Chapitre 3 : connexion des succursales

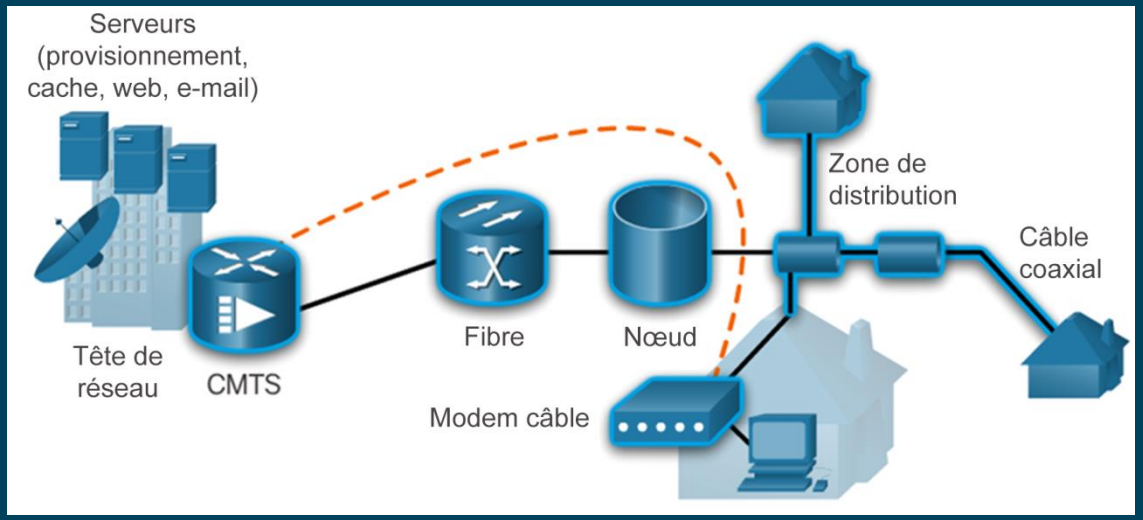
Chapitre 3 : Sections et objectifs

- 3.1 Connexions d'accès distant
  - Sélectionnez les technologies d'accès distant à haut-débit pour répondre aux besoins de l'entreprise.
- 3.2 PPPoE
  - Configuration d'un routeur Cisco avec PPPoE.
- 3.3 VPN
  - Expliquez comment les VPN sécurisent la connectivité de site à site et d'accès distant.
- 3.4 GRE
  - Mise en œuvre d'un tunnel GRE.
- 3.5 eBGP
  - Mise en œuvre d'eBGP dans un réseau d'accès distant à un seul fournisseur d'accès.

