ANTISECHE 1: Réseau

Plan de zone

Zone 1

La zone 1 représente “le grand extérieur”, une zone externe interagissant avec le système d'information de la DGFIP. En d'autres termes, cette zone regroupe l’ensemble des réseaux non maîtrisés par la DGFIP, et pour lesquels aucun “contrat de services partenaires” ne peut être formalisé, incluant au premier plan le réseau Internet. De fait, la zone 1 représente la menace la plus forte pour la DGFIP, c'est-à-dire la source la plus probable d'attaques.

Zone 2 Publique

La Zone 2 Publique est l'interface du système d'information de la DGFIP avec l'extérieur, la zone 1. Il s'agit d'une zone tampon entre les réseaux externes et le reste du réseau Interne de la DGFIP. En plus du filtrage et du traitement des flux non légitimes en provenance de l'extérieur, cette zone doit permettre une première rupture de protocole. Ce principe apporte le double avantage, de présenter des données aux utilisateurs extérieurs sans compromettre les autres zones internes, et d'améliorer les performances en aval. Une zone d'isolation entre les usagers et le cœur applicatif, hébergé en zone 2 privée. Cette zone, divisée en sous-ensembles logiques et isolés, communément appelées zones démilitarisées (DMZ) publiques, héberge :

- les services d'authentification et/ou reverse-proxy (Dispositif d’Accès et de Contrôle des flux, LemonLDAP::NG…) ;
- les serveurs du portail publique de l’administration fiscale (SYRACUSE) ;
- les services d'infrastructures (proxys Internet, DNS, messagerie…).

En conséquence, seules les serveurs devant être directement accessibles depuis la zone 1 sont situées dans une DMZ de la zone 2 publique.

Zone 2 Privée

La Zone 2 Privée héberge, également avec application du principe de zones démilitarisées (DMZ), le cœur des services DGFIP ouverts sur la zone 1, et pouvant être, le cas échéant, également accessible du réseau DGFIP. En d'autres termes, les DMZ privées accueillent principalement des serveurs applicatifs et de données (base de données, annuaires…), avec un positionnement en aval d'un reverse-proxy ou d'une brique d'authentification présents au sein de la zone 2 publique. Dans le principe de défense en profondeur, ce positionnement permet un second étage de filtrage, et donc une isolation complémentaire du cœur applicatif, par rapport à la zone la moins sécurisée, à savoir la zone 1.

Zone 3

La Zone 3 correspond au réseau privé virtuel (VPN) nommé “RUBIS”, et tous les réseaux locaux connectés à ce VPN sans filtrage. Cet espace commun de confiance permet de relier l’ensemble des ressources physiquement présentes et raccordées sur les différents sites de l'Administration Fiscale.
Nota :

- des équipements, physiquement distants, peuvent accéder, sous contrôle, à des ressources de cet espace via les équipements d'interconnexions de la zone 5 ou de la Z6. Dans ce cas, elles sont connectées à la zone 3, mais en aucun cas considérées à même niveau de confiance qu'une ressource zone 3.
- un équipement présent initialement en zone 3 mais justifiant, pour des raisons de sécurité, un besoin d'isolation, doit être positionné en zone 3 renforcée

Zone 4

La Zone 4 correspond à la zone d'administration de l'ensemble des équipements du réseau DGFIP, c'est-à-dire au cloisonnement des fonctions d’exploitation, d’administration et de supervision au sein d’un même sous-réseau, sécurisé et physiquement séparé des autres sous-réseaux. Cette zone est construite, à l'instar de la zone 3, sur un VPN opérateur afin d'interconnecter les équipements d'administration des différents sites DGFIP. Ce réseau d’administration est exclusivement à l’usage des exploitants, et chaque équipement administré doit avoir une interface réseau dédiée à l'administration connectée à la zone 4, et ce quelque soit sa zone d'hébergement. Tous les flux inter-zones impliquant la zone 4 doivent être à l'initiative de cette dernière, y compris avec la zone 4 pushable.

Tout équipement administré par la zone 4 doit être équipé d'une interface réseau dédiée.

Zone 4 pushable

La Zone 4 pushable rassemble, dans un contexte de mutualisation, des fonctions d’administration nécessitant des échanges bidirectionnel, incluant donc des échanges à l’initiative des équipements hébergés dans les autres zones. Pour rappel ce sens de flux est strictement interdit vers la zone 4 d'administration. La mutualisation est actuellement possible uniquement pour les fonctions clairement identifiées suivantes :

- sauvegarde,
- supervision,
- déploiement,
- “grid control”.

