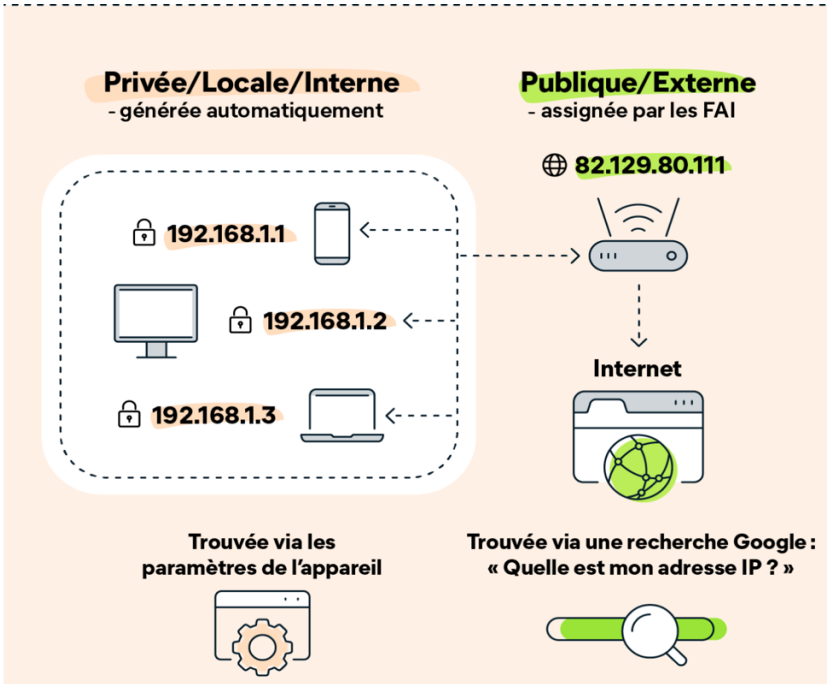
Questions Réseaux Partiel 2

1) Quels sont les différents types d'adresses IPV4 ? Quelles plages pour les adresses privées ? Qu'est-ce que le NAT ?

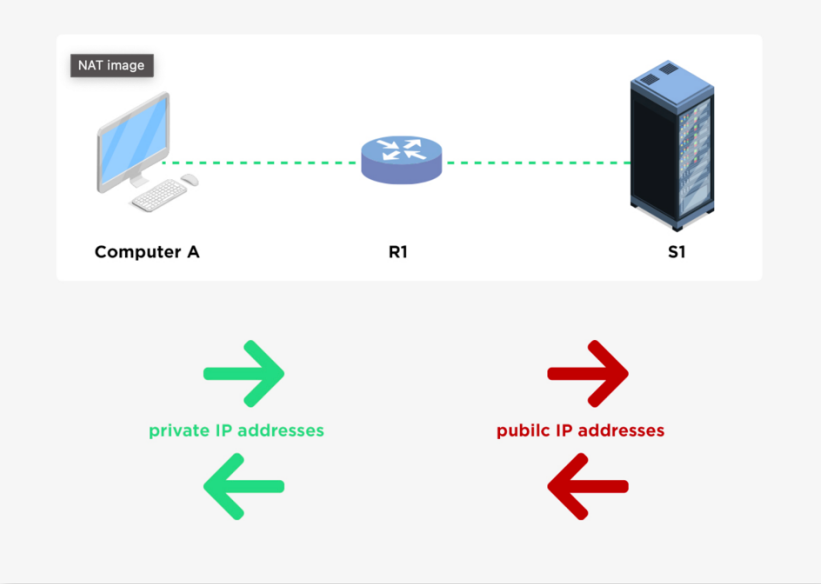
Une **adresse IP publique** permet d'identifier le périphérique auprès du réseau Internet, de telle sorte que toutes les informations recherchées puissent être retrouvées. Une **adresse IP privée** est utilisée à l'intérieur d'un réseau privé pour établir une connexion sécurisée à d'autres appareils du réseau. Une adresse IP privé n'est donc pas utilisable sur internet. Une adresse IP publique est unique dans le monde alors que pour une adresse IP privée c'est dans le réseau local qu'elle est unique.

Les adresses IPv4 **publiques** appartiennent aux plages suivantes :

10.0.0.0 – 10.255.255.255 (10.0.0.0/8)
172.16.0.0 – 172.31.255.255 (172.16.0.0/12)
192.168.0.0 – 192.168.255.255 (192.168.0.0/16)



Le protocole **NAT** (Network Adress Translation) est une fonction assurée par un routeur et qui permet de **changer les adresses IP privée en adresse publique**. Cela correspond donc à une **factorisation** : on a juste besoin d'une seule adresse IP publique à l'ISEP pour que tout le monde puisse accéder à Internet. Le numéro de port permet d'identifier à quel périphérique la réponse doit être transmise. **Ce processus permet de réduire le besoin d'adresses publiques IPv4.** (N'existe plus en IPv6 car il y a suffisamment d'adresses).