3.1 Connexions d'accès distant

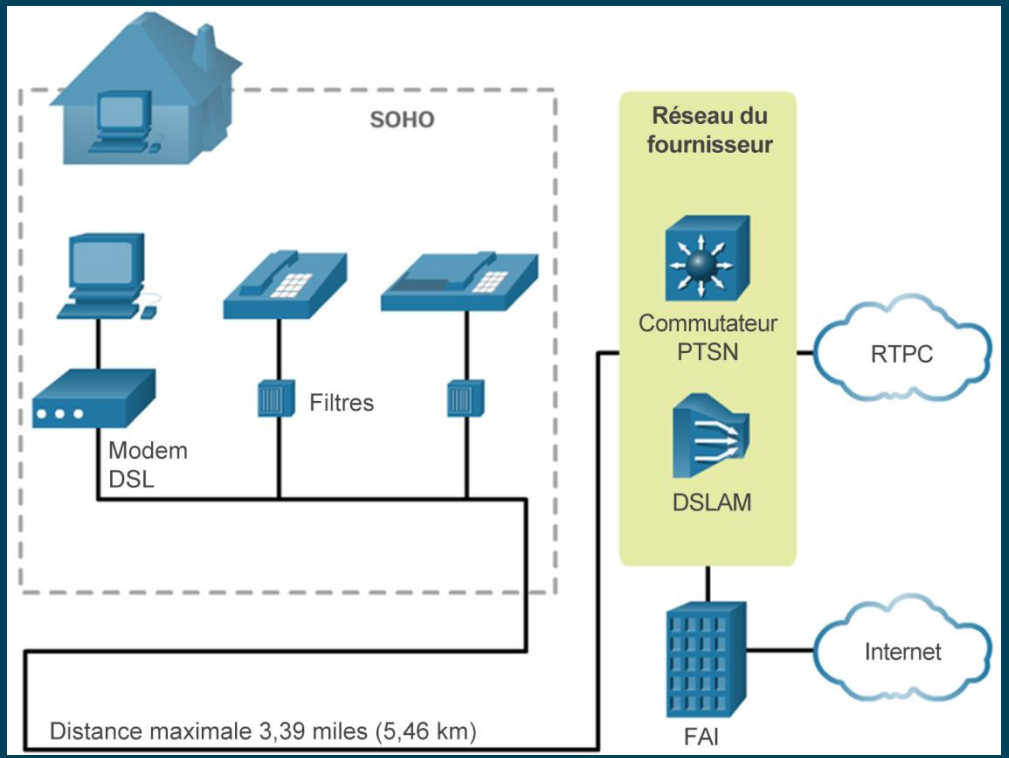
Connexions à haut-débit

- Le système de câblage utilise un câble coaxial qui transporte les signaux de radiofréquence (RF) sur le réseau.
- Un système CMTS de tête de réseau communique avec les modems câble situés aux domiciles des abonnés.
- Le réseau HFC est un réseau mixte optique-coaxial au sein duquel la fibre optique remplace le câble coaxial qui fournit une bande passante inférieure.



Connexions à haut-débit

- Une ligne d'abonné numérique (DSL) est un moyen de fournir des connexions haut débit sur des fils de cuivre installés.
- L'émetteur-récepteur DSL et le DSLAM sont les deux composants importants.
- L'avantage de la technologie DSL par rapport à la technologie du câble est qu'elle n'est pas un support partagé. Chaque utilisateur bénéficie d'une connexion directe et distincte au multiplexeur DSLAM.



Connexions à haut-débit

- Les développements de la technologie sans fil haut débit augmentent la disponibilité du sans-fil par le biais de trois technologies principales :
  - **Wi-Fi municipal** : la plupart des réseaux sans fil municipaux utilisent un maillage de points d'accès interconnectés. Chaque point d'accès est sur le même canal et peut communiquer avec au moins deux autres points d'accès. Le réseau maillé couvre une zone donnée à l'aide de signaux radio.
  - **Cellulaire/mobile** : les téléphones mobiles utilisent les ondes radios pour communiquer par l'intermédiaire des tours de téléphonie mobile voisines. L'accès au haut débit mobile/cellulaire répond à diverses normes.
  - **Internet par satellite** : les services Internet par satellite sont utilisés dans les endroits où aucun accès Internet par voie terrestre n'est disponible ou pour les installations mobiles temporaires. L'accès à Internet par satellite est disponible dans le monde entier.