La mutualisation porte uniquement sur des équipements accédant à des zones identiques. En d'autres termes, un équipement mutualisé commun à des machines situées dans des zones différentes (par exemple zone 2 publique ou zone 2 privée) est

interdit.

Zone 5

La Zone 5 représente l'espace partenaire. En effet, les partenaires bénéficient ainsi d'un accès privilégié aux ressources du réseau interne de la DGFIP. Inversement, l'usage de cette zone peut également répondre à des besoins d'accès à des ressources partenaires à partir du réseau interne DGFIP. Les partenaires peuvent être de natures diverses, par exemples :

- autres directions du Ministère du Budget, des Comptes publics et de la Réforme de l'État,
- autres ministères,
- ordonnateurs,
- institutionnels,
- prestataires de tierces maintenance applicative (TMA),
- prestataires au niveau métier (banques)...

Zone 6

La Zone 6 représente l'espace contenant les agents des administrations financières pouvant accéder aux ressources du réseau interne de la DGFIP de manière sécurisée, tout en travaillant depuis un site externe à partir d'un poste nomade. Ces postes sont soumis à des directives et règles opérationnelles de sécurité informatique.

Zone 7

La Zone 7 représente l'interconnexion ou l'extension de DMZ de la zone 2 privée. En d'autres termes, cette zone peut permettre d'interconnecter deux DMZ privées hébergées dans des Passerelles d'Accès Sécurisées différentes.

Zone 8

La Zone 8 représente l'espace de secours permettant la réplication entre les serveurs de données du service nominal et ceux du service de secours présents sur un site distant. Cette zone peut également être support de réplications de serveurs de données dérogatoires entres zones, sous certaines conditions dont :

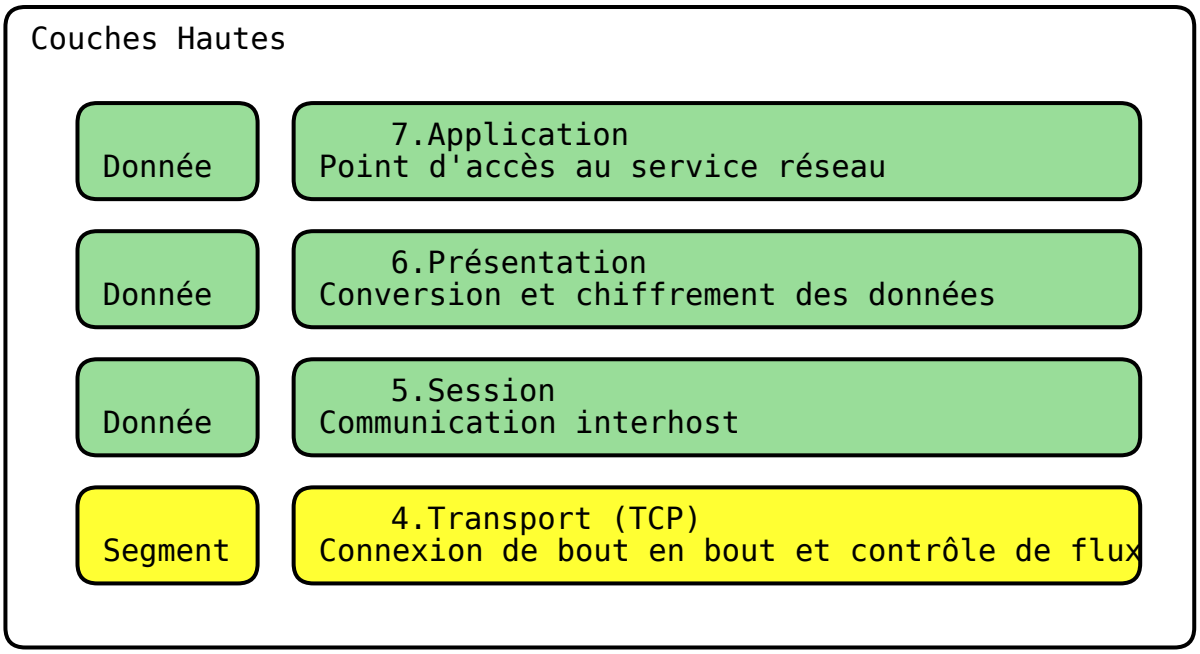
- le respect des sens de flux du plan de zone,
- réplication entre serveurs présents sur le même site géographique,
- des principes de durcissement des serveurs de données (mots de passe différents...).