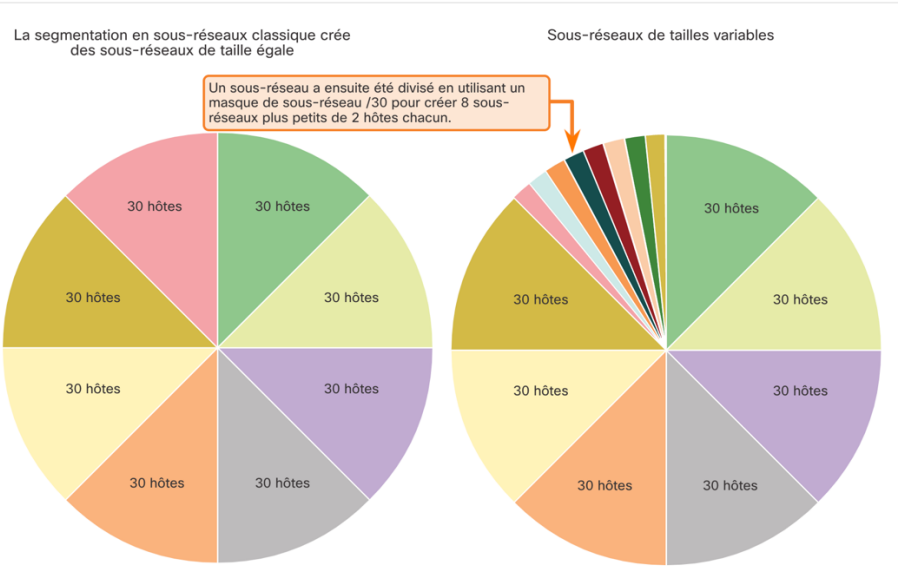
2) Quel est l'intérêt de la segmentation pour les réseaux et quelles sont les méthodes pour créer un sous-réseau en IPv4 (VLSM) ? Qu'en est-il en IPv6 ? (*)

La segmentation réseau consiste à **diviser le réseau en plusieurs sous-réseaux opérant chacun comme un mini-réseau en soi**. La segmentation en sous-réseaux réduit le trafic global et améliore les performances réseau. Elle permet également aux administrateurs de mettre en œuvre des politiques de sécurité, notamment pour définir si les différents sous-réseaux sont autorisés ou non à communiquer entre eux. Une autre raison est qu'il **réduit le nombre de périphériques affectés** par un trafic de diffusion anormal dû à des erreurs de configuration, à des problèmes matériels/logiciels ou à une intention malveillante.

Il existe plusieurs manières d'utiliser les sous-réseaux pour gérer les périphériques réseau :

- **Sous-réseau en fonction du lieu** (Étage 1, Étage 2, etc.)
- **Sous-réseau en fonction de groupe ou de la fonction** (Administration, Compta, Étudiants...)
- **Sous-réseau en fonction du type d'appareils** (les hôtes, les serveurs, les imprimantes...)

En IPv4, il existe deux méthodes principales pour créer des sous réseaux **: soit en utilisant le même masque de sous-réseau** (dans ce cas tous les sous-réseaux possèdent le même nombre d'hôtes possibles, ce qui fait que de nombreuses adresses IPv4 peuvent être allouées mais non attribuées), soit en utilisant un masque de sous-réseau variable (méthode VLSM – *Variable Length Subnet Mask*). Comme le montre le côté droit de la figure, le VLSM permet de diviser un espace réseau en parties inégales. Avec la méthode VLSM, le masque de sous-réseau varie selon le nombre de bits empruntés pour le sous-réseau, d'où la partie « variable » de cette méthode.



Contrairement à IPv4 où l'on doit emprunter des bits à la partie hôte pour créer des sous-réseaux, IPv6 a été créé avec l'idée des sous-réseaux en tête. Dispose en effet **d'un champ ID de sous-réseau** : pour créer des sous-réseaux, il suffit d'incrémenter l'ID de sous-réseau.

3) Pourquoi avoir créer IPv6 ? Quels sont les processus permettant la cohabitation des protocoles IPv4 et IPv6

Les adresses IPv6 ont été créée à la suite de la pénurie d'adresse IPv4. Pour permettre une bonne cohabitation sur le réseau, des techniques de migrations de IPv4 vers IPv6 ont été créés :

- ⇒ **Double pile** (dual-strack) : Permet aux adresses IPv4 et IPv6 de coexister sur le même segment.
- ⇒ **Tunneling** : Adresses IPv6 encapsulées dans un paquet IPv4
- ⇒ **Traduction** : Traduction des adresses IPv6 en IPv4, et inversement, grâce à une technique de traduction analogue NAT64.

4) Comment sont représentées les adresses IPv6 + donner des exemples (avec les ::) (*)

Les adresses IPv6 ont une longueur de **128 bits** et sont notées sous forme de chaînes de valeurs hexadécimales (8 groupes). Tous les groupes de 4 bits sont représentés par un caractère hexadécimal unique. Soit un total de **32 valeurs hexadécimales**. Plusieurs règles permettent de réduire l'écriture des adresses IPv6 : Enlever les zéros au début des segments et remplacer les chaines de zéros par « :: ».

5) Quels sont les différents types d'adresses IPv6 (mono, multi, anycast). Détailler les adresses de monodiffusion (GUA et LLA) et de multidiffusion (*)

Il existe 3 grands types d'adresses IPv6 : monodiffusion (GUA et LLA), multidiffusion (attribuée ou de nœud sollicité) et anycast. Les adresses de monodiffusion sont détaillées dans la question suivante.

