilisées pour cette liaison :

DTE,DCE,CPE,PDP,Point de démarcation,...

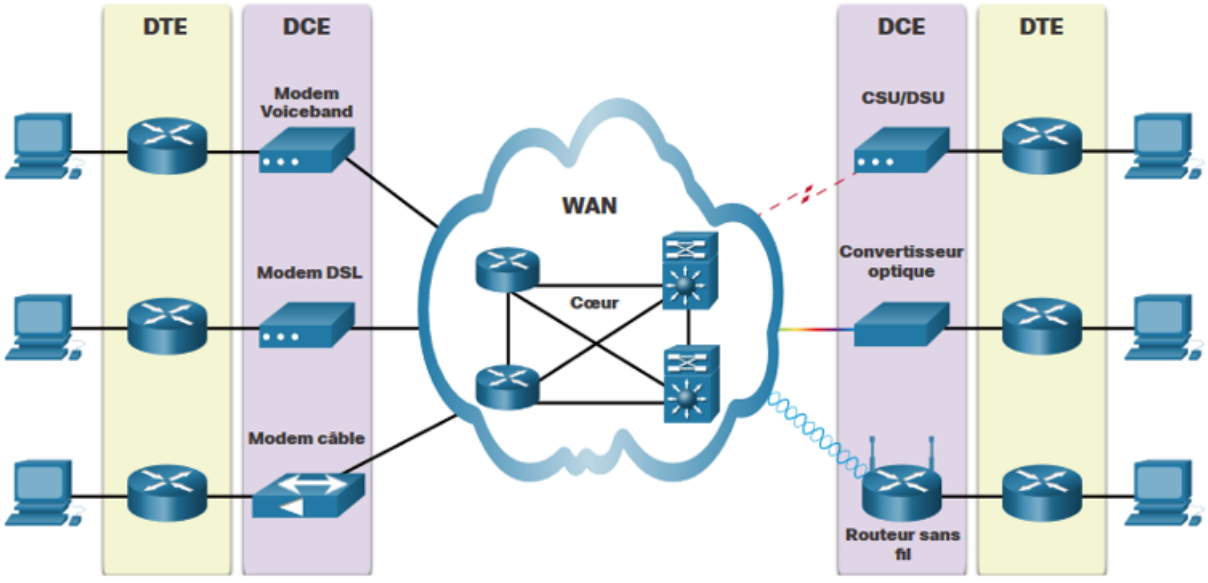
DTE : device qui permet aux employés d'être connecté au DCE et d'y envoyer du traffic. C'est un routeur mais peut aussi être serveur ou un host

DCE : device pour communiquer avec le fournisseur

CPE : s'agit du DTE et DCE de l'entreprise. Il est soit loué auprès du fournisseur soit l'entreprise en est propriétaire

POP : point où se connecte l'employé au réseau du fournisseur

démarcation point : point qui sépare l'équipement du fournisseur et du client



Les protocoles de couche 1 décrivent les composants électriques et mécaniques pour transmettre des bits sur un WAN. Les normes de protocoles de fibre optique de couche 1 incluent SDH, SONET et DWDM.

Le SDH et SONET sont 2 fibres optiques pour le transport de donnée,voix;vidéo sur de longues distances et DWDM permet d'augmenter leur capacité sur à

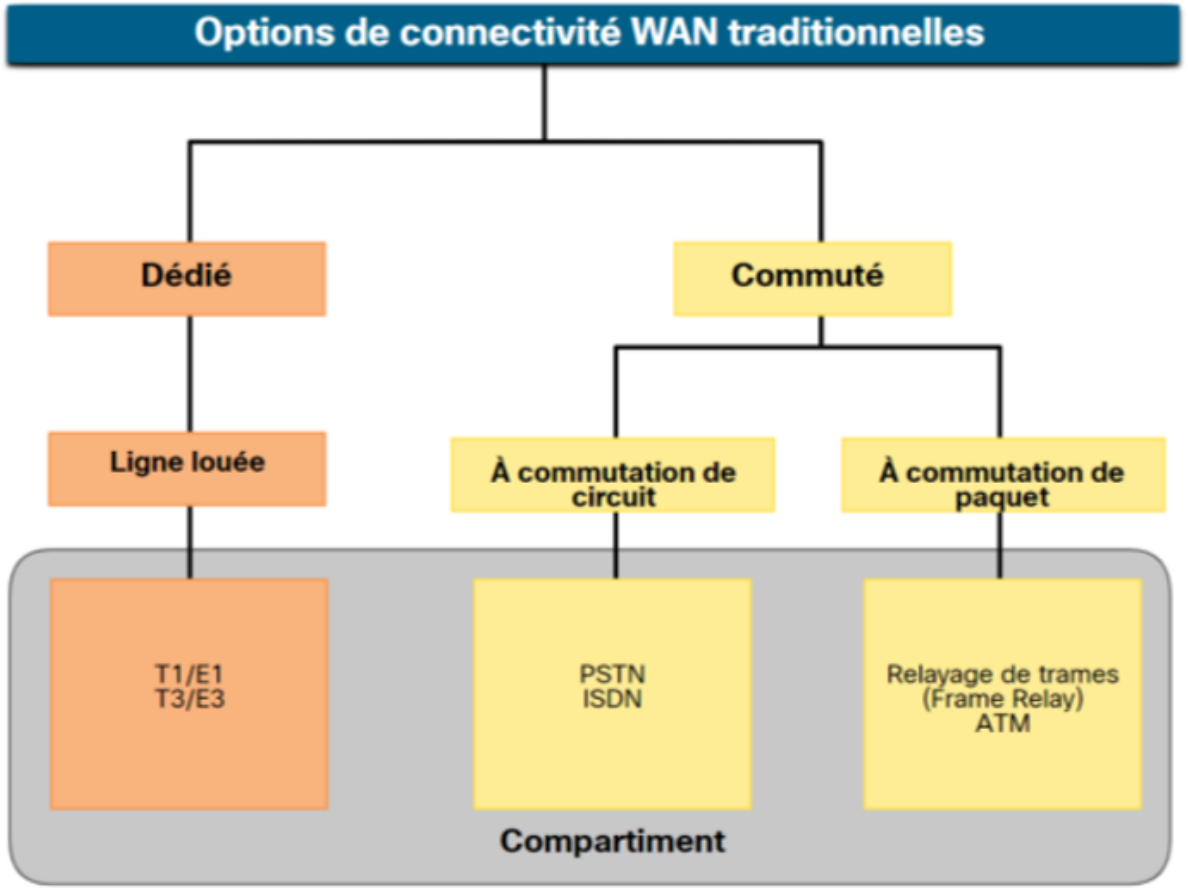
transporter l'info, ils sont utilisés dans la topologies en ring

Les protocoles de la couche 2 déterminent comment les données sont encapsulées. Ils incluent une large bande, sans fil, Ethernet WAN,MPLS,PPP,HDLC.

La communication en série transmet des bits de manière séquentielle sur un seul canal. En revanche, les communications parallèles transmettent simultanément plusieurs bits à l'aide de plusieurs fils sur des courtes distances. Pour WAN on privilégera toujours la communication en série.

❓ les différents types de connectivité ?

Connectivité WAN traditionnelle :



Les lignes réservées louées étaient des lignes T1/E1 ou T3/E3.

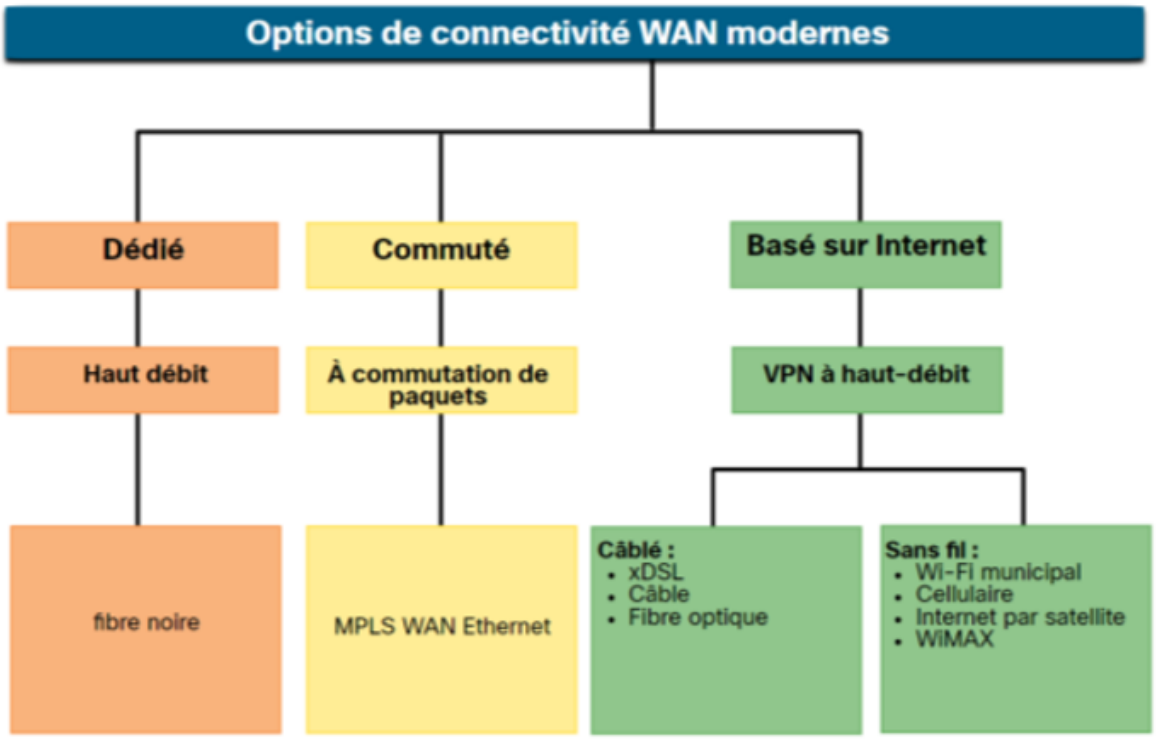
Les connexions à commutation de circuits ont été fournies par des transporteurs PSTN

Le ISDN est une technologie de commutation de circuit qui permet d'obtenir des connexions commutées de plus grande capacité que l'accès par ligne commutée.

Les réseaux à commutation de paquets permettent à plusieurs paires de noeuds de communiquer sur le même canal. Frame Relay est une technologie WAN simple de couche 2 NBMA (non-broadcast multi-access) utilisée pour connecter des LAN d'entreprises entre eux.