Sélectionner une connexion haut-débit

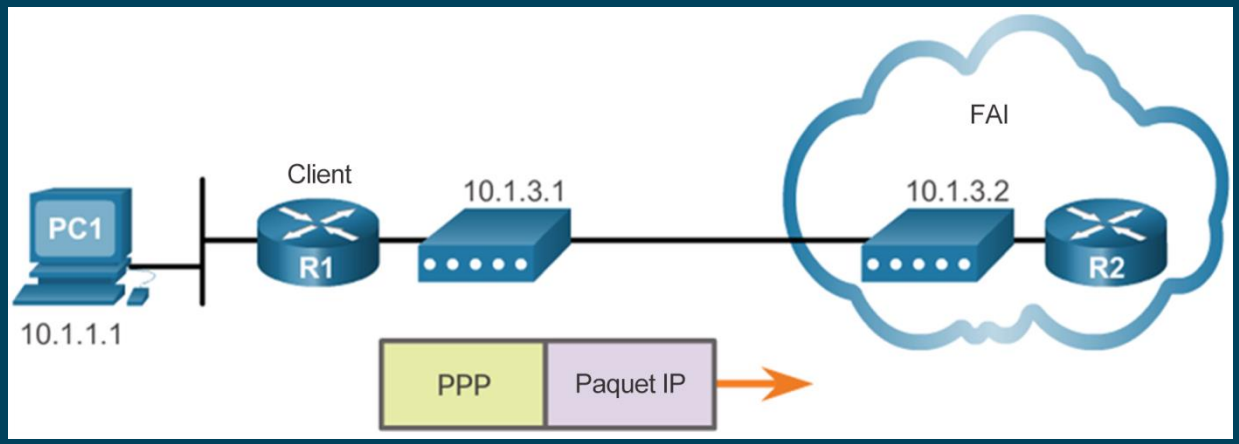
- Chaque solution haut débit présente des avantages et des inconvénients.
- Voici quelques-uns des facteurs à prendre en considération pour la prise de décision :
  - **Câble** : la bande passante est partagée par nombreux utilisateurs ; les débits de données montants sont souvent lents pendant les heures de fort trafic, dans les zones où les abonnés sont nombreux.
  - **DSL** : bande passante limitée qui dépend de la distance (jusqu'au central du FAI), débit montant très faible par rapport au débit descendant.
  - **Fibre optique jusqu'au domicile** : requiert l'installation de la fibre optique directement jusqu'au domicile.
  - **Cellulaire/Mobile** : la couverture constitue souvent un problème, même au sein d'un petit bureau ou d'un bureau à domicile (SOHO) pour lequel la bande passante est relativement limitée.
  - **Maillage Wi-Fi** : la plupart des municipalités n'ont pas déployé de réseau maillé ; toutefois, si c'est le cas et si le SOHO se situe dans la portée d'émission, il s'agit d'une option envisageable.
  - **Satellite** : solution onéreuse, capacité limitée par abonné ; offre souvent un accès lorsqu'aucune autre solution n'est possible.

3.2 Types de protocoles STP

PPPoE

Présentation de PPPoE

- Le protocole PPP peut être utilisé sur l'ensemble des liaisons série, y compris celles créées à l'aide de modems analogiques à ligne commutée et de modems RNIS.
  - Le protocole PPP permet d'attribuer des adresses IP aux extrémités distantes d'une liaison PPP.
  - Le protocole PPP prend en charge l'authentification CHAP.
  - Les liaisons Ethernet ne prennent pas en charge le protocole PPP de manière native. Le protocole PPPoE (PPP over Ethernet) fournit une solution à ce problème. Le protocole PPPoE crée un tunnel PPP sur une connexion Ethernet.