En IPv6, les adresses de multidiffusion ont le préfixe ff00::/8. Il existe deux types d'adresses de multidiffusion :

- Les adresses de multidiffusion attribuée : c'est une adresse unique utilisée pour joindre un groupe de périphériques prédéfinis (par ex ceux éxecutant un service ou un protocole commun)
- Les adresses de multidiffusion de nœud sollicité : le paquet est envoyé à tous les périphériques et c'est l'adresse MAC de destination (= adresse MAC de multidiffusion) qui est analysée pour savoir si le périphérique est la cible du paquet IPv6.

6) Quelles sont les spécificités des adresses GUA et LLA : structure, plage etc.

- **Adresse GUA** (*Global Unicast Address*) : correspond à une adresse unique au monde et routable sur Internet (l'équivalent des adresses publiques en IPv4). Elle peut être attribuée de façon statique ou dynamiquement (cf. qst 7). Leur structure est la suivante :

  - **Préfixe de routage global** : correspond à la partie réseau et est attribuée par le fournisseur à un client ou à un site. (Le plus souvent en /48).
  - **ID de sous-réseau** : IPv6 utilise en effet l'ID de sous-réseau pour identifier les sous-réseaux. (Souvent en /16 donc 2^{16} = 65536 sous-réseaux possibles en IPv6 ce qui offre des possibilités immenses).
  - **ID de l'interface** : correspond à la partie hôte.

Schéma :

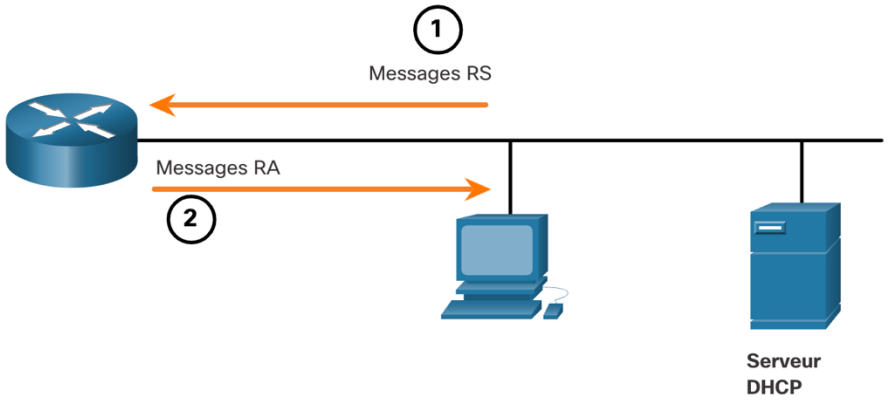
- **Adresse LLA** (*Link-Local Address*) : cette adresse est requise pour chaque périphérique compatible IPv6. Elle est utilisée pour communiquer avec d'autres équipements sur la même liaison locale (= **adresse privé**). Elle est donc unique dans le LAN. **Les LLA se trouvent dans la plage fe80::/10**

7) Comment se réalise l'adressage dynamique des adresses GUA (3 méthodes SLAAC etc..) ? Des adresses LLA ?

Pour configurer automatiquement des adresses GUA, des messages ICMPv6 doivent être envoyés au routeur (cf. q 8) :

- Un **message RS** (Routeur Sollicitation) envoyé par l'hôte pour demander au routeur des informations d'adressages.
- Un **message RA** (Routeur Annonce) indique à un périphérique comment obtenir une adresse GUA et d'autres info d'adressage (son message contient donc la préfixe de réseau et la longueur de préfixe, l'adresse LLA de la passerelle par défaut, les adresses DNS).

Messages RS et RA ICMPv6

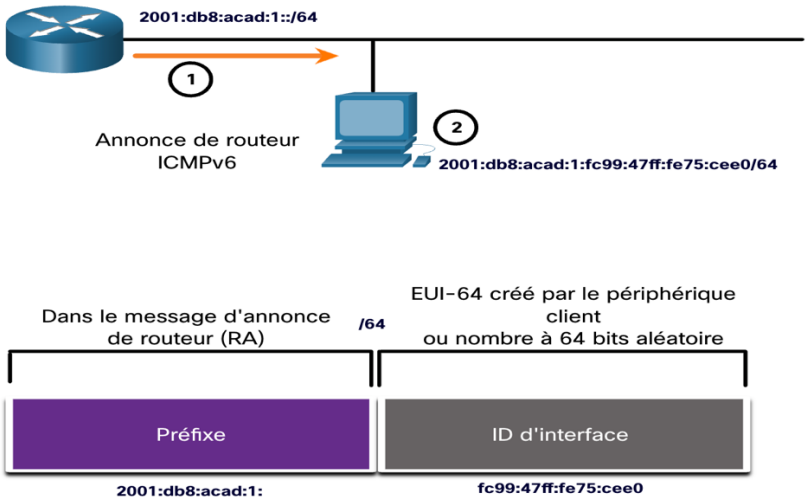


1. Les messages RS sont envoyés à tous les routeurs IPv6 par des hôtes demandant des informations d'adressage.
2. Les messages RA sont envoyés à tous les nœuds IPv6. Si la méthode 1 (SLAAC uniquement) est utilisée, l'RA inclut le préfixe réseau, la longueur du préfixe et les informations de passerelle par défaut.