La technologie ATM (Asynchronous Transfer Mode) peut transférer de la voix, de la vidéo et des données sur des réseaux privés et publics. Elle s'appuie sur une architecture basée sur des cellules, plutôt que sur une architecture basée sur des trames.

Connectivité WAN moderne :



Les options de connectivité WAN modernes incluent le haut débit dédié, le WAN Ethernet et le MPLS(commuté par paquets), ainsi que diverses versions filiares et sans fil du haut débit basé sur Internet.

Haut débit dédié :

La fibre optique peut être installée indépendamment par une organisation pour connecter des emplacements distants directement entre eux. Cependant, la fibre noire peut être également louée ou achetée auprès d'un fournisseur. La location de fibres noires est généralement plus coûteuse que toute autre option WAN disponible aujourd'hui. Cependant, il offre la plus grande flexibilité,contrôle, vitesse et sécurité

A commutation de paquets :

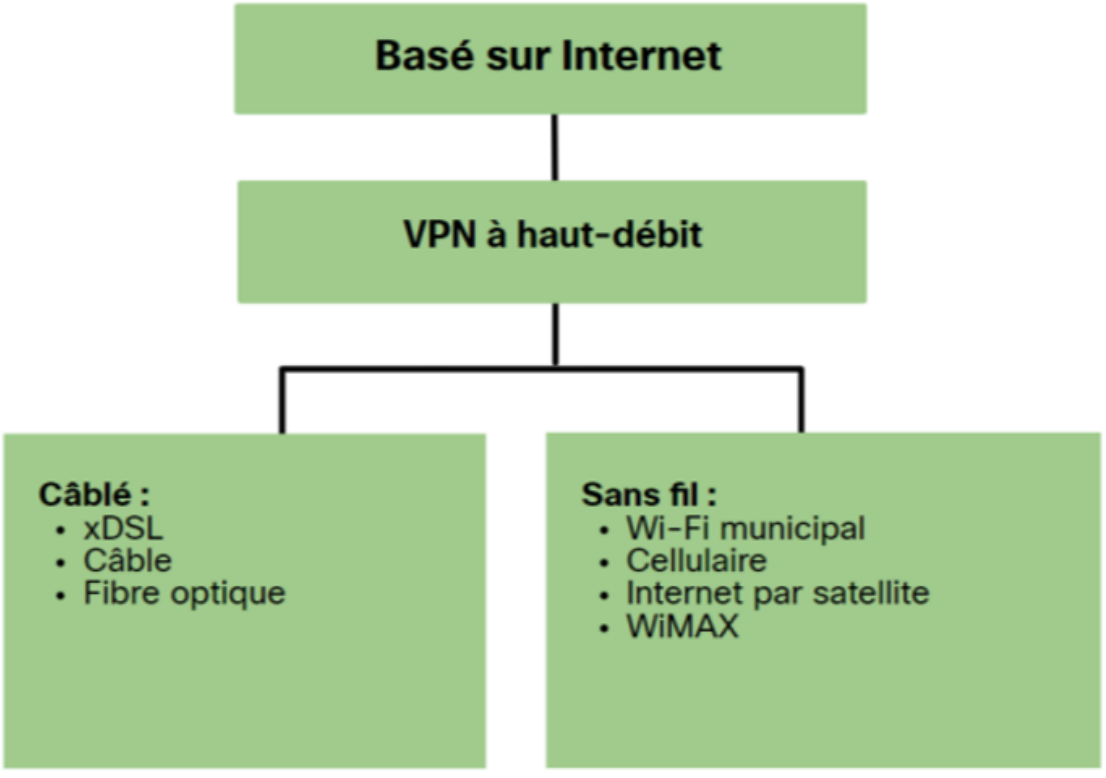
MPLS permet au réseau du fournisseur WAN de transporter n'importe quel protocole (par ex paquets ipv4,paquets ipv6,Ethernet,DSL) comme données de charge utile. Cela permet à différents sites de se connecter au réseau du fournisseur indépendamment de ses technologies d'accès

Haut débit sur Internet :

Plus que répondre aux problèmes de sécurité, les options de connectivité sont souvent combinées avec les technologies VPN.

Les options de réseau WAN valides incluent la ligne d'abonné numérique (DSL), le câble, le sans fil et la fibre optique

Connectivité basée sur Internet :



Il existe des versions câblées et sans fil de VPN haut débit

Options câblées : Les options câblées utilisent un câblage permanent (ex : cuivre ou fibre optique) pour fournir une bande passante cohérente et réduire les taux d'erreurs et la latence.

Ex de connectivité à large bande câblée : DSL, les connexions par câble et les réseaux de fibres optiques

Options sans fil : Les options sans fil sont moins coûteuses à mettre en oeuvre que les autres options de connectivité WAN, car elles utilisent des ondes radio plutôt que des supports filiaires pour transmettre des données.

Toutefois, les signaux sans fil peuvent être affectés négativement par des facteurs tels que la distance par rapport aux tours radio,les interférences provenant d'autres sources,la météo et le nombre d'utilisateurs qui accèdent à l'espace partagé.

Ex de services à large bande sans fil : 3G/4G/5G ou les services Internet par satellite.

Q3 : OSPF

Expliquer les concepts de l'OSPF :
caractéristiques du protocole OSPF ?

OSPF :

OSPF = protocole de routage à état de liens (1 lien est une interface sur un routeur) qui a pour but de déterminer la meilleure ou la route la plus rapide vers un réseau.

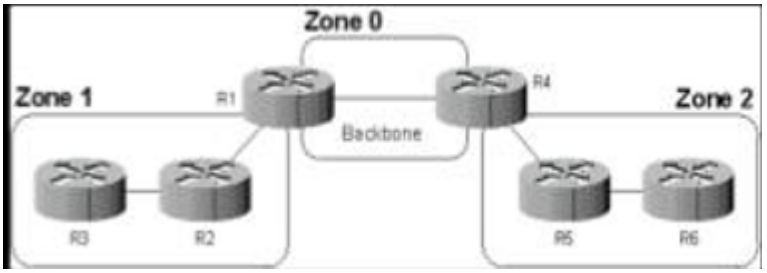
(Chaque table de routage d'un routeur est unique car chaque routeur a son point de vue, mais il y'a certaines infos que chacun doit avoir et on dit alors qu'ils sont CONVERGER, ils sont en convergeance)

Caractéristiques :

- offre une convergence plus rapide et s'adapte mieux aux réseaux de plus grande taille

- utilise une notion d'aire (ou concept de zones) qui permet de réduire le trafic réseau
- authentification possibles sous ospf
- c'est un protocole ouvert

Concept de zones :



Chaque zone identifiée par un n°, possède sa propre topologie et ne connait pas la topologie des autres zones. Chaque routeur d'une zone donnée ne connait que les routeurs de sa propre zone ainsi que la façon d'atteindre une zone particulière, la zone n°0. Toutes les zones doivent être connectés physiquement à la zone 0 (appeler backhome). Elle est constituée de plusieurs routeurs interconnectés. Le backhome est chargé de diffuser les infos de routage qu'il reçoit d'une zone aux autres zones. Tout routage basé sur OSPF doit posséder une zone 0.

contiguité = càd lien avec ces voisins

<u>présentation OSPF :</u>

- OSPF a des avantages par rapport à RIP car il offre une convergence + rapide et s'adapte mieux aux réseaux de + grandes tailles
- protocole de routage à état de liens qui prend en charge le concept de zones pour assurer l'évolutivité
- Une liaison = interface sur un routeur, un segment de réseau qui connecte 2
  routeurs, ou un réseau stub tel qu'1 LAN Ethernet connecte à 1 routeur

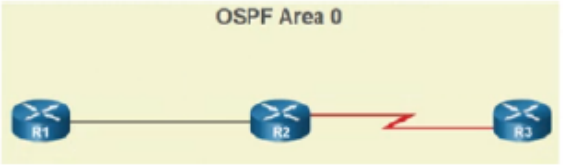
- les infos sur les états de ces liens = états des liens → ce sont une série d'infos qu'il faut récolté. Les principales sont l'@ réseau avec un subnet mask. Ttes les infos inclu le préfixe réseau,la longueur du préfixe et le coût.

On a l'OSPF à zone unique et multiple :

OSPF prend en charge le routage hiérarchique à l'aide de zones.
zone OSPF = groupe de routeurs qui partagent les mêmes infos d'état de liens dans leurs LSDB.

Le protocole OSPF peut être implémenter de 2 manières ≠ :

- zone unique : tous les routeurs sont dans une zone. Meilleure pratique → utiliser zone 0



- OSPF à zone multiples : plusieurs zones de façon hiérarchique. Toutes les zones doivent se connecter à la 0. Les routeurs qui relient les zones entre elles sont les routeurs ABR. Cela amène des avantages telles que :
  - tables de routage + petites : car il y'a moins d'entrées de table d'acheminement et est du au fait que les @ réseaux sont résumées entre les zones.
  - réduction de la charge de màj des états de liens : minimise la puissance de calcul et la mémoire requise
  - réduction de la fréquence des calculs SPF : localise l'impacte d'une modification topologique au sein d'une zone

(réseau stub = un routeur connecté à internet, il n'y en a pas d'autres)

Inconvénients :

- consomme de la mémoire, car a des bases de données pour chaque routeur (état des liens)

- Consomme de la CPU au démarrage du processus OSPF, car il doit construire sa base de données
- Protocole complexe à mettre en place

❓ composants du protocole OSPF ? (pas sure si bonne réponse)

Les routeurs exécutant l'OSPF échangent des messages pour transmettre des informations de routage en utilisant cinq types de paquets :

Les paquets sont :

1 → Hello → découvre les voisins et crée des contiguités entre eux

2 → DBD(DataBase Description) → vérifie la synchronisation de la base de données entre les routeurs

3 → LSR(Link-State Request) → demande des enregistrements d'état de liens spécifiques d'un routeur à un autre

4 → LSU(Link-State Update) → envoie les enregistrements d'état de liens spécifiquement demandés

5 → LSAck(Link-State Acknowledgment) → reconnait les autres types de paquet

Ces 5 paquets servent à détecter les routeurs voisins et à échanger des informations de routage

Les messages OSPF sont utilisées pour créer et gérer 3 bases de données OSPF :

- Base de données sur les contiguités : cela crée la table des voisins
- LSDB(link state database) : cela crée la table de topologie
- Base de données de transmission : cela crée la table de routage

Algorithme :

- Le routeur crée la table topologique à l'aide des résultats des calculs basés sur l'algorithme SPF de Dijkstra.
- L'algo SPF est basé sur le cout cumulé permettant d'atteindre une destination

- L'algo SPF crée une arborescence SPF en plaçant chaque routeur à la racine de l'arborescence et en calculant le plus court chemin vers chaque noeud
- L'arborescence SPF est ensuite utilisée pour calculer les meilleures routes
- Le protocole OSPF insère les meilleures routes dans la base de données de réacheminement, qui est utilisée pour créer la table de routage.

fonctionnement des états de lien ?