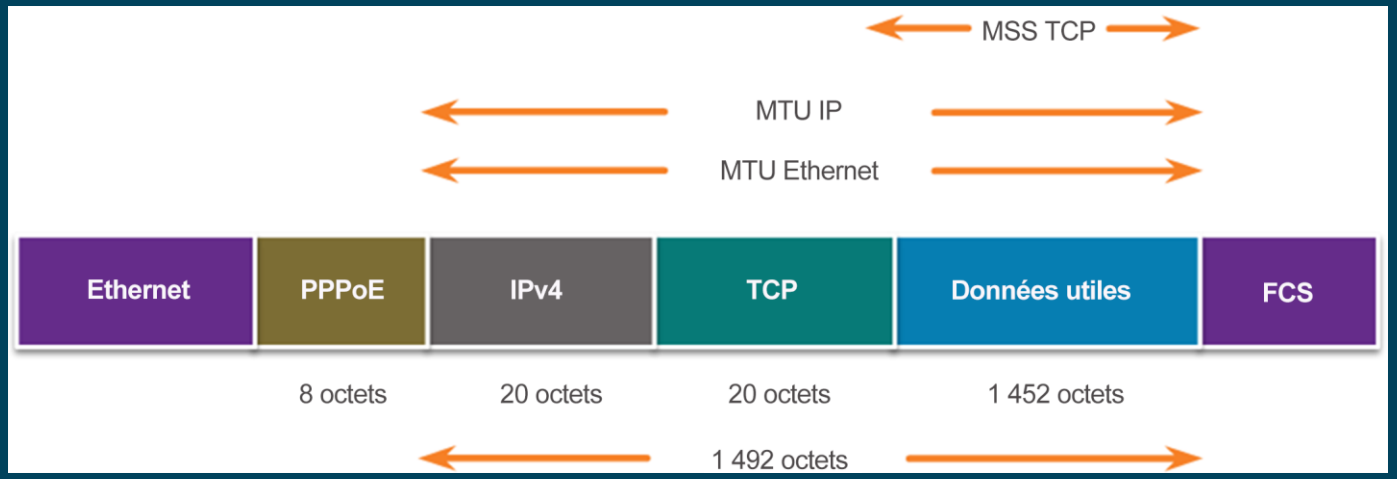


Mise en œuvre de PPPoE

- Configuration de PPPoE
  - L'interface de numérotation est créée à l'aide de la commande **interface dialer** *numéro*.
  - La configuration PPP CHAP définit généralement une authentification unidirectionnelle ; par conséquent, c'est le FAI qui authentifie le client.
  - L'interface Ethernet physique qui se connecte au modem DSL est ensuite activée à l'aide de la commande **pppoe enable**.
  - L'interface de numérotation est liée à l'interface Ethernet à l'aide des commandes **dialer pool** et **pppoe-client**, en utilisant le même numéro.
  - L'unité de transmission maximale (MTU) doit être diminuée à la valeur 1492, par rapport à la valeur par défaut 1500, et ce, afin de prendre en compte les en-têtes PPPoE.
- Vérification du protocole PPPoE
  - La commande **show ip interface brief** est émise pour vérifier l'adresse IPv4 affectée automatiquement à l'interface de numérotation par le routeur du FAI.
  - La commande **show interface dialer** vérifie l'encapsulation MTU et PPP configurée sur l'interface de numérotation.
  - La commande **show pppoe session** permet d'afficher des informations sur les sessions PPPoE actuellement actives.
  - Les adresses MAC Ethernet peuvent être vérifiées en exécutant la commande **show interfaces** sur chaque routeur.

Mise en œuvre de PPPoE

- Dépannage de PPPoE
  - Vérifiez la négociation PPP à l'aide de la commande **debug ppp negotiation**.
  - Réexaminez la sortie de la commande **debug ppp negotiation**.
  - La valeur MTU prise en charge par PPPoE est 1 492 octets seulement, afin d'accueillir l'en-tête PPPoE supplémentaire de 8 octets.
  - La commande d'interface **ip tcp adjust-mss** *taille-max-segment* ajuste la valeur MSS pendant la connexion TCP en trois étapes.



3.3 VPN

VPN

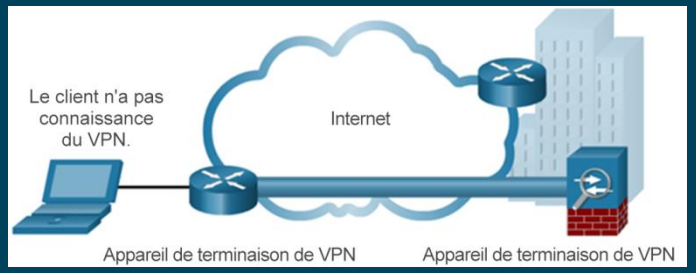
Notions de base des VPN

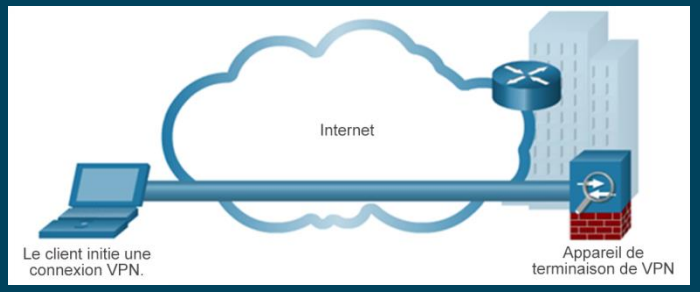
- Présentation des VPN
  - Les entreprises utilisent des VPN pour créer une connexion réseau privée de bout en bout sur un réseau tiers, par exemple Internet.
  - À l'heure actuelle, l'implémentation sécurisée de VPN avec chiffrement, tels que des VPN IPsec, correspond à ce qu'on entend habituellement par réseau privé virtuel.
  - Une passerelle VPN est requise pour l'implémentation de VPN. La passerelle VPN peut être un routeur, un pare-feu ou un périphérique Cisco ASA (Adaptive Security Appliance).
- Bénéfices des réseaux privés virtuels
  - Économies
  - Évolutivité
  - Compatibilité avec la technologie haut-débit
  - Sécurité