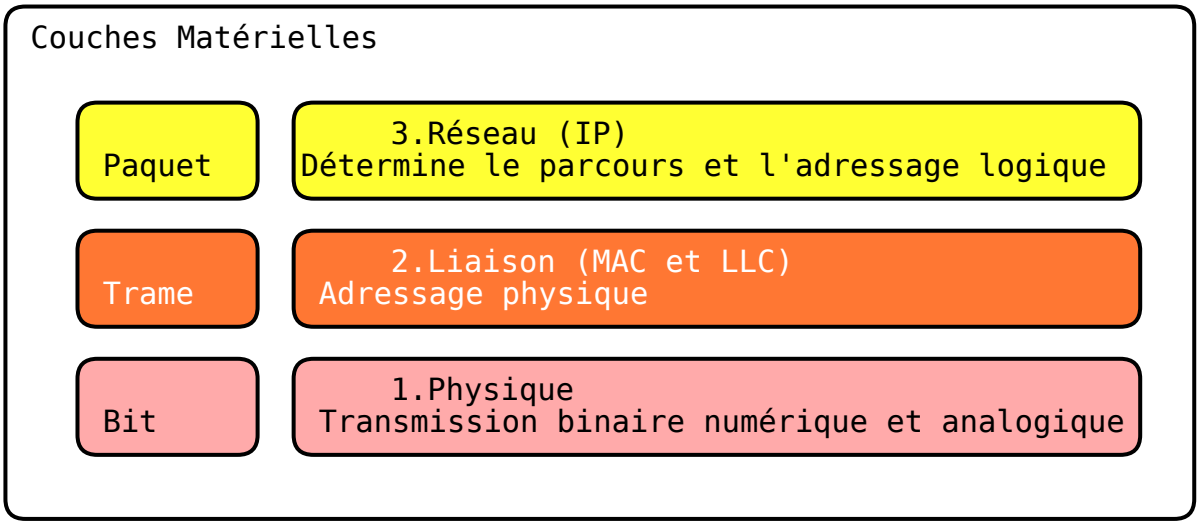
L'usage de cette zone nécessite une interface réseau dédiée à la zone 8 pour les serveurs impliqués dans le processus de réplication.

Interconnexion Réseau

Modèle OSI

	PDU	Couche	Fonction	
Couches hautes	Donnée	7	Application	Point d'accès aux services réseau
		6	Présentation	Gère le chiffrement et le déchiffrement des données, convertit les données machine en données exploitables par n'importe quelle autre machine
		5	Session	Communication Interhost, gère les sessions entre les différentes applications
	Segment (en) Datagramme	4	Transport	Connexion de bout en bout, connectabilité et contrôle de flux ; notion de port (TCP et UDP)
Couches matérielles	Paquet	3	Réseau	Détermine le parcours des données et l'adressage logique (adresse IP)
	Trame	2	Liaison	Adressage physique (adresse MAC)
	Bit	1	Physique	Transmission des signaux sous forme numérique ou analogique





La couche de liaison de données Ethernet IEEE comporte deux sous-couches : * Media Access Control (MAC) 802.3: Définit comment les paquets sont placés sur le média. * Logical Link Control (LLC) 802.2: Responsable de l'identification des protocoles de la couche réseau

hubs, routeurs, concentrateurs et ponts

- **Les hubs**: Ne segmentent pas un réseau ; ils connectent simplement des segments de réseau entre eux. Les concentrateurs, comme les répéteurs, n'examinent aucune partie du trafic lorsqu'il entre et est ensuite transmis aux autres parties du support physique. Chaque appareil connecté au hub, ou aux hubs, doit écouter si un périphérique transmet.
- **Les routeurs**: Sont utilisés pour connecter des réseaux entre eux et acheminer des paquets de données d'un réseau à un autre. Les routeurs sont en réalité des commutateurs ; ce sont en fait ce que l'on appelle des commutateurs de couche 3. **Les routeurs brisent les domaines de diffusion par défaut, mais ils divisent également les domaines de collision.**
- **Les commutateurs**:Ne sont pas utilisés pour créer des interréseaux (ils ne divisent pas les

domaines de diffusion par défaut) ; ils sont employés pour ajouter des fonctionnalités à un réseau LAN. L'objectif principal d'un commutateur est d'améliorer le fonctionnement d'un réseau local, d'optimiser ses performances, de fournir plus de bande passante pour les utilisateurs du LAN. Et les commutateurs ne transfèrent pas les paquets vers d'autres réseaux comme le font les routeurs. Au lieu de cela, ils ne « commutent » que les trames d'un seul port à un autre au sein du réseau commuté.**Par défaut, les commutateurs divisent les domaines de collision.**