Fonctionnement de l'état des liens :

Pour mettre à jour les info de routage, les routeurs OSPF effectuent le processus
de routage à état de liens générique qui suit afin d'atteindre un état de convergence. Les étapes de routage d'état de lien qui sont effectuées par un routeur :

- établissement des contiguités de voisinage : les routeurs compatibles OSPF doivent se connaitre sur le réseau avant de pouvoir partager des infos. Un routeur compatible OSPF envoie des paquets Hello à partir des interfaces compatibles OSPF pour déterminer si des voisins se trouvent sur ces liens. Si un voisin est présent, le routeur compatible OSPF tente d'établir une contiguité de voisinage avec celui-ci
- échange d'annonces à état de liens : Une fois les contiguités établies, les routeurs échangent ensuite des annonces d'état de lien (LSA). Les LSA contiennent l'état et le coût de chaque lien connecté directement. Les routeurs transmettent leurs LSA aux voisins contigus. Les voisins contigus recevant les LSA les diffusent immédiatement aux autres voisins connectés directement,jusqu'à ce que tous les routeurs de la zone aient tous les LSA.
- créer la base de données à l'état des liens : Après réception des LSAs, les routeurs compatibles OSPF construisent la table de topologie (LSDB) sur la base des LSAs reçus. Cette base de données contient finalement toutes les infos sur la topologie de la région.
- éxécution de l'algo SPF : Les routeurs éxécutent ensuite l'algo SPF. Les engrenages dans la figure pour cette étape sont utilisées pour indiquer l'éxécution de l'algo SPF. L'algo SPF crée une arborescence SPF

- choisir la meilleure route : Une fois l'arbre SPF construit, les meilleurs chemins vers chaque réseau sont proposés à la table de routage IP. La route sera insérée dans la table de routage à moins qu'il existe une route source vers le même réseau avec une distance administrative inférieure, telle qu'une route statique. Les décisions de routage sont prises en fonction des entrées de la table de routage.

❓ Expliquer les commandes principales de configuration de l'OSPF ?

`router ospf process-id` → pour activer OSPFv2 en mode de configuration globale. La valeur process-id représente un nombre compris entre 1 et 65 535 et est sélectionnée par l'administrateur du réseau.

Les messages OSPF sont utilisés pour créer et gérer 3 bases de données OSPF :
base de données de contiguité →
`show ip ospf neighbor`
bdd d'états de liens (LSDB)→
`show ip ospf database`
bdd de réacheminement →
`show ip route`

pour activer OSPFv2 → `router ospf`

pour attribuer un id à un routeur → `router-id` *`rid du routeur OSPF`*

`network` → pour spécifier les interfaces appartenant à un réseau point à point

`ip ospf` → configurer l'ospf directement sur l'interface

`network-address wildcard-mask` → pour activer l'ospf sur les interfaces

(la syntaxe
`area area-id` fais référence à la zone OSPF. Lors de la configurat° de l'OSPFv2 à zone unique, la commande network doit être configurée avec la même valeur area-id sur tous les routeurs.)

Q.4. Concepts ACL et NAT

Expliquer les concepts ACL et NAT :
❓ Qu'est-ce qu'une ACL et à quoi peut-elle servir ?

ACL = liste de controle d'accès
= est une liste d'ACE(entrées de contrôle d'accès)

Une liste de controle d'accès = une série de commandes IOS qui déterminent si un routeur achemine ou abandonné les paquets en fonction des infos contenues dans l'en-tête de paquet.

→ Elle permet au routeur de pouvoir prendre une décision sur ce qu'il fait avec un paquet

Aucun ACL n'est configuré sur un routeur mais lorsqu'elle est appliquée sur une interface le routeur évalue en outre tous les paquets réseau lorsqu'ils traversent l'interface pour déterminer s'ils peuvent être acheminées.

Pourtant le nombre l'ACL appliquées sur une interface de routeur est limitée. L'interface d'un routeur peut avoir :

- une liste ACL sortante ipv4
- une ACL ipv4 entrante
- une ACL ipv6 entrante
- une liste ACL sortante ipv6

(On peut définir jusqu'à 4 listes)

Une ACL utilise une ACE qui est une liste de déclarations d'autorisation ou de refus. (ACE = une suite d'instructions)

> L'utilisation d'ACL nécessite beaucoup de précisions, les erreurs peuvent couter cher et se solder en pannes de réseau importantes

❓ Fonctionnement d'une ACL : niveau 3 et niveau 4 ?

Lorsque le trafic réseau traverse une interface configurée avec ACL, le routeur compare les info du paquet à chaque ACE, dans l'ordre, afin de déterminer si le paquet correspond à l'une des entrées ACE. C'est ce que l'on appelle le `filtrage de paquet.`

ACL revient à filtrer les paquets au lieu de les routeur : sur couche 3 et 4

On a 2 types d'ACL IPv4 :

- ACL standard : ces listes autorisent ou refusent les paquets basés uniquement sur l'@ ipv4 source
- ACL étendues : autorisent ou refusent les paquets basés sur l'@ ipv4 source et l'@ ipv4 de destination, le type de protocole, les ports TCP ou UDP source et destination et plus encore

ACL 1-99 ou 1300-1999 → ACL standard
ACL 100-199 ou 2000-2699 → ACL étendues

Où placer les ACL ?

doit être placer là ou elles autont le + grand impact des performances
ACL étendues → le + près de la source du trafic à filtrer
ACL standard → le + près de la destinat°

c3 : sur la source → ACL standards
c4 : on autorise certaine appli mais pas d'autres → ACL étendues

C'est au niveau de la couche 3 et 4 que nous effectuons le filtrage des paquets

Les ACL standards filtrent uniquement au niveau de la couche 3 à l'aide de l'@ ipv4 source uniquement

Les ACL étendues : FiltreACL à la couche 3 à l'aide de l'adresse ipv4 source et/ou destinat°. Ils peuvent également filtrer au niveau de la couche 4 en utilisant les ports TCP et UDP.

Fonctionnement des étapes lorsque le trafic entre et sort:

Une fois entrer dans le routeur

1. Le routeur extrait l'adresse IPv4 source de l'en-tête du paquet.
2. Le routeur commence en haut de l'ACL et compare l'adresse IPv4 source à chaque ACE dans un ordre séquentiel.
3. Lorsqu'une correspondance est établie, le routeur exécute l'instruction, soit en autorisant soit en refusant le paquet, et les ACE restants dans l'ACL, le cas échéant, ne sont pas analysés.
4. Si l'adresse IPv4 source ne correspond à aucun ACE de l'ACL, le paquet est ignoré car un ACE de refus implicite est automatiquement appliqué à toutes les ACLs.

Masque générique ?

Un masque générique est similaire au masque de sous-réseau sauf que

pr indiquer les machines dont l'adresse ip est autoriser on met le préfixe à 0 Et 1 pour l'inverse

- **Bit 0 de masque générique** - permet de vérifier la valeur du bit correspondant dans l'adresse
- **Masque générique bit 1** - ignorer la valeur du bit correspondant dans l'adresse

EXEMPLE : on a comme adresse 192.168.1.1
le subnet mask est 255.255.225.0
préfixe : 192.168.1.0 → adresse du réseau → préfixe
masque générique → indiquer ce qui peut varier dans le préfixe càd 0.0.0.255
Si on a un masque générique de 0.0.0.63 on a de 0 à 63 soit 64 possibilités

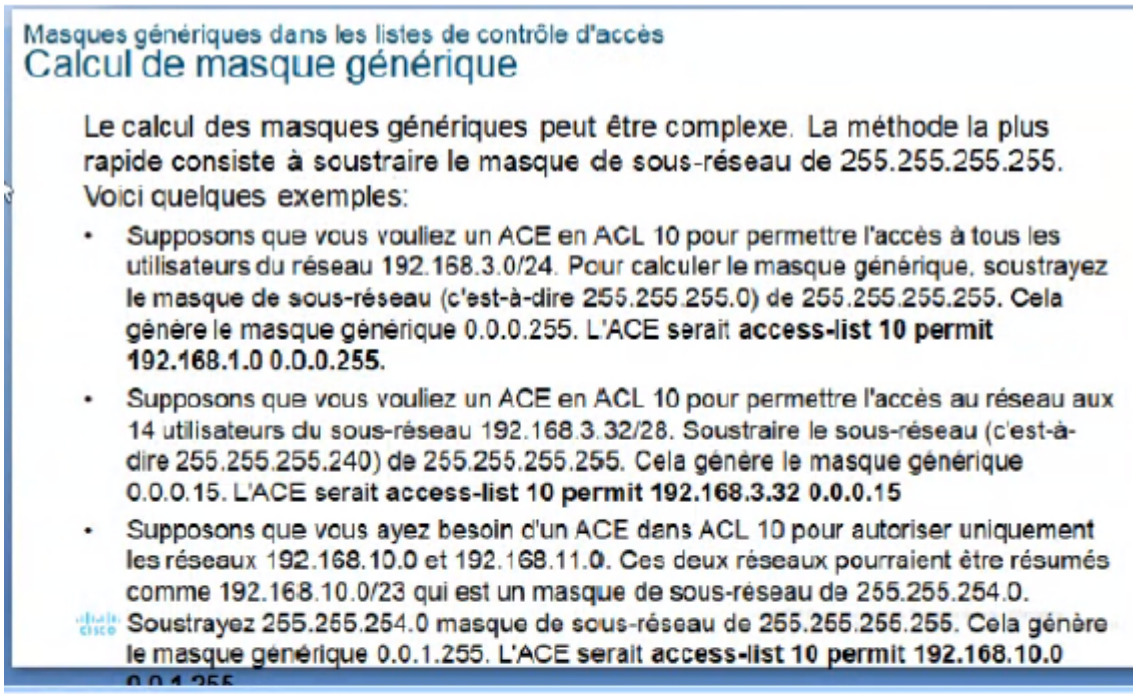
Masques génériques dans les listes de contrôle d'accès