Il existe 3 méthodes pour l'adressage dynamique :

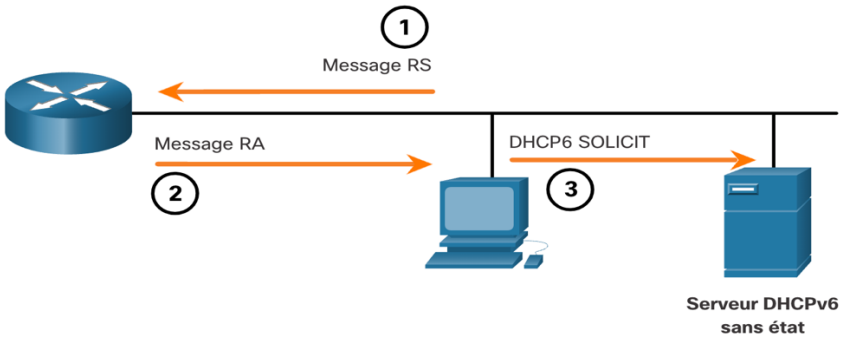
1- **<u>La méthode SLAAC</u>** (« J'ai tout ce dont vous avez besoin, y compris le préfixe, la longueur du préfixe et l'adresse de la passerelle par défaut »).

Permet à un appareil d'obtenir sa propre GUA sans les servicesd DHCP. Avec le SLAAC, le périphérique utilise uniquement les informations du message RA pour créer sa propre adresse de diffusion globale (=GUA)



1. Le routeur envoie un message RA avec le préfixe du lien local.
2. Le PC utilise SLAAC pour obtenir un préfixe à partir du message RA et crée son propre ID d'interface.

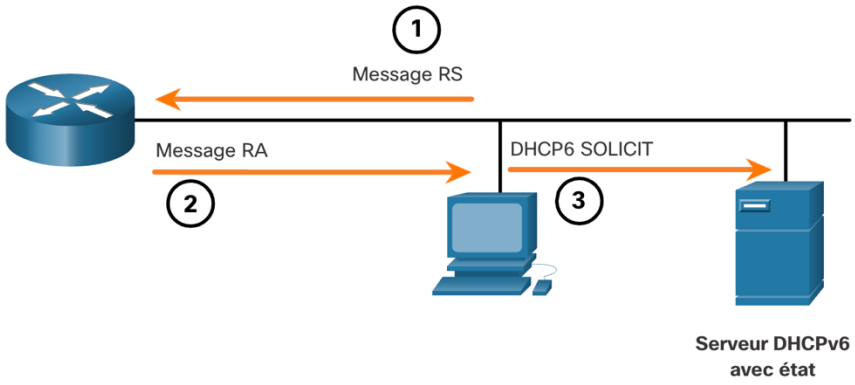
2- La **méthode SLAAC et DHCPv6 sans état** (« Voici mes informations mais vous avez besoin d'info supplémentaires telles que les adresses DNS d'un serveur DHCP »).



1. Le PC envoie un RS à tous les routeurs IPv6, «J'ai besoin d'informations d'adressage».
2. Le routeur envoie un message RA à tous les nœuds IPv6 avec la méthode 2 (SLAAC et DHCPv6) spécifiée. Voici votre préfixe, une longueur de préfixe et des informations sur la passerelle par défaut. Mais vous aurez besoin d'obtenir des informations DNS à partir d'un serveur DHCPv6.»
3. Le PC envoie un message de sollicitation DHCPv6 à tous les serveurs DHCPv6. J'ai utilisé SLAAC pour créer mon adresse IPv6 et obtenir mon adresse de passerelle par défaut, mais j'ai besoin d'autres informations d'un serveur DHCPv6 sans état.

3- La méthode DCHPv6 avec état

Permet à un périphérique de recevoir automatiquement ses informations d'adressage à l'aide des services d'un serveur DHCP.



1. Le PC envoie un RS à tous les routeurs IPv6, «J'ai besoin d'informations d'adressage».
2. Le routeur envoie un message RA à tous les nœuds IPv6 avec la méthode 3 (DHCPv6 Stateful) spécifiée "Je suis votre passerelle par défaut, mais vous devez demander à un serveur DHCPv6 avec état pour votre adresse IPv6 et d'autres informations d'adressage".
3. Le PC envoie un message de sollicitation DHCPv6 à tous les serveurs DHCPv6, j'ai reçu mon adresse de passerelle par défaut du message RA, mais j'ai besoin d'une adresse IPv6 et de toutes les autres informations d'adressage d'un serveur DHCPv6 avec état.

Note : La méthode EUI-64 permet de générer un ID d'interface de 64 bits à partir de l'adresse MAC de l'hôte.