- **Les ponts**:Les ponts et les commutateurs font essentiellement la même chose. Un commutateur est fondamentalement un pont à plusieurs ports mais avec une capacité de gestion et des fonctionnalités considérablement améliorées.

Ethernet

Domaine de collision

Un périphérique envoie un paquet sur un segment de réseau, forçant ainsi tous les autres appareils sur ce même segment de réseau physique à y prêter attention. Cela peut être mauvais car si deux appareils sur un segment physique transmettent en même temps, un événement de collision - une situation où les signaux numériques de chaque appareil interférer avec un autre sur le fil - se produit et force les appareils à retransmettre plus tard.

Domaine de diffusion

Le domaine de diffusion fait référence à un groupe d'appareils sur un segment de réseau qui entendent toutes les diffusions envoyées sur ce segment réseau.

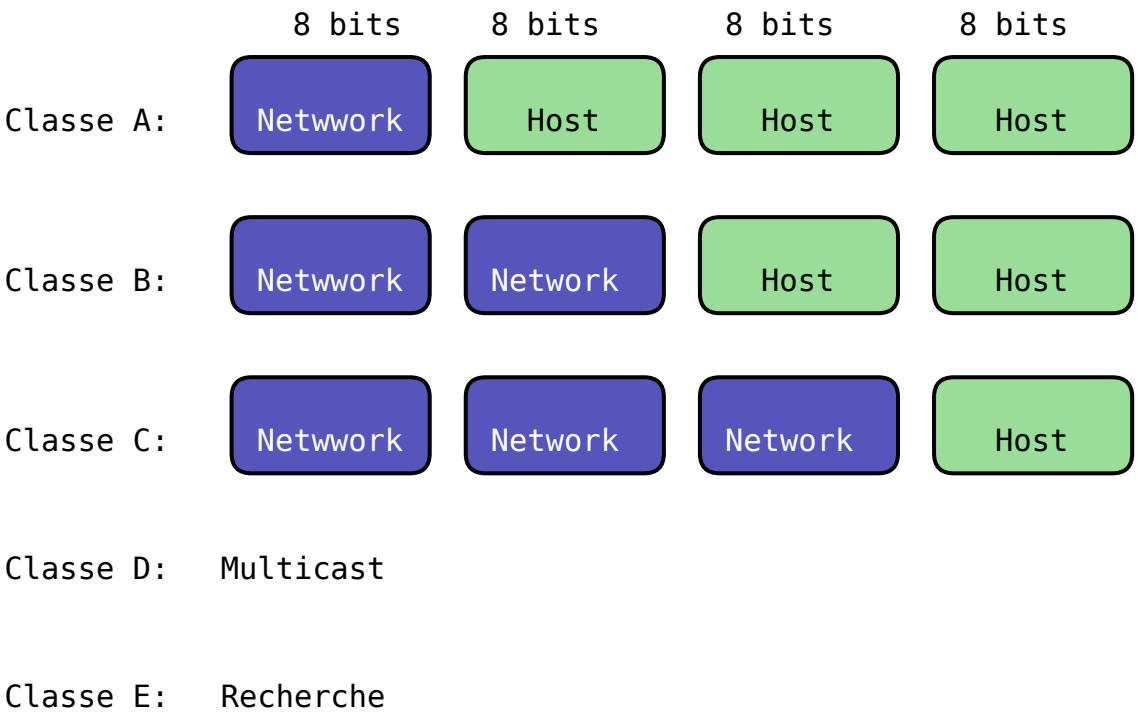
CSMA/CD

Ethernet utilise Carrier Sense Multiple Access with Collision Detection (CSMA/CD), un protocole qui aide les appareils à partager la bande passante uniformément sans que deux appareils transmettent en même temps sur le support réseau. CSMA/CD a été créé pour surmonter le problème de ces collisions qui se produisent lorsque des paquets sont transmis simultanément à partir de différents nœuds.