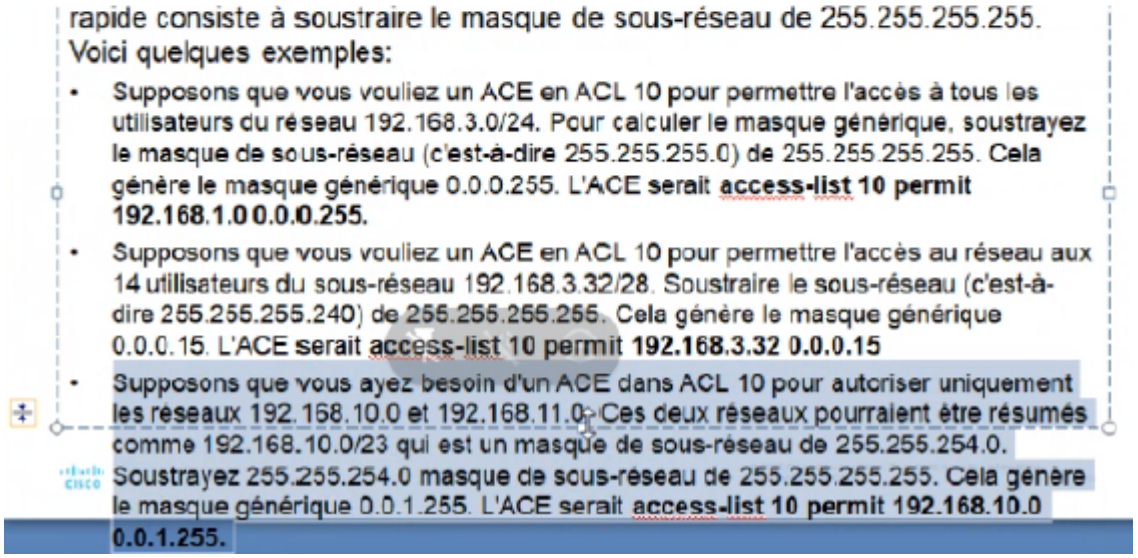
Types de masques génériques (Suite)

Masque générique pour correspondre à une plage d'adresses IPv4

- ACL 10 a besoin d'un ACE qui autorise tous les hôtes des réseaux 192.168.16.0/24, 192.168.17.0/24,..., 192.168.31.0/24.
- Lorsqu'il est traité, le masque générique 0.0.15.255 autorise tous les hôtes des réseaux 192.168.16.0/24 à 192.168.31.0/24. L'ACE résultant dans l'ACL 10 serait **access-list 10 permit 192.168.16.0 0.0.15.255.**

	Décimal	Binaire
Adresse IPv4	192.168.16.0	11000000.10101000.00010000.00000000
Masque générique	0.0.15.255	00000000.00000000.00001111.11111111
Adresse IPv4 autorisée	**192.168.16.0/24 à 192.168.31.0/24**	11000000.10101000.00010000.00000000 11000000.10101000.00011111.00000000





Voici la fourchette de réseaux que j'ai

si on connait le masque de sous réseau inverse

[192.168. 16.0/24

192.168. 31.0/24]

Maintenant il faut voir ce qui est en commun :

[192.168. 16.0/24 : 0001 0000 0000 0000

192.168. 31.0/24] : 0001 1111 0000 0000

on a 0001 même et le reste diff

[192.168. 16.0/24 : 0001 0000 0000 0000

192.168. 31.0/24] : 0001 1111 0000 0000

255.255.240.0 SNM du range d'adresses autorisées (PERMIT)

donc pr le subnet mask on met tt les mêmes bits mis à 1 → voir bleu en bas donc 240

[192.168. 16.0/24 : 0001 0000 0000 0000

192.168. 31.0/24] : 0001 1111 0000 0000

11110000

Maintenant on doit faire 255.255.255.255 - le masque obtenu càd le masque générique

255.255.255.255

255.255.240.0

0.0.15.255

🟥 Expliquer la NAT à partir d'un schéma topologique ? (manque le schéma topologique)

Toutes les machines qui ont besoin de communiquer avec internet ont besoin de ça. Le commutateur aussi parce qu'on a besoin d'administrer sinon non.

Pour qu'on puisse accéder aux ressources en dehors du réseau il faut que l'adresse privée soit traduite en adresse publique la traduction d'adresse réseau (NAT) assure donc cette traduction d'adresses privées en adresses publiques

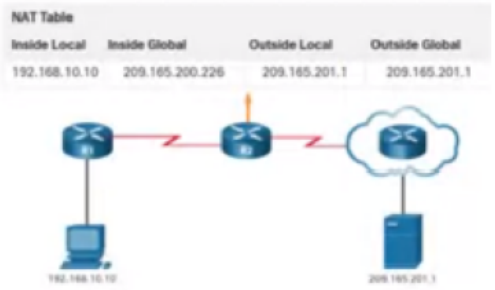
Le nat fait la passerelle entre les adresses privées et publiques.
pat = avec les ports

Nat pas un protocole mais plutôt un algorithme de traduction d'adresses. Il fait la frontière entre le réseau interne et externe(comme internet)

Explication avec un exemple :

PC1 souhaite communiquer avec un serveur Web externe dont l'adresse publique est 209.165.201.1.

1. PC1 envoie un paquet adressé au serveur Web.
2. R2 reçoit le paquet et lit l'adresse IPv4 source pour déterminer s'il a besoin d'une traduction.
3. R2 ajoute un mappage de l'adresse locale en adresse globale à la table NAT.
4. R2 envoie le paquet avec l'adresse source traduite vers la destination.
5. Le serveur Web répond par un paquet destiné à l'adresse globale interne de PC1 (209.165.200.226).
6. R2 reçoit le paquet portant l'adresse de destination 209.165.200.226. R2 examine la table NAT et trouve une entrée correspondant à ce mappage. R2 utilise ces informations pour traduire l'adresse globale interne (209.165.200.226) en adresse locale interne (192.168.10.10), et le paquet est transféré vers PC1.



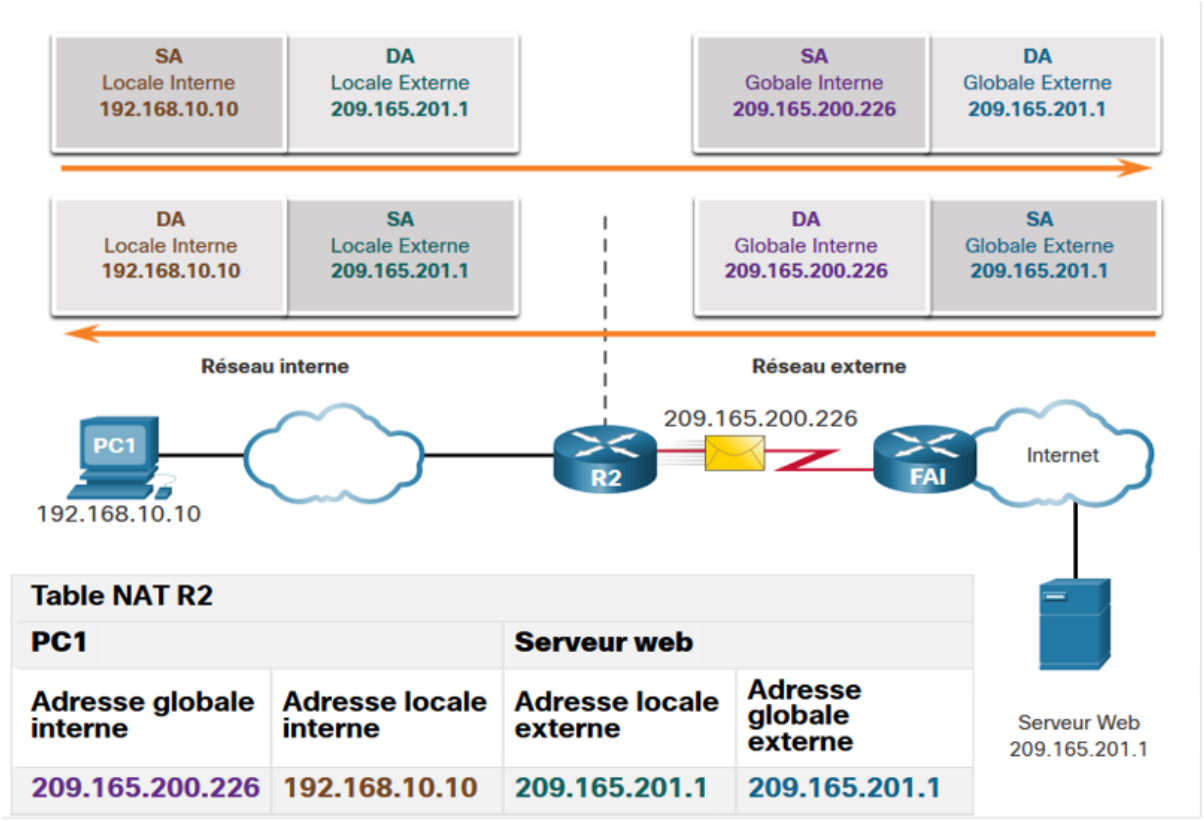


Table NAT R2			
PC1		**Serveur web**	
Adresse globale interne	**Adresse locale interne**	**Adresse locale externe**	**Adresse globale externe**
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

@ interne : l'@ du périph traduite via NAT

@ externe : l'@ du périph de destinat°

@ locale : peut faire référence à toute @ qui apparait sur la partie interne du réseau

@ globale : peut faire référence à tte adresse qui apparaît sur la partie externe du réseau

❓ Quels sont les différents types de NAT ?

- **NAT statique :**

utilise le mappage 1 à 1 des @ locales et globales configurées par l'administrateur réseau qui restent constantes. Elles servent aussi aux périphériques qui doivent être accessibles à distance par le personnel autorisé, mais pas par tous les utilisateurs d'internet

⚠

le nat statique nécessite qu'il existe suffisamment d'@ publiques dispo pour satisfaire le nb total de sessions utilisateurs simultanées

On a besoin d'une adresse IP permanente

On peut utiliser plusieurs systèmes de natting en même temps

Nécessite assez d'@ publiques dispo pour satisfaire le nb total de session utilisateur simultanés.

- **NAT dynamique :**

utilise un pool d'@ publiques et les attribue selon la méthode du 1er arrivé, 1er servi.