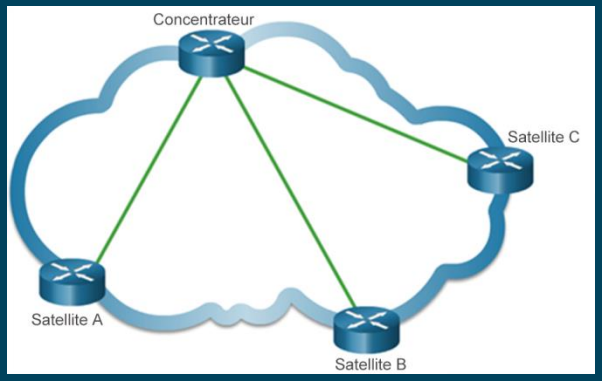
VPN

Types de VPN

- Site à site
  - Les VPN site à site connectent entre eux des réseaux entiers. Ils peuvent par exemple connecter un réseau de filiale au réseau du siège d'une entreprise.
- Accès à distance
  - Les VPN d'accès à distance sont utilisés pour la connexion d'hôtes individuels devant accéder en toute sécurité au réseau de leur entreprise via Internet.
- DMVPN
  - DMVPN (Dynamic Multipoint VPN) est une solution logicielle de Cisco qui permet de créer plusieurs VPN de façon simple, dynamique et évolutive.







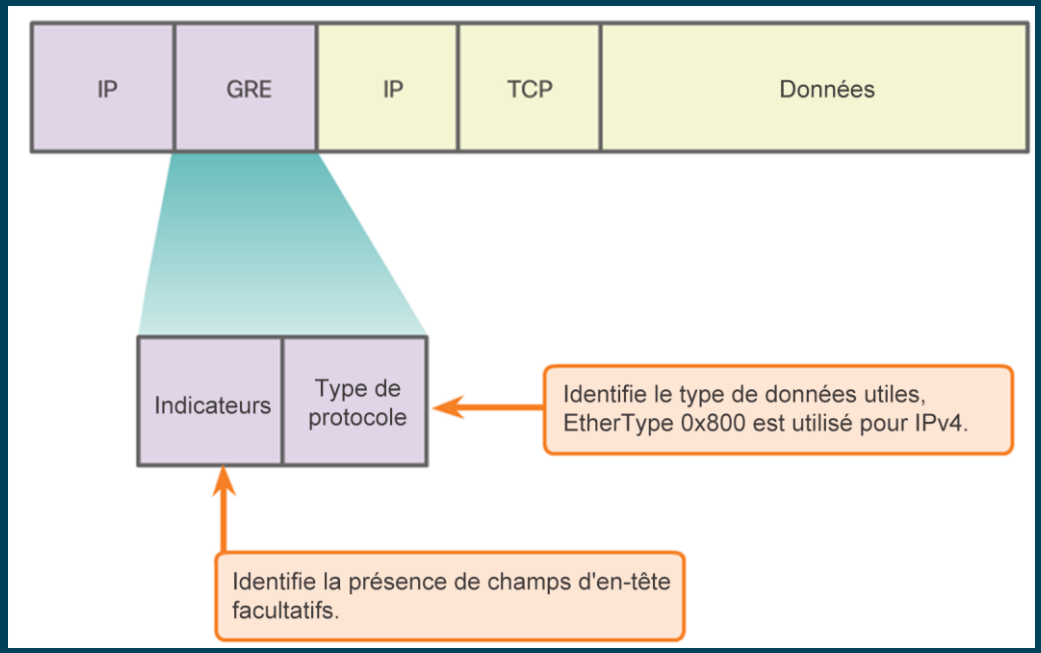
3.4 GRE

GRE

Présentation de GRE

- Introduction au protocole GRE
  - Le protocole GRE (Generic Routing Encapsulation) est conçu pour gérer le transport du trafic multiprotocole et multidiffusion IP entre deux sites ou plus, qui peuvent ne posséder que la connectivité IP.