modèle hiérarchique à trois couches de Cisco

- La couche centrale = cœur du réseau, au sommet de la hiérarchie, la couche centrale est responsable du transport de grandes quantités de trafic
- La couche de distribution = point de communication entre la couche d'accès et le noyau
- La couche d'accès = contrôle l'accès des utilisateurs

TCP/IP



Les adresses privées réservées sont répertoriées dans le Tableau suivant:

Classe d'adresse	Espace d'adressage réservé
Classe A	10.0.0.0 à 10.255.255.255
Classe B	172.16.0.0 à 172.31.255.255
Classe C	192.168.0.0 à 192.168.255.255

Les quatre types d'adresses IPv4:

- **Diffusions de couche 2**: Elles sont envoyées à tous les nœuds d'un réseau local.
- **Diffusions (couche 3)**: Elles sont envoyées à tous les nœuds du réseau.
- **Unicast**: Il s'agit d'une adresse pour une seule interface, et celles-ci sont utilisées pour envoyer des paquets à un seul hôte de destination.
- **Multidiffusion**: Ce sont des paquets envoyés à partir d'une seule source et transmis à de nombreux appareils sur différents réseaux. Appelé « un-à-plusieurs ».

Les sous Réseaux

Routage inter-domaines sans classe (CIDR)

le routage interdomaine sans classe (CIDR) est essentiellement la méthode que les FAI (fournisseur de service Internet) utilisent pour attribuer un certain nombre d'adresses à une entreprise, un domicile, un client. Ils fournissent des adresses dans une certaine taille de bloc.

Voici une liste de puissances 2 à mémoriser :

2^1 = 2
2^2 = 4
2^3 = 8
2^4 = 16
2^5 = 32
2^6 = 64
2^7 = 128
2^8 = 256
2^9 = 512
2^10 = 1 024
2^11 = 2 048
2^12 = 4 096
2^13 = 8 192
2^14 = 16 384
2^15 = 32 768
2^16 = 65 536

Voici une petite astuce pour travailler avec les puissances 2 : Chaque puissance successive de 2 est le double de la précédente.
Par exemple, tout ce qu'on a à faire pour retenir la valeur de 2^9 est de savoir d'abord que 2^8 = 256. Pourquoi ? Parce que lorsqu'on double la puissance huit (256), on obtien 2^9 (ou 512). Pour déterminer la valeur de 2^10, on commence simplement à 2^8 = 256, puis on la double deux fois.

On peut aussi aller dans l'autre sens. Si on besoin de savoir ce qu'est 2^6, par exemple, il suffit de couper 256 en deux deux fois : une fois pour atteindre 2^7, puis une fois de plus pour atteindre 2^6.

Masques de sous-réseau de longueur variable (VLSM)

la mise en réseau VLSM est un moyen simple de prendre un réseau et de créer de nombreux réseaux en utilisant des masques de sous-réseau de différentes longueurs sur différents types de conceptions de réseaux.

Routage

Types et classes de protocoles de routage

- Deux types de protocoles de routage sont utilisés dans les interréseaux : les protocoles de passerelle intérieure (**IGP**) et les protocoles de passerelle extérieure (**EGP**). Les **IGP** sont utilisé pour échanger des informations de routage avec des routeurs dans le même système autonome (**AS**). Un **AS** est un ensemble de réseaux sous un même domaine administratif, ce qui signifie essentiellement que tous les routeurs partageant les mêmes informations de table de routage sont dans le même **AS**. Les **EGP** sont utilisés pour communiquer entre les **AS**. Un exemple d'**EGP** est le Border Gateway Protocol (**BGP**).
- Il existe trois classes de protocoles de routage: les protocoles de **vecteur de distance** utilisés

aujourd'hui trouvent le meilleur chemin vers un réseau distant en jugeant la distance, les protocoles **à état de liaison**, également appelés protocoles du chemin le plus court en premier, les routeurs créent chacun trois tables distinctes. Une de ces tables assure le suivi des voisins directement attachés, l'une détermine la topologie de l'ensemble de l'interréseau et l'autre est utilisé comme table de routage, les protocoles **hybrides** utilisent des aspects à la fois du vecteur de distance et de l'état de liaison, par exemple, EIGRP