C'est le même fonctionnement que le nat statique sauf que l'adresse publique partager ne sera pas toujours la même elle sera prise dans un pool d'adresses à la disposition d'un routeur pour un temps déterminer

- **PAT (traduction d'adresses de port):**

variante du nat dynamique

aussi appellé surcharge NAT, mappe plusieurs adresses ipv4 privées à une seule @ ipv4 publique ou à quelques adresses en utilisant des ports

Différence entre pat et nat → le nat modifie uniquement les @ipv4 et que le pat modifie à la fois l'@ ipv4 et le n° de port.

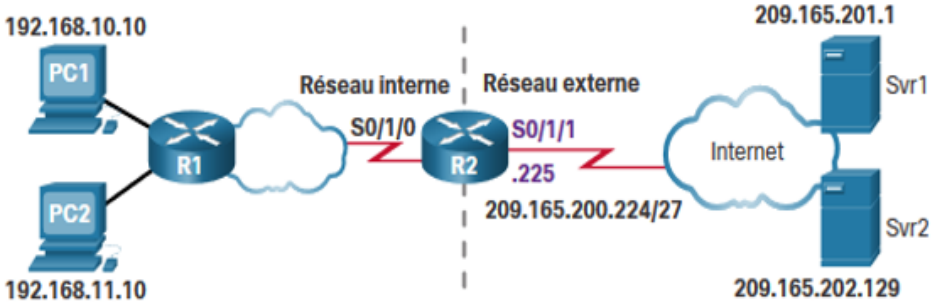


Table NAT			
Adresse locale interne	**Adresse globale interne**	**Adresse globale externe**	**Adresse locale externe**
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.11.10:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

Avantages de la nat :

- augmente la souplesse des connexions au réseau public
- cache les @ipv4 des utilisateurs et autres périphériques
- conserve le schéma des @ipv4 privées existant et de passer facilement à un nouveau schéma d'adressage public

Inconvénients de la nat :

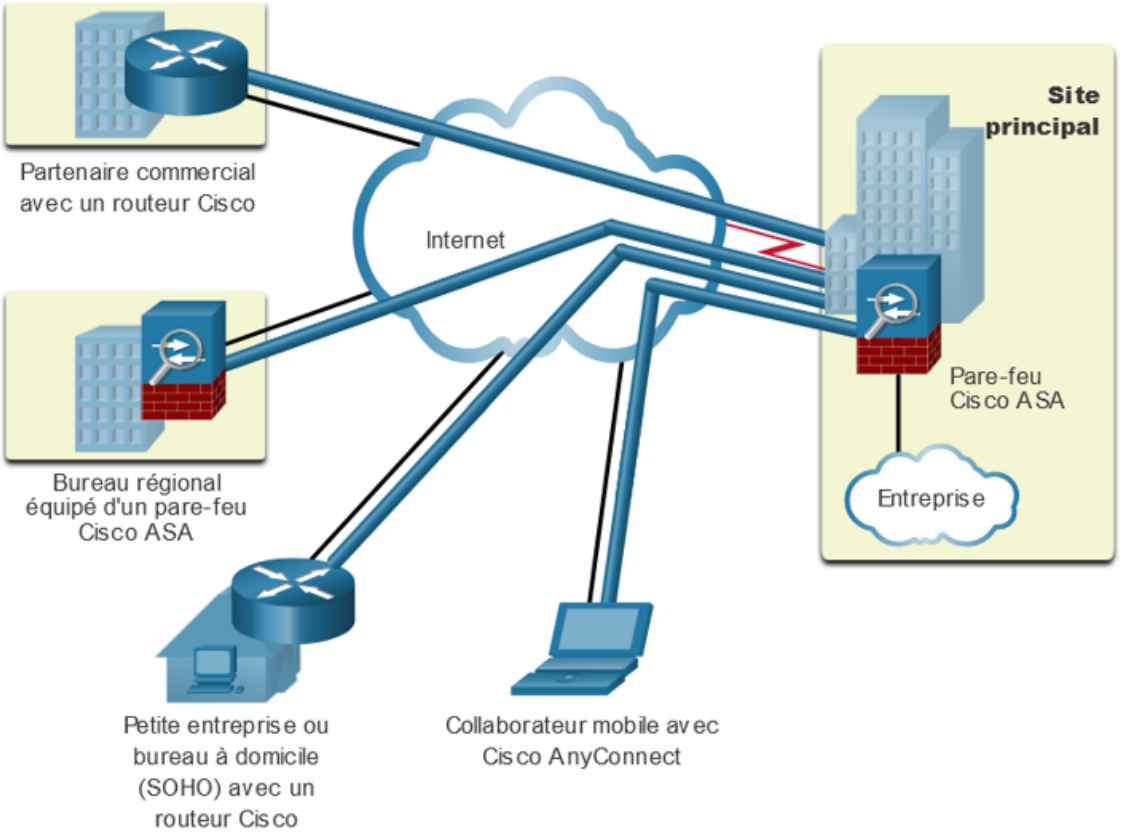
- augmente le délai de transfert
- l'@ssage de bout en bout est perdu
- perte de la traçabilité ip de bout en bout

Q.5. Concepts VPN (lire notes en + avec)

Expliquer les concepts de VPN :
❗ pourquoi les VPNs ?

Les VPN sont là pour créer des connexions de réseau privé de bout en bout. Un VPN est privé càd que le trafic est chiffré pour assurer la confidentialité des données pendant qu'il est transporté à travers le réseau public. Il chiffre les données et prend en charge les fonctionnalités de chiffrement comme les protocoles IPSec et SSL pour sécuriser le trafic réseau entre sites.

Le principe du vpn est de mettre un paquet ip dans un autre paquet ip (c'est ce qu'on appelle un tunnel)



Le VPN a énormément d'avantages :

- une réduction des coûts : en utilisant les VPN on réduit les coûts de connectivité tout en augmentant simultanément la bande passante de connexion à distance
- sécurité : les protocoles de chiffrement protégent les données contre les accès non autorisé
- sensibilité : les VPN permettent aux organisations d'utiliser Internet ce qui facilite l'ajout de nouveaux utilisateurs sans ajouter d'infrastructure importante
- comptabilité : les travailleurs distants peuvent utiliser ces connexions à haut débit pour accéder en toute sécurité aux réseaux d'entreprise

VPN → permet aux utilisateurs distants et mobiles de se connecter en toute sécurité à l'entreprise en créant un tunnel crypté. Les VPN peuvent être créer en utilisant IPSec ou SSL.

VPN de site à site → utiliser pour connecter des réseaux sur un réseau non fiable tel qu'internet

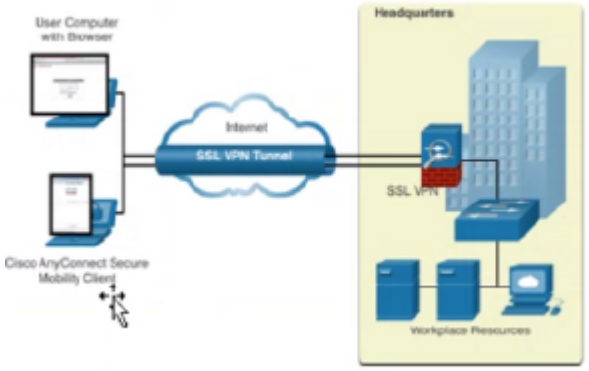
Dans un VPN site à site les hôtes finaux envoient et reçoivent le trafic TCP/IP

DMVPN est une solution logicielle Cisco pour créer facilement des VPN multiples, dynamiques et évolutifs

🚦 différents types de VPN ?

Nous avons comme type de VPN :

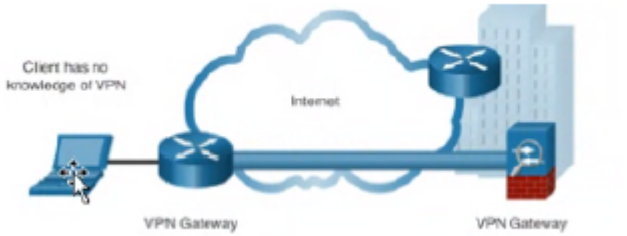
- VPN d'accès à distance : permet aux utilisateurs distants et mobiles de se connecter en toute sécurité à l'entreprise. Ces VPN sont activés dynamiquement par l'utilisateur lorsque cela est nécessaire et peuvent être créées à l'aide d'IPSec ou de SSL.



Nous avons 2 types de connexions avec ceci :

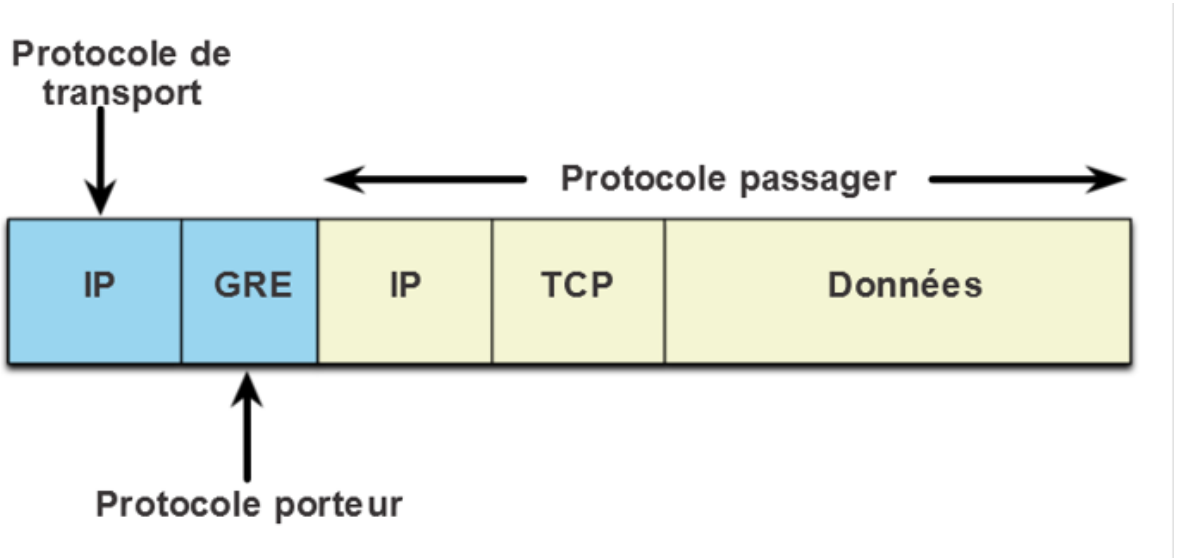
  - La connexion VPN sans client : La connexion est sécurisée à l'aide d'une connexion SSL par navigateur Web (https donc http avec un tunnel ssl)
  - La connexion VPN basée sur le client : le logiciel client VPN (tel que Cisco AnyConnect Secure Mobility Client) doit être installé sur le terminal de l'utilisateur distant
- SSL VPN's : SSL utilise l'infrastructure de clé publique et les certificats numériques pour authentifier les pairs.
- VPN IPSec site à site : connectent des réseaux sur un réseau non fiable tel qu'Internet. Les hôtes finaux envoient et reçoivent du trafic TCP/IP non chiffré normal via une passerelle VPN
  La passerelle VPN encapsule et crypte le trafic sortant d'un site et envoie le trafic via le tunnel VPN à la passerelle VPN sur le site cible. La réception de

la passerelle VPN élimine les en-têtes, déchiffre le contenu et relaie le paquet vers l'hôte cible au sein de son réseau privé