8) Qu'est-ce qu'un message ICMP ? À quoi servent-ils ? Quels sont les différents types de messages ICMP. Citer deux commandes utilisant des messages ICMP et leur fonction (ping et tracert) (*)

Les messages ICMP (Internet Control Message Protocol) permettent de fournir à la suite TCP/IP des messages d'erreurs et des messages d'information lors de la communication avec un autre périphérique IP. Ils peuvent être de différents types :

- **Accessibilité de l'hôte** : un message d'écho ICMP peut être utilisé pour tester l'accessibilité d'un hôte sur un réseau IP. (c'est la base de la commande ping).
- **Destination** (ou service) inaccessible : lorsqu'un hôte ou une passerelle ne peut pas acheminer un paquet, il envoie un message ICMP de destination inaccessible.
- **Délai dépassé** : utilisé par un routeur pour indiquer qu'il ne peut pas transférer un paquet car le champ TTL (Time to Live) a atteint 0. Le paquet est alors abandonné et un message ICMP 'délai dépassé' est envoyé à l'hôte source.

En IPv6, les messages ICMP (RS : routeur sollicitation et RA : routeur annonce) sont utilisés pour l'allocation dynamique d'adresses (cf. Q 7), tandis que les messages (NS : Sollicitation de voisin et NA : annonce de voisin) sont utilisés pour le protocole ND (= l'équivalent du protocole ARP mais pour IPv6).

Les messages ICMP sont à la base de 2 commandes :

- ***Ping*** : Pour tester la connectivité sur le réseau en donnant le temps écoulé entre l'envoie et la réception de l'écho ICMP. (→ Mesure des performances réseau)

- ***Traceroute*** : permet de générer la liste de sauts qui ont été atteints avec succès par le paquet le long du chemin de destination. (→ Affiche la liste des interfaces de tous les routeurs par où le paquet est passé).

9) Quel est le rôle de la couche Transport ? Quels sont les deux protocoles principaux ?

La couche transport est responsable des communications logiques entre les applications exécutées sur différents hôtes. Elle définit les services à **segmenter**, à **réassembler** et **contrôle de flux de données** pour permettre une connexion bout à bout. Elle comprend deux protocoles : **TCP** et **UDP**.

10) Quelles sont les spécificités des protocoles UDP et TCP ? Dans quels cas choisir l'un par rapport à l'autre. Donner des exemples. (*)

Les protocoles UDP et TCP spécifient **comment transférer les messages entre les hôtes**.

TCP (*Transmission Control Protocol*) est un protocole de transport de données **fiable** et **complet** qui garantit que toutes les données arrivent bien à destination grâce une numérotation et **un suivi des segments**, un **accusé de réception** des données reçues et la retransmission de toute donnée non reconnue. TCP doit d'abord établir une connexion avec la destination : c'est un **protocole de connexion orientée** (cf. Q 12).

UDP (*User Datagram Procotol*) ne fournit pas de fiabilité ni de contrôle de flux. En revanche, **les données sont traitées plus rapidement** que les segments TCP. C'est un **protocole sans connexion**. Il ne renvoie pas les données perdues et il n'y a pas d'accusé de réception. Les données sont reconstituées dans l'ordre de réception.

Le choix entre TCP et UDP dépend du service que l'on souhaite effectuer. Si pour l'application il ne doit pas y avoir de retard de transmission (par ex. la voix, vidéo, DNS...) UDP est plus approprié. Toutefois, s'il est important que les toutes les données arrivent dans un ordre approprié (ex. Messagerie, navigation Web), alors TCP convient mieux dans ce cas.

11) À quoi correspondent les numéros de port ? À quoi servent-ils ? (*)

Les numéros de port sont utilisés **pour gérer plusieurs communications en simultanées**. Ils **identifient l'application d'origine** (pour l'hôte local) et **l'application de destination** (pour l'hôte distant).

Une **interface de connexion** correspond à l'association des adresses IP source et destination avec les numéros de port source et destination → **sert à identifier le serveur et le service demandé par le client.**

Il existe 3 types de numéros de port : les ports bien connus (http, SMTP, etc.), les ports dynamiques (correspondant aux ports sources et générés aléatoirement)

Voici quelques numéros de port connus :
http (80)
DNS (53)
FTP (21)
SMTP (25)
SSH (22)
Telnet (23)