- Caractéristiques du protocole GRE
  - Le tunneling IP à l'aide du protocole GRE permet l'extension du réseau au sein d'un environnement fédérateur à protocole unique.



Mise en œuvre de GRE

- La configuration d'un tunnel GRE s'effectue en cinq étapes :
  - **Étape 1.** Créez une interface de tunnel à l'aide de la commande **interface tunnel number**.
  - **Étape 2.** Configurez une adresse IP pour l'interface du tunnel. Il s'agit normalement d'une adresse IP privée.
  - **Étape 3.** Spécifiez l'adresse IP source du tunnel.
  - **Étape 4.** Spécifiez l'adresse IP de destination du tunnel.
  - **Étape 5.** (Facultatif) Spécifiez le mode de tunnel GRE en tant que mode d'interface de tunnel.

Commande	Description
`tunnel mode gre ip`	Spécifie que le mode de l'interface du tunnel est GRE sur IP.
`tunnel source` *ip_address*	Spécifie l'adresse source du tunnel.
`tunnel destination` *ip address*	Spécifie l'adresse de destination du tunnel.
`ip address` *ip_address mask*	Spécifie l'adresse IP de l'interface du tunnel.

Mise en œuvre de GRE

- Vérification du protocole GRE
  - Afin de déterminer si l'interface de tunnel est active ou non (état « up » ou « down »), exécutez la commande **show ip interface brief**.
  - Pour vérifier l'état d'un tunnel GRE, exécutez la commande **show interface tunnel**.
  - Vérifiez qu'une contiguïté OSPF est établie sur l'interface du tunnel à l'aide de la commande **show ip ospf neighbor**.
- Dépannage de la fonctionnalité GRE
  - Utilisez la commande **show ip interface brief** sur les deux routeurs pour vérifier que l'interface du tunnel est active et configurée avec les adresses IP correctes pour l'interface physique et l'interface du tunnel.
  - Utilisez la commande **show ip ospf neighbor** pour vérifier la contiguïté des voisins.
  - Utilisez **show ip route** pour vérifier que les réseaux sont transmis entre les deux routeurs.