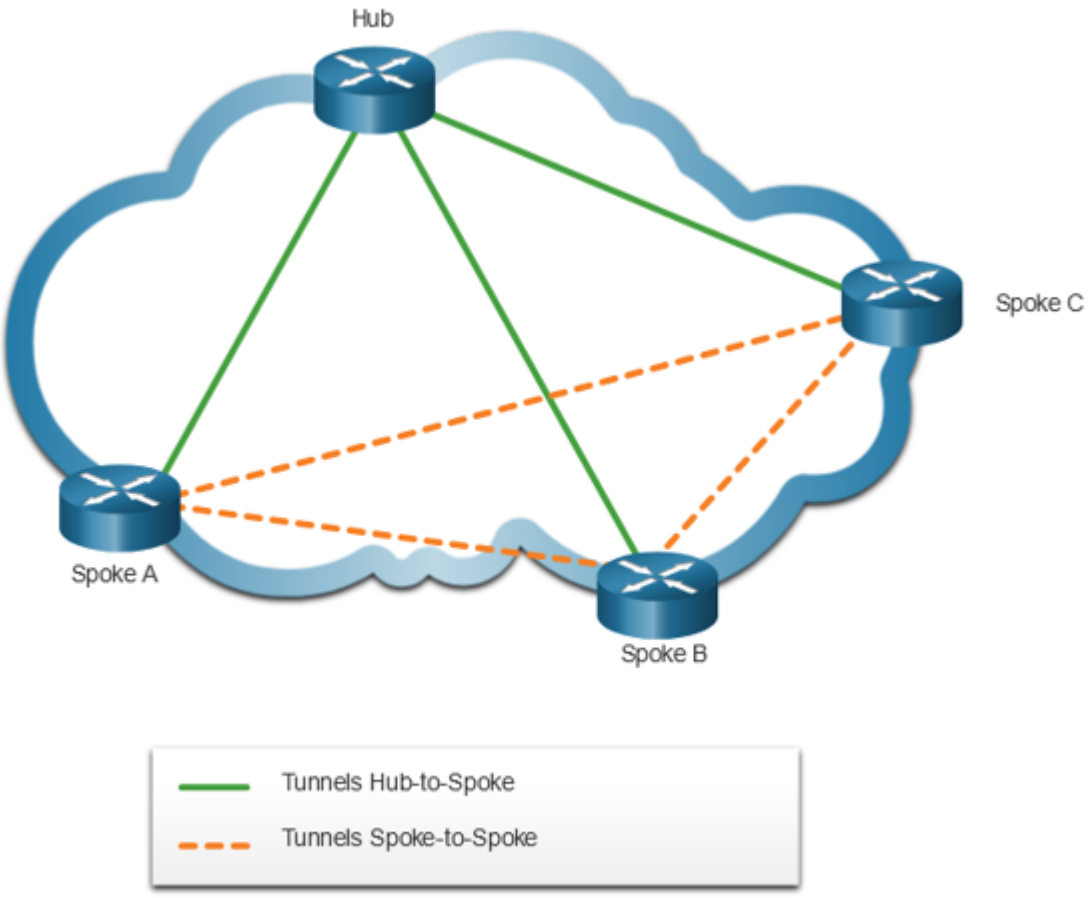


- GRE sur IPSec = protocole de tunneling VPN de site à site non sécurisé.

GRE permet au trafic du protocole de routage d'être ok car IPSec VPN est en unicast → paquet GRE dans paquet IPSec.
Les VPN IPSec standard (non GRE) ne peuvent créer que des tunnels sécurisées pour le trafic unicast. L'encapsulation de GRE dans IPSec permet de sécuriser les mises à jour du protocole de routage de multidiffusion via un VPN.



- VPN multipoints dynamiques : Facilite la mise en place de filiale grace a la methode hub to spike (site central). Utilise IPSec pour communiquer de maniere sécurisé et mGRE. GRE permet à une interface GRE (HUB) de gérer d'une manière dynamique plusieurs tunnels IPsec. Du coup si un nouveau spoke doit étre ajouté il doit juste prendre la conf du hub.



- VPN MPLS prestataires de service : on utilise maintenant dans le réseau principal MPLS où le trafic est transmis via le réseau principal MPLS à l'aide d'étiquettes. Le client est sécurisé car les clients des fournisseurs de services ne peuvent pas voir le trafic de l'autre.

MPLS peut fournir aux clients des solutions VPN gérées par conséquent la sécurisation du trafic entre les sites clients est la responsabilité du prestataire de services
Il existe 2 types de solutions VPN MPLS prises en charge par les prestataires de services :

- VPN MPLS de couche 3 : Le prestataire de services participe au routage client en établissant trunking entre les routeurs du client et les routeurs du prestataire
- VPN MPLS de couche 2 : Le prestataire déploie un service LAN privé virtuel (VPLS) pour émuler le segment LAN multi-accès Ethernet sur le réseau MPLS. Aucun routage n'est impliqué. Les routeurs du client appartiennent effectivement au même réseau à accès multiple.

Les hôtes finaux envoient et reçoivent du trafic TCP/IP non chiffré normal via une passerelle VPN. La passerelle VPN encapsule et crypte le trafic sortant d'un site et envoie le trafic via le tunnel VPN à la passerelle VPN sur le site cible. La réception de la passerelle VPN élimine les en-têtes, déchiffre le contenu et relaie le paquet vers l'hôte cible au sein de son réseau privé.

Q.6. Concepts QoS

Expliquer la QoS selon les points suivants :
❗ La QoS c'est quoi ?

La QOS signifie la qualité de service.
Les transmissions vocales et vidéos en direct créent des attentes plus élevées en matière de qualité parmis les utilisateurs et créent un besoin de qualité de service.

La voix et la vidéo sont 2 des principales raisons de la QOS.
Sur Internet nous n'avons pas de QOS car pas de priorité de paquets
La QOS = une priorité sur les trafics. Si le réseau n'est pas saturé nous n'avons PAS besoin de QOS. La QOS intervient une fois qu'il y'a saturation càd quand il y'a :

- de l'agrégation
- différence de vitesse
- LAN to WAN (càd que la vitesse du LAN est + faible que celle du WAN)

La gigue : lié à la latence → (le temps que le paquet prend à être transporter)
: c'est la variation de la latence / du délai
Internet est une variation d'envoi de paquets.
(Pour qu'on ai pas de variations il faudrait tout mettre dans un buffer)

❗ Quels sont les besoins et les problèmes de la QoS ? (pas sur pour les besoins)

Les problèmes liés à la qos est qu'en cas d 'encombrement d'un lien, les paquets sont routés par un autre chemin ; si le chemin est trop long, les paquets sont détruits.
Si le débit maximum est supérieur à la bande passante du lien , des paquets seront détruits.

La qos a plusieurs types de besoins :

- le besoin applicatif :

Les applications interactives ont des exigences strictes. Les applications de voix nécessitent des caractéristiques de réseaux très précises. Les techniques de la QOS vise à retenir que les 2 paramètres en dessous

- le besoin en bande passante :

débit constant, majoritairement utilisé par les applications audio/vidéo et par les applications intéractives

débit immédiat, privilégié par les applications de type transfert de fichi

- le délai de traversée du réseau :

Les besoins seront variables, des applications n'ayant pas de contraintes de délais aux applications à forte contrainte temporelle telles que la voix. Il appartient alors au réseau de rendre prioritaires les flux de certaines applications sensibles.

Décrire les concepts qui expliquent la QoS : caractéristiques du traffic, mise en file d'attente, modèle de QoS et technique d'implémentation

D'autres éléments qui rajoute de la latence :

- données → compression des données
- groupage par paquets → encapsulation
- mise en file d'attente → durée variable d'une trame

(La mise en file d'attente est un outil des congestions qui permet de stocker en mémoire tampon, de hiérarchiser et, si nécessaire, de réorganiser les paquets avant leur transmission à la destination) .

Perte de paquets → lorsque le paquet arrive trop tard on le jette

- Voix : si cela passe sans perte → on a un bon réseau sinon il est mauvais
  : fluide mais sensible aux abandons et aux délais
  : peut tolérer un certain degré de latence, de gigue et de perte sans effets notables
- Vidéo : est en **salves** = pics sur le réseau pour afficher l'image → sensible aux abandons et paquets et aux délais.
  : gourmand, supporte mal les pertes

: + exigeant que la voix vu que les paquets envoyés sont plus importants

- Data/données : ex: transfert de fichiers, un backup, 1 grand download,..
  → se fait d'un coup mais consomme le + de ressources ! (donc peut impacter d'autres trafics)

la vitesse des éléments = la latence la plus lente
→ incensibles aux pertes → car on est en TCP et on a des accusés de réception
→ incensibles aux retards
Nous avons 2 types de données : les données intéractives (1)et non intéractives (2)
(1)il y'a 2 activités : nous et la machine (un dialogue entre les 2)
(2) AVANT !! BASH = traitement par lots. (programme avec les données,calculs,...)

Types de files d'attentes :

- mise en file d'attente FIFO → nous n'avons pas de QOS !

met en file d'attente les paquets et les transfère dans l'ordre de leur arrivée. Le FIFO n'a pas de concept de priorité ou de classe de trafic et de ce fait, ne prend pas de décision sur la priorité des paquets.

- WFQ → file d'attente automatique en fonction des types de paquets.

WFQ est une méthode de programmation automatisée grâce à laquelle la bande passante est allouée au trafic réseau de façon équitable. Elle applique des priorités ou des pondérations au trafic identifié et le classe en conversations ou flux.