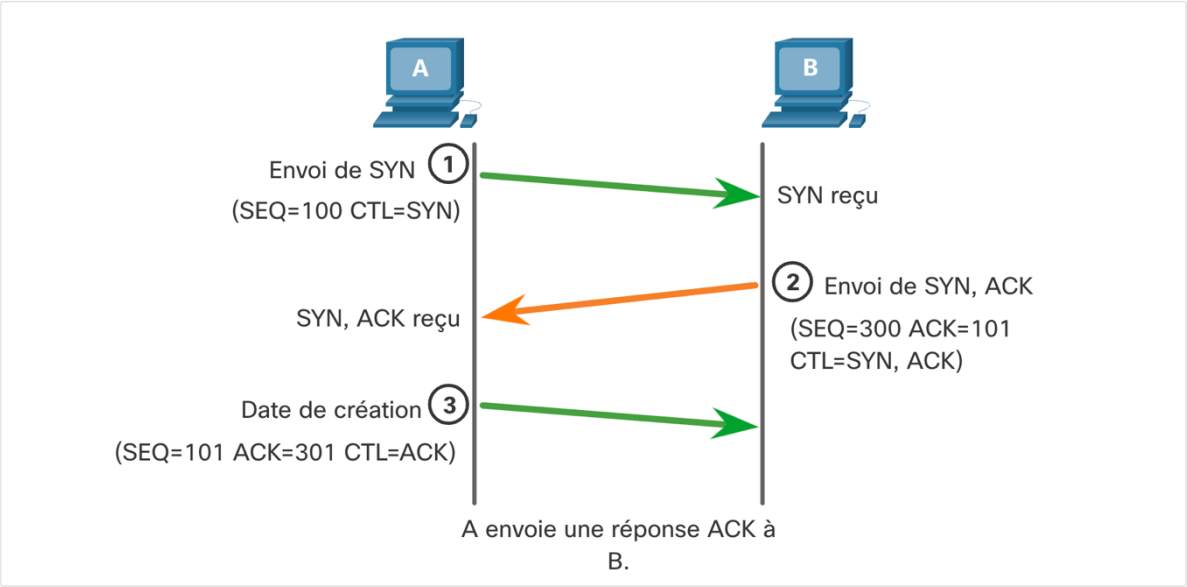
w : Le numéro de port indique l'application à laquelle les données sont destinées. De cette manière, lorsque l'ordinateur reçoit des informations destinées à un port, les données sont envoyées vers l'application correspondante.

12) Comment établir/interrompre une connexion TCP ?

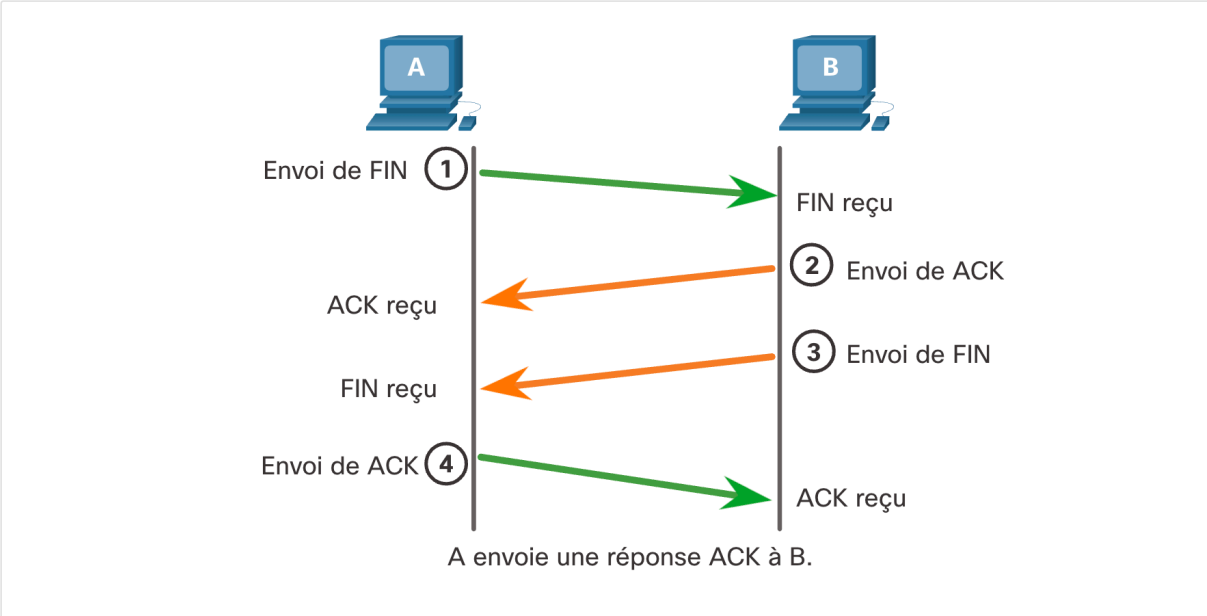
L'établissement d'une session TCP se réalise en 3 étapes :

- Étape 1 : Envoi d'un SYN → Demande l'établissement d'une session entre la source et la destination
- Étape 2 : ACK et SYN → le serveur accuse réception de la session de communication client-serveur et demande l'établissement d'une session serveur-client
- Étape 3 : ACK → Le client accuse réception de la session serveur-client.

L'hôte est alors disponible pour communiquer via TCP.



Pour interrompre une session, le schéma est :



13) Comment TCP gère la fiabilité et le contrôle de flux ? et UDP ?

Le protocole TCP est le protocole le plus fiable. Il **renvoie les paquets abandonnés** et **les numérotes dans l'ordre**, et il aide à la non-surcharge. Il effectue un **contrôle de flux** en déterminant le **volume de données que l'hôtes de destination peut recevoir et traiter de manière fiable**. Le contrôle de flux aide à maintenir la fiabilité des transmissions TCP en réglant le flux de données entre la source et la destination pour une session donnée. Pour cela, l'en-tête TCP inclut un champ de 16 bits appelé taille de fenêtre. La taille de fenêtre détermine le **nombre d'octets qui peuvent être envoyés avant de recevoir un accusé de réception**. Le numéro d'accusé de réception est le numéro du prochain octet attendu.

UDP ne numérote pas les paquets et les **réassemble dans l'ordre de réception**. Il n'envoie d'accusé réception. **En cas de paquet perdus, ils ne sont pas renvoyés**.