3.5 eBGP

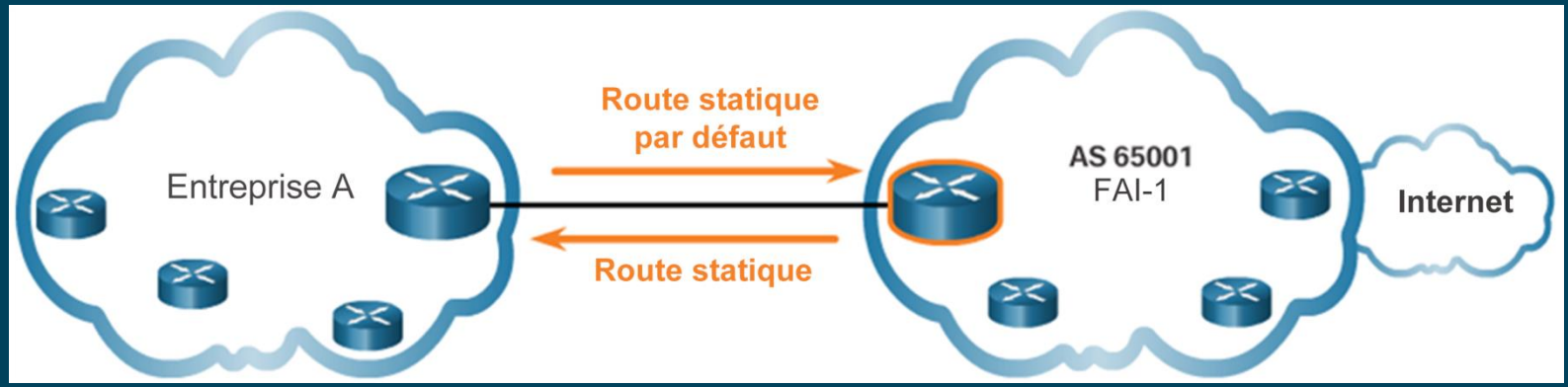
Présentation de BGP

- Protocoles IGP et EGP
  - Les protocoles IGP (Interior Gateway Protocol) permettent d'échanger des informations de routage dans un réseau d'entreprise ou un système autonome (AS).
  - Les protocoles EGP (Exterior Gateway Protocol) permettent d'échanger des informations de routage entre des systèmes autonomes.
- eBGP et iBGP
  - BGP externe (eBGP) est le protocole de routage utilisé entre les routeurs de différents systèmes autonomes.
  - BGP interne (iBGP) est le protocole de routage utilisé entre les routeurs d'un même système autonome.
- Ce cours traite uniquement de l'eBGP.

eBGP

Considérations de conception BGP

- Quand utiliser le protocole BGP
  - L'utilisation du protocole BGP est indiquée lorsqu'un système autonome se connecte à plusieurs systèmes autonomes.
  - N'utilisez pas BGP si au moins l'une des conditions suivantes est remplie :
    - Connexion unique à Internet ou un autre système autonome - C'est ce qu'on appelle le « single-homing » ou résidence simple.
    - Connaissances limitées de BGP.



Considérations de conception BGP

- Options BGP
  - Dans un environnement multirésident, une entreprise peut implémenter BGP de l'une des trois manières suivantes :
    - Route par défaut uniquement - il s'agit de la méthode la plus simple pour mettre en œuvre BGP. Cependant, dans la mesure où l'entreprise reçoit une route par défaut des deux FAI, les performances de routage risquent d'être sous-optimales.
    - Route par défaut et routes de FAI - cette option permet à l'entreprise A de transférer le trafic vers le FAI approprié pour les réseaux annoncés par ce FAI.
    - Toutes les routes Internet - dans la mesure où elle reçoit toutes les routes Internet des deux FAI, l'entreprise A peut déterminer celui qui offre le meilleur chemin pour transférer le trafic pour tout type de réseau. Si cette solution résout le problème de performances de routage, elle implique cependant que le routeur BGP de l'entreprise A contienne toutes les routes Internet.

Configuration de succursale BGP

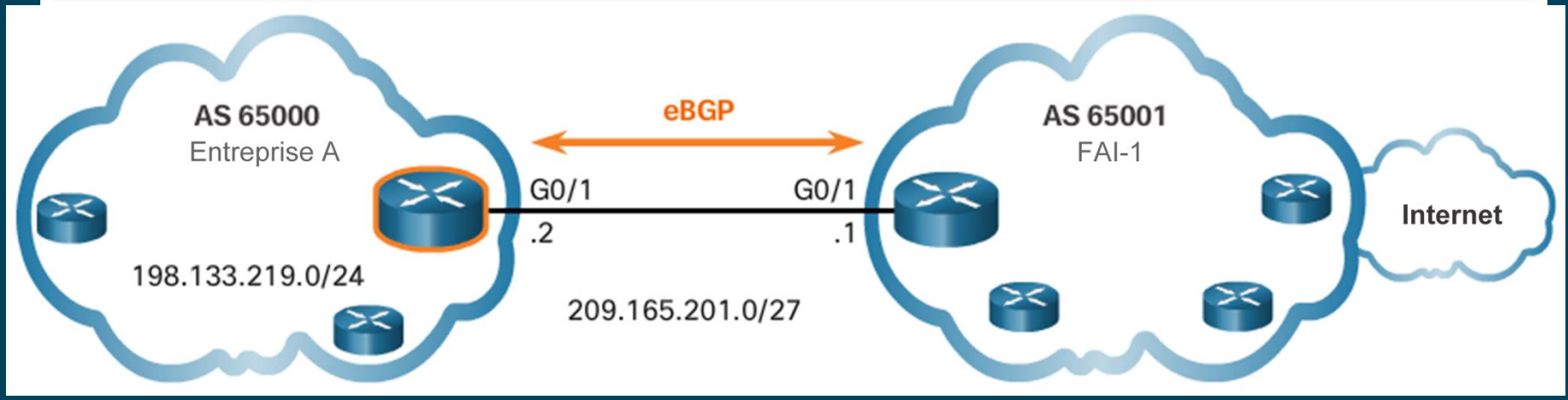
- Commandes de configuration BGP
  - La mise en œuvre d'eBGP requiert trois étapes :
    - **Étape 1** : Activer le routage BGP.
    - **Étape 2** : Configurer les voisins (pairs) BGP.
    - **Étape 3** : Annoncer les réseaux provenant de ce système autonome (AS).