- CBWFQ → c'est nous qui classons les paquets avec un tag en écrivant un n°de priorité dans le paquet

CBWFQ étend la fonctionnalité de mise en file d'attente pondérée (WFQ) standard afin de fournir la prise en charge des classes de trafic définies par l'utilisateur.

Avec le CBWFQ, vous définissiez des classes de trafic en fonction de critères de correspondance incluant les protocoles, les listes de contrôle d'accès (ACL)

et les interfaces d'entrée. Avec la fonctionnalité LLQ, la stratégie CBWFQ bénéficie d'une capacité de mise en file d'attente à priorité stricte (PQ).

- LLQ → priorité à celui qui vient, est direct servi (1er arrivé,1er servi)

  Classes bases (CBWFQ) → on va mettre des classes à nos paquets
  Une mise en fille d'attente peut provoquer des retards car les nouveaux paquets ne peuvent pas être transmis avant le traitement des paquets précédents.

3 façons de faire de la QOS :

- Best Effort : On ne fait pas de QOS. Réseau fait de son mieux pour envoyer les paquets. Etat par défaut du réseau.
- Intserv : la bande passante est garantie (il faut payer)

A l'intérieur MPLS et RSVP (RSVP = système de réservation de ressources dans le réseau)
Le modèle d'architecture IntServ a été développé pour répondre aux besoins des applications en temps réel, telles que la vidéo à distance, les conférences multimédia, les applications de visualisation de données et la réalité virtuelle.

- Diffserv : marquage de paquets en mettant une priorité. On a une latence pratiquement garantie

Le modèle de QOS DiffServ spécifie un mécanisme simple et évolutif pour la classification et la gestion du trafic réseau. La conception du modèle DiffServ s'affranchit des limites associées aux modèles de remise au mieux et des services intégrés.

Implémentation de la QOS:

C'est le fait qu'on veuille que le réseau fonctionne même si il y'a de la saturation.
On va donc faire plusieurs étapes :

- On marque les paquets (prévention des pertes de paquets) et classification des paquets(La classification détermine la classe de trafic à laquelle les paquets ou les trames appartiennent) :

Mettre un tag dans le paquet (au niveau de la couche 2 et 3
Pour 802.1q qui est une @ pour un lan on a 16 bits dont 3 pour la QOS donc 8 niveaux de priorité au niveau 2 et au niveau 3 nous avons 6 bits pour la QOS soit 64 niveaux de priorité
Les priorités les plus hautes sont pour la maintenance et la gestion des réseaux.
C'est en fonction de l'équipement que l'on va écire dans la couche 2 ou couche 3

- On prévient les encombrements

Les outils de prévention des encombrements permettent de surveiller les charges de trafic sur les réseaux afin d'anticiper et d'éviter les encombrements au niveau des congestions du réseau commun et de l'internet avant que les encombrements ne deviennent un problème.

- On gère les encombrements

Où faire de la QOS ?

On le fait le plus près de la source et le long du chemin → LIMITES DE CONFIANCE
On place la QOS sur tout les équipements de la chaine depuis la source si possible le + près

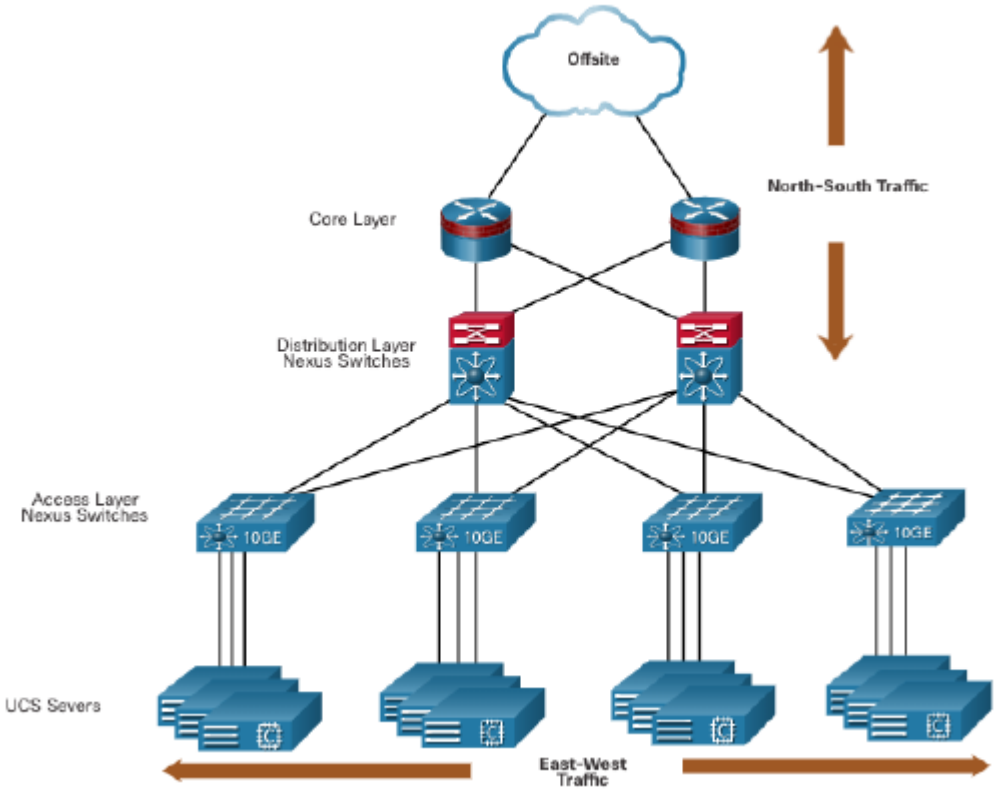
Prévention de la congestion :

Nous avons le shapping et le pollicing.
Le shapping → je retarde le paquet pour le trafic
Le pollicing → je drop les paquets pour diminuer le trafic (on drop ce qui est en retard soit au dessus de la limite)
Lorsque nous avons un trafic qui ne dépasse pas la limite nous avons un bon réseau et dans le cas contraire un mauvais réseau

Q.7. Conception, virtualisation et automatisation des réseaux

Expliquer les principes et concepts suivants :
Réseaux hiérarchiques : grâce à un schéma montrant la topologie d'un

réseau à 3 couches, expliquer comment Cisco envisage de supporter des réseau sans frontière et évolutifs



Nous avons plusieurs niveaux :

- le 1er niveau (couche d'accès) est composé de commutateur (couche2) qui s'occupent de relier plusieurs noeuds en gérant les trames intelligemment et d'offrir un accès réseau aux utilisateurs.
- le 2eme niveau (couche distribution) est composée de commutateur de couche 3 donc de commutateurs qui peuvent faire le travail d'un routeur. Ils s'occupent du routage(inter vlan), la QOS et la sécurité. Ils interconnectent les commutateurs de la couche d'accès, offre de la redondance au cas où une machine tombe (VRRP) et de la QOS.
- Le 3ème niveau (couche coeur) est aussi composée de commutateur de couche 3, ce sont eux qui vont s'occuper d'envoyer les paquets le plus rapidement possible au routeur edge qui lui communique avec le FAI

Définir Cloud computing et virtualisation

CLOUD COMPUTING : utilisation d'ordinateurs en nuage (càd opaque et qu'on ne voit pas la structure de l'architecture de ces nuages) et jsp où se trouve mon application.

On a des ordi interconnectés entre eux et qui ensemble produisent des services
(services = stocké des données et éxécuter des traitements)
On peut demander des services de calculs et de stockage
Cloud = un ensemble de centres interconnectés
un cloud offre des services à des terminaux et on gere les droits des utilisateurs
On a une architecture client-serveur : On met les serveurs dans un endroit et tt les terminaux peuvent y accéder normalement de partout

Avantages :

- réduit le cout de possession du matériel,dépenses énergétiques,..
- donne une réponse rapide face au besoin croissant d'espace de stockage des données
- permet l'accès aux données organisationnelles en tout lieu et à tout moment

(données organisationnelles = données de l'entreprise, fichiers etc (OneDrive, cloud,..) et donc avoir notre base de données

le cloud offre des services sur 3 niveaux :

- SaaS (ou logiciel en tant que service) : sur du software and services et on est co a l'internet et au cloud et on peut accéder aux logiciels installer sur le cloud
- PaaS (ou plateforme en tant que services) : plateformes and services : tourner vers les développeurs càd pour faire du développement on doit se tourner vers une plateforme de développement, il faut des outils de développement

Jai des machines, jai des os et jutilise les outils de développement du cloud et donc je gérer le matériel et le logiciel chez moi

- IaaS (infrastructure comme un service) : de + bas niveau → Infrastructure and services → je loue des machines (qui ne sont pas physiques mais virtuelles) et elles se comportent comsi c'était mes vrais machines alors qu'en réalité elles ne sont pas dans mon data center et pas besoin de les entretenir mais je peux installer des os et les gérer comme je le souhaite comme si c'était mes données etc..

Nous avons 4 principaux types de cloud :

- Cloud publics : des appli et des services basés sur le cloud accessibles par le grand public
- Cloud privés : des appli et des services basés sur le cloud sont destinés à une entreprise ou à une entité spécifique, par exemple une administration
- Cloud hybrides : est constitué de 2 ou plusieurs nuages (ex : partie privée, partie publique) , où chaque partie reste un objet distinct, mais où les 2 sont reliés par une architecture unique
- Cloud communautaires : est créé pour l'usage actuel d'une communauté spécifique. Les ≠ entre clouds publics et clouds communautaires se réfèrent aux besoins fonctionnels qui ont été personnalisés pour la communauté. Par ex : les organisations de soins de santé doivent se conformer à certaines stratégies et règlementations (par ex : HIPAA) qui nécessitent une authentification et une confidentialité particulières

data center = coeur du cloud qui offre un espace de stockage ou traitement de données

cloud computing = plusieurs data center interconnectés sur une zone géographique très étendue

VIRTUALISATION : la virtualisation forme le socle du cloud computing. Sans elle, le cloud computing n'existerait pas. La virtualisation sépare le système d'exploitation (OS) du matériel.