14) À quoi servent les couches application, session et présentation ? Donner un exemple de protocole de chaque couche

La **couche application** sert d'interface entre les applications que nous utilisons pour communiquer et le réseau sous-jacent via lequel les messages sont transmis. Elle utilise comme protocole : HTTP, DNS, FTP

La **couche présentation** possède 3 fonctions principales :

- ⇒ **Mettre en forme les données** dans un format compatible pour la réception avec le destinataire
- ⇒ **Compresser les données** (pour que le destinataire les décompresse)
- ⇒ **Chiffrage des données**

Exemple de protocoles : GIF, JPEG, PNG

La **couche session** crée et gère les dialogues entre les applications.

15) Qu'est-ce qu'un réseau Peer-to-Peer ?

Dans un réseau Peer-to-Peer, chaque périphérique final connecté peut opérer aussi bien en tant que serveur et que client. Par exemple, un ordinateur peut servir le rôle de serveur pour une application et servir simultanément de serveur pour une autre. L'application **Peer-to-Peer peut agir en tant que client et serveur dans une même connexion.**

16) Comment fonctionne http ?

Lorsqu'une adresse web (ou URL) est tapée dans un navigateur web, ce dernier établit une connexion au service web s'exécutant sur le serveur à l'aide du protocole http.

Étape 1 : Le navigateur commence par interpréter les 3 parties de l'URL ;

- http (le protocole)
- www.cisco.com (le nom de domaine)
- Index.html (le fichier HTML à demander au serveur)

Étape 2 : Le navigateur Web traduit le nom de domaine en adresse IP (DNS) qu'il utilise pour se connecter au serveur Web ;

Étape 3 : Le serveur Web renvoie le code html de la page Web ;
Étape 4 : La navigateur déchiffre le code html et met en forme la page Web.

Le protocole http est de type requête/réponse. Il y a 3 types de requêtes :

- **GET** : pour demander un fichier HTML
- **POST** : pour télécharger des données vers le serveur (par ex : un formulaire sur le site)
- **PUT** : pour télécharger des ressources vers le serveur Web (ex : une image)

Pour une communication sécurisée sur Internet, il faut utiliser le protocole ***https***.

17) Comment fonctionne les protocoles de messageries electroniques (SMTP, POP, IMAP) ? (*)

3 protocoles permettent l'envoi et la réception de messages électroniques.

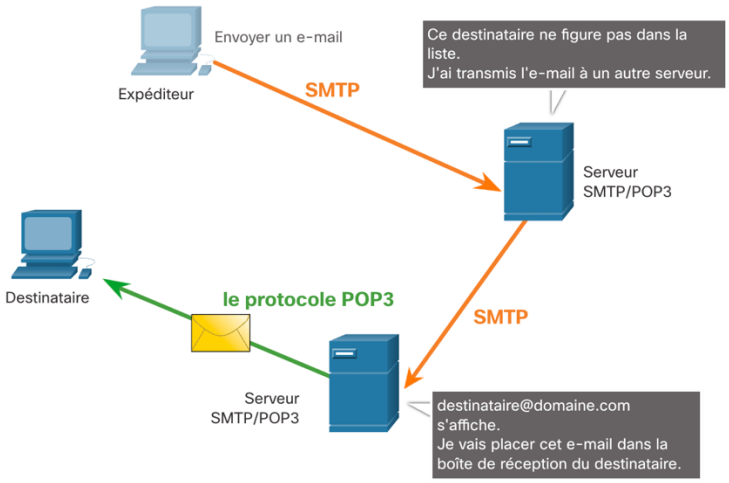
SMTP : Lorsqu'un client envoie un e-mail, le processus SMTP client se connecte à un processus SMTP serveur sur le port réservé 25. Une fois la connexion établie, le client essaie d'envoyer l'e-mail au serveur via la connexion. Si le destinataire ne figure pas de la liste de destinataires du serveur Mail, alors le message doit être transmis à un autre serveur.

→ **Protocole SMTP : pour ENVOYER des emails.**

POP : Le protocole POP est utilisé par une application pour récupérer le message électronique à partir d'un serveur de messagerie. Avec POP, le courrier électronique est téléchargé du serveur au client, puis supprimé du serveur.

IMAP : Le protocole de messagerie IMAP décrit une autre méthode de récupération des messages électroniques. Contrairement au protocole POP, lorsque l'utilisateur se connecte à un serveur IMAP, des copies des messages sont téléchargées vers l'application cliente. Les messages originaux sont conservés sur le serveur jusqu'à ce qu'ils soient supprimés manuellement. Les utilisateurs affichent des copies des messages dans leur logiciel de messagerie.

→ **Protocole POP et IMAP : pour RECEVOIR et LIRE des emails.**



18) Comment fonctionnent DNS et DHCP ? (*)

Le **protocole DNS** (*Domain Name System*) définit un service automatisé qui associe les noms de domaine à l'adresse réseau IP correspondante.