Commande	Description
`Router(config)# router bgp as-number`	Active un processus de routage BGP et place le routeur en mode de configuration.
`Router(config-router)# neighbor ip-address remote-as as-number`	Spécifie un voisin BGP. Le numéro AS est le numéro AS du voisin.
`Router(config-router)# network network-address [mask network-mask]`	Annonce une adresse réseau à un voisin eBGP en indiquant qu'elle provient de cet AS. Le masque de réseau est le masque de sous-réseau du réseau.

Configuration de succursale BGP

- Vérification eBGP
  - Trois commandes peuvent être utilisées pour vérifier eBGP

Commande	Description
`Router# show ip route`	Permet de vérifier que les routes annoncées par le voisin BGP figurent bien dans la table de routage IPv4.
`Router# show ip bgp`	Permet de vérifier que les réseaux IPv4 reçus et annoncés figurent bien dans la table BGP.
`Router# show ip bgp summary`	Permet de vérifier les voisins BGP IPv4 et d'autres informations BGP.



3.6 Synthèse du chapitre

Synthèse du chapitre

Synthèse

- La transmission haut débit est fournie par un large éventail de technologies, y compris DSL, FFTH (fibre optique jusqu'au domicile), systèmes de câbles coaxiaux, sans fil et satellite. Cette transmission nécessite la présence de composants supplémentaires à la fois au domicile de l'abonné et au niveau de l'entreprise. Les solutions sans fil haut débit incluent le Wi-Fi municipal, les réseaux cellulaires/mobiles et Internet par satellite. Les réseaux maillés Wi-Fi municipaux ne sont pas fréquents. La couverture des solutions cellulaires/mobiles est parfois limitée et leur bande passante peut représenter un problème. L'accès Internet par satellite est relativement cher et limité, mais il s'agit parfois de la seule solution possible.
- Si plusieurs connexions haut débit sont disponibles à un emplacement spécifique, une analyse coûts/avantages doit être effectuée en vue de déterminer la meilleure solution. Il se peut que la meilleure solution consiste à se connecter à plusieurs fournisseurs de services pour des raisons de redondance et de fiabilité.
- PPPoE est un protocole répandu de liaison des données permettant de connecter des réseaux distants à leurs FAI. PPPoE fournit la flexibilité de PPP et la commodité d'Ethernet.

Synthèse - Suite

- Les VPN servent à créer une connexion sécurisée de bout en bout par réseau privé sur un réseau tiers, par exemple Internet. La technologie GRE est un protocole de tunneling VPN de site à site de base, non sécurisé, capable d'encapsuler une large variété de types de paquets de protocoles au sein de tunnels IP, permettant ainsi à une entreprise de fournir d'autres protocoles par l'intermédiaire d'un WAN IP. À l'heure actuelle, ce protocole est principalement utilisé pour l'acheminement de trafic de multidiffusion IP ou de trafic IPv6 sur une connexion IPv4 de monodiffusion uniquement.
- BGP est le protocole de routage implémenté entre des systèmes autonomes. Les trois options de conception de base pour eBGP sont les suivantes :
- Le FAI annonce une route par défaut seulement pour le client.
- Le FAI annonce au client une route par défaut ainsi que toutes ses routes.
- Le FAI annonce au client toutes les routes Internet.
- L'implémentation d'eBGP au sein d'un réseau à résidence unique requiert seulement quelques commandes.