Pour la virtualisation, nous avons des serveurs qui y sont dédiés (comme Windows Server ou Linux Server,..) qui fournissait une certaine puissance de

traitement et l'espace d'un serveur étaient consacrés au service fourni (comme internet,..) → hyperviseur

Avantages :

- - de matériels requis
- - d'énergie consommée
- - d'espaces occupés

Infrastructure de réseau virtuel

La virtualisation se fait à 2 niveaux :

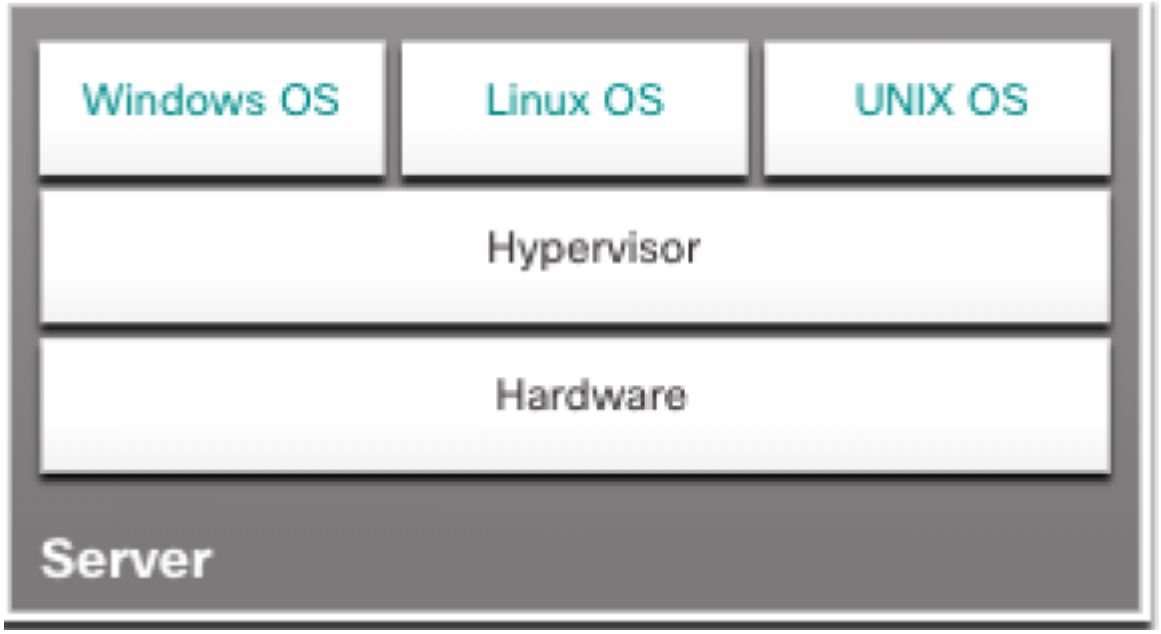
- Hyperviseur de type 1
- Hyperviseur de type 2 = un logiciel qui crée et éxécute des instances de VM. L'ordi sur lequel est un hyperviseur prend en charge une ou plusieurs machines hôtes (= machines virtuelles)

(Hyperviseur = un programme de niveau frameware ou bios ou de niveau système d'exploitation)

Un hyperviseur est installer entre le firmware et le SE. L'hyperviseur peut prendre en charge plusieurs instances de SE

- Hyperviseur de type 1= (sont sans SE) càd qu'ils sont installés directement sur le matériel. Utilisés sur des serveurs d'entreprise et des périphériques de mise en réseau de centres de données.

Un hyperviseur de type 1 est installé directement sur le serveur ou le matériel de mise en réseau, Plusieurs instances d'un système d'exploitation sont ensuite installées au-dessus de l'hyperviseur, comme le montre la figure.



Les hyperviseurs de type 1 bénéficient d'un accès direct aux ressources matérielles. Par conséquent, ils sont plus efficaces que les architectures hébergées. Ils améliorent l'évolutivité, les performances et la robustesse.

En réseau cette technologie est très utile afin d'optimiser nos réseaux, en effet, nous évitons tout types de problèmes liés à la visibilité des ressources, avoir besoin d'une maintenance / d'une gestion du réseau. Les hyperviseurs permet aux machines virtuelles d'être déplacable et permet également à l'administrateur réseau d'ajouter, supprimer et modifier des ressources et profil réseau pour faciliter leur mobilité.

Complexité de la virtualisation :

- si les machines virtuelles sont déplacées, l'administrateur réseau doit pouvoir toujours ajouter,supprimer et modifier des ressources Processus qui prendrait beaucoup de temps avec les commutateurs de réseau traditionnels.
- Lorsqu'un serveur est virtualisé, ses ressources ne sont pas visibles. Cela peut créer des problèmes lors de l'utilisation d'architectures de réseau traditionnelles,...

Réseau SDN et contrôleur SDN

Le contrôleur SDN est une entité logique qui permet aux administrateurs réseau de gérer et de définir la manière dont le plan de données des routeurs et des commutateurs virtuels doit gérer le trafic réseau.

Le contrôleur SDN définit les flux de données entre le plan de contrôle centralisé et les plans de données sur les routeurs et les commutateurs individuels. Pour pouvoir traverser le réseau, chaque flux doit être approuvé par le contrôleur SDN qui vérifie que la communication est autorisée dans le cadre de la politique réseau de l'entreprise.

Si le contrôleur autorise le flux, il calcule l'itinéraire que ce dernier doit suivre et ajoute une entrée correspondante au flux dans tous les commutateurs situés sur le trajet. Le contrôleur alimente les tables de flux. Les commutateurs gèrent les tables de flux.

Un tableau de flux fait correspondre les paquets entrants à un flux particulier et spécifie les fonctions qui doivent être exécutées sur les paquets. Il peut y avoir plusieurs tables de flux qui fonctionnent à la manière d'un pipeline. Un tableau de flux peut diriger un flux vers un tableau de groupe, ce qui peut déclencher une série d'actions qui affectent un ou plusieurs flux.

Quand on considère un routeur sur le plan conceptuel on peut considérer qu'on ai 2 plans/fonctions : (il y'a un 3e)

- plan de contrôle :

permet de prendre des décisions de transmission.

ex : la table de routage, des algo qui tournent et qui permettent de tourner correctement
consomme du cpu et nécessite le stockage de l'information

- plan de données/d'acheminement des données :

matrice de commutation qui relie les ≠ ports du réseau sur un appareil. Le plan de données de chaque périphérique permet de transmettre les flux de trafic.

plans d'acheminement vers un port de sortie
reçoit les trames des paquets les traite ou les stocke mais ce sont des opérat° qui ne nécessitent pas l'utilisation d'une unité centrale

SDN = la séparation du plan de contrôle et du plan de données.

= c'est une architecture de réseau qui virtualise le réseau, offrant une nouvelle approche de l'administration et de la gestion du réseau qui vise à simplifier et à rationnaliser le processus d'administration

QUESTIONS DETAILS :

1.Quels sont les équipements terminaux possibles de l'Internet en 2021 ? Comment sont-ils raccordés à l'Internet ?

Pc , gsm, imprimante, routeur , commutateur , acces point . Carte réseau sans fil ou filaire et connexion oslm.

2.D'après vous, est-il possible de classer les protocoles TCP/IP en protocoles LAN et en protocoles WAN ? Proposer et défendre votre classification ?

3.WAN et modèle OSI : les normes WAN se concentrent sur quelles couches du modèle OSI ? Citer 3 protocoles de chaque couche concernée ?

Couche 1 et 2

1) SDH , SONET et DWDM ce sont des protocoles pour la fibre optique.

2) MPLS, Frame Relay et DSL

4.Quelle est la différence entre un fournisseur de service d'accès et un transporteur sur Internet ?

FAI donne l'acces a internet et connecte plusieurs filiale des entreprise .

5.Qu'est-ce que une ligne T1/E1? Quel est le rapport avec SDH, SONET et DWDM ?

Ligne T1 et E1 sont des lignes de co louée, T1 USA 1,544 MBPS E1 europe 2MBPS

SDH SONET ET DWDM sont des protocoles utilisé dans les fibre optiques utilisé pour les wan.

6.Différence entre OSPFv2 et OSPFv3 ?

OSPFv2 que pour ipv4 et sécurité géré avec authentification OSPFv2

OSPFv3 pour ipv6 (et v4) et sécurité avec IPSec

7.Pourquoi y a-t'il différents protocoles de routage : RIP, OSPF, BGP ?

RIP se basait uniquement sur le nombre de saut nécessaire pour la dest alors que ospf regarde également l'état des liens donc si certaines connexion sont

en bonne état ou pas (bonne bande passante) si il trouve un chemin avec plus de saut mais de meilleurs lien ils prendras le plus de sauts.

BGP est protocole de routage pour les AS .

8.OSPF est un protocole de routage à état de lien : ça veut dire quoi ? Un lien c'est quoi ? Un état de lien c'est quoi ?

Un lien c'est une communication entre 2 routeur qui font tourner ospf, état de lien c'est le cout (une mesure comme les sauts oslm) pour atteindre un autre routeur.

9.Pourquoi les routeurs OSPF s'échangent des paquets Hello ?

Pour détecter si un autre routeur effectuant ospf se trouve sur le réseau.

10.Comment configurer la propagation d'une route par défaut avec OSPF ?

11.Expliquer le problème de la perte de paquets et comment la QoS peut le prévenir ?

Certains application ou protocole nécessite une délai d'attente faible et trés peu voir pas de perte de paquets comme voIP qui peut causer de gros probleme lors de l'utilisation.

Prioriser les paquets.

12.Expliquer le phénomène de congestion et donner 3 exemples susceptibles de provoquer une congestion ?

Congestion : lorsque le flux de donnée dans un réseau est trop important et que une attente est crée au niveau des appareils (routeur commutateur) donc possible drop des paquets et tout. Pas assez d'écoulement des paquets par rapport a l'entrée.

Ajout de nouveau appareils dans le reseau, appareils pas assez performant , utilisation d'application qui demande bcp de bande passante en simultané.

13.Expliquer DiffServet IntServ ? De quoi s'agit-il?

Diff serv (differentiated services) : on mets des priorité sur les paquets pas de reservation de ressources (bande passante toussa)

Intserv (Integrated services) : reservation des ressources avant l'envoi des paquets pour obtenir la qos demandé.

14.Quand est-ce qu'un appareil doit implémenter la QoS ?

Lorsque le réseau va bientot étre saturé ou bien lorsqu'il faut utiliser des application critique (genre voip).

15.Qu'est-ce que la classification et le marquage des paquets ?

Classification: Les paquets sont classé dans des types et des stratégie sont appliqué sur les types (genre ACL),

Marquage : Ajoute une valeur a l'en-tete ip, selon valeur priorité.