Étape 1 : L'utilisateur entre un nom de domaine dans le navigateur
Étape 2 : Une requête DNS est envoyée au serveur DNS associé
Étape 3 : Le serveur DNS fait correspondre le nom de domaine à une adresse IP. S'il ne trouve pas, il contacte un autre serveur DNS pour résoudre le nom en adresse IP.
Étape 4 : La réponse à la requête DNS est renvoyée au client.
Étape 5 : L'ordinateur client utilise l'adresse IP pour effectuer des requêtes du serveur

Le **protocole DHCP** (*Dynamic Host Configuration Protocol*) automatise l'affectation des adresses IPv4, des masques de sous-réseau, des passerelles etc. Le serveur DHCP est généralement un serveur local dédié.

Étape 1 : Le client diffuse un message de détection DHCP (DHCP DISCOVER) pour identifier les serveurs DHCP disponibles sur le réseau.
Étape 2 : Un serveur DHCP répond par un message d'offre DHCP (DHCP OFFER) qui offre un bail au client (càd une durée de validité de l'adresse IP configurée)
Étape 3 : Le client indique le serveur et l'offre qu'il accepte (DHCP REQUEST)
Étape 4 : Le serveur envoie un accusé de réception (DHCPACK)

19) Quelles sont les menaces pour un réseau ? Quelles vulnérabilités ?

Il **existe 4 types de menaces pour un réseau** :

- ⇒ Vol d'information
- ⇒ Perte et manipulation des données
- ⇒ Usurpation d'identité
- ⇒ Interruption du service

De plus, il y a **3 types de vulnérabilités principales** :

- ⇒ **Vulnérabilités Technologique** : à cause de la faiblesse des protocoles (HTTP, SNMP…), du système d'exploitation (Linux, Mac …), des équipements réseau (routeur, pare-feu…)
- ⇒ **Vulnérabilités de configuration** : compte utilisateur non sécurisé, mots de passe facile à deviner …
- ⇒ **Vulnérabilités de stratégies** : installations non conformes, absence de stratégie de sécurité globales écrites …

20) Citer 4 types d'attaques de réseau. Quelles sont leurs spécificités ? (*)

Il existe 4 types d'attaques de réseau :

- ⇒ **Attaque par programme malveillant** : Cheval de Troie, Virus et Vers
- ⇒ **Attaque de reconnaissance** : Découverte et mappage non autorisé de systèmes, services, ou vulnérabilités
- ⇒ **Attaque par accès** : Manipulation non autorisée des données, des accès aux systèmes ou des privilèges utilisateur
- ⇒ **Attaque par déni de service** (DoS) : Désactivation ou corruption de réseaux, de systèmes ou de services

21) Quelle est la différence entre virus, cheval de Troie, Vers ?

Un programme malveillant (malware) est un logiciel spécialement conçu pour endommager, perturber ou voler des données des hôtes ou des réseaux. Il en existe différent :

Le **virus** se transmet par copie d'un ordi à l'autre. Il doit être rattaché à un fichier pour se transmettre. Alors que le **ver** se transmet de façon autonome sans être rattaché à un fichier. Quant au **Cheval de Troie**, il présente une apparence tout à fait légitime et se propage par le biais d'une interaction avec l'utilisateur, par exemple en ouvrant une pièce jointe à un courriel ou en téléchargeant et en exécutant un fichier sur l'internet.

22) Citer des méthodes pour atténuer les risques d'attaques et se protéger (*)

Pour atténuer les attaques réseaux, il est nécessaire de sécuriser les routeurs, les commutateurs, les serveurs et les hôtes. Pour cela, plusieurs appareils et service de sécurité sont mis en œuvre.

⇒ **VPN** : permet de créer des tunnels cryptés sécurisés entre l'hôte et le réseau Internet

⇒ **Pare-feu** : Empêche le trafic indésirable de pénétrer dans le réseau interne. Un pare-feu se trouve entre 2 réseaux (ou plus) et contrôle le trafic entre-deux tout en contribuant à interdire les accès non-autorisés. S'occupe de :

- *Filtrage des paquets* : empêche ou autorise les paquets sur la base d'adresses IP ou MAC
- *Filtrage des applications* : empêche ou autorise les paquets en fonction du numéro de ports
- *Filtrage par URL* : empêche ou autorise l'accès des sites Web basé sur des URL.

⇒ **IPS** : Il s'agit d'un système de prévention des intrusions dont le rôle est de surveiller le trafic entrant et sortant à la recherche de logiciels malveillants ou de signatures d'attaques.

⇒ **ESA/WSA** : filtre les spams et les mails suspects.

23) Commandes netsat + nslookup + show ip route

Nslookup : affiche le serveur DNS configuré par défaut sur l'hôte et les correspondances IP – Nom de domaine enregistrées.

Netstat : Livre des statistiques de base sur toutes les activités de réseau et donne par exemple des indications sur le port et l'adresse sur lesquels une connexion (TCP, UDP) est établie, mais également des indications sur quels ports sont ouverts pour des demandes.

Show ip route : La commande "show ip route" sur Cisco permet de voir la table de routage IP de l'appareil. Cela montre les routes connues par l'appareil, les protocoles utilisés pour les apprendre et d'autres informations telles que les métriques et les interfaces de sortie. Cela permet de voir comment les paquets seront acheminés à travers un réseau et d'identifier les problèmes potentiels de routage.