Protocoles de routage

- Le protocole d'information de routage (**RIP**) est un protocole de routage à vecteur de distance. Protocoles de routage à vecteur de distance
- Enhanced IGRP (**EIGRP**) est un protocole à vecteur de distance amélioré sans classe qui utilise le concept d'un système autonome (**AS**) pour décrire l'ensemble des routeurs contigus qui exécutent le même protocole de routage et partagent des informations de routage. EIGRP utilise Diffusing update algorithm (**DUAL**) pour sélectionner et maintenir le meilleur chemin vers chaque réseau distant.
- Open Shortest Path First (**OSPF**) est un protocole de routage à état de lien (**DR**=Routeur désigné, **BDR**=Routeur désigné de secours, **LSA**=Annonce d'état de liaison paquet de données OSPF contenant des informations d'état de liaison et de routage partagé entre les routeurs OSPF,

Termes à connaitre

- **Congestion sténopé**: survient lorsque les deux liens vers un réseau distant ont des bandes passantes différentes mais le même compte de saut
- **Boucles de routage**: pour éviter que les boucles ne se produisent on dispose:
  - nombre maximum de sauts
  - horizon partagé (Split Horizon) règle selon laquelle les informations de routage ne peuvent pas être renvoyées dans la direction à partir de laquelle elles ont été reçues.
  - Empoisonnement d'itinéraire
  - Retenues empêche les messages de mise à jour réguliers de rétablir un itinéraire qui monte et descend (appelé battement).

VLAN

Méthodes d'identification des VLAN

- Lien inter-commutateur (**ISL**): Inter-Switch Link (ISL) est un moyen de marquer explicitement les informations VLAN sur une trame Ethernet
- **IEEE 802.1Q**: méthode standard de marquage de trame, IEEE 802.1Q insère en fait un champ dans la trame pour identifier le VLAN. Si on est dans un trunk entre une liaison commutée Cisco avec d'autres marques de commutateurs, il faut utiliser 802.1Q pour que le trunk fonctionne.

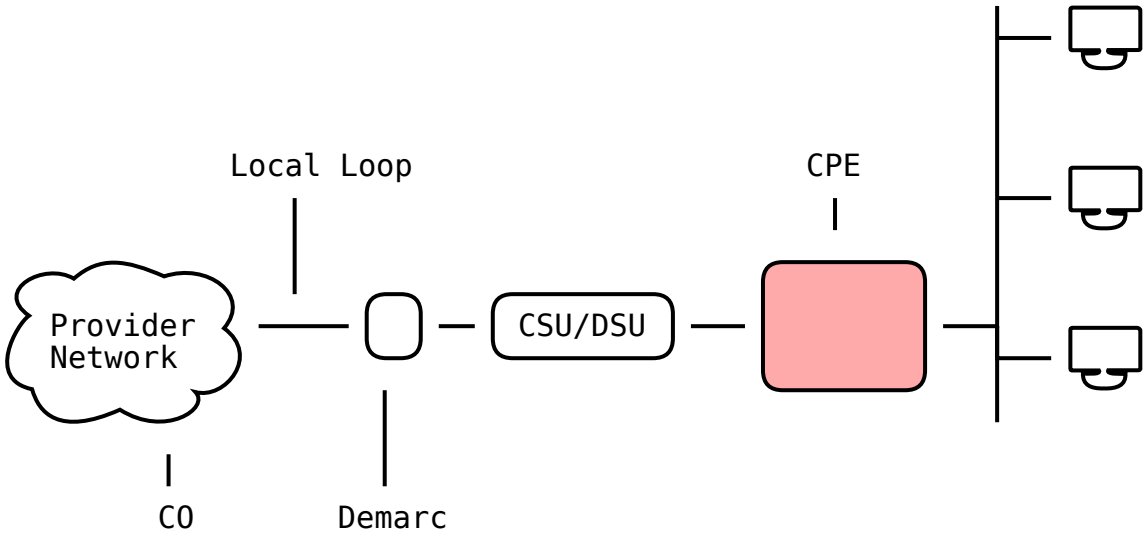
Balisage des trames (tagging)

- Le marquage des trames attribue de manière unique un ID de VLAN défini par l'utilisateur à

chaque trame. Parfois, les gens l'appellent un ID de VLAN.
- Une fois que la trame atteint une sortie déterminée par la table de transfert/filtre comme étant un lien d'accès correspondant à l'ID de VLAN de la trame, le commutateur supprime l'identifiant du VLAN. C'est ainsi que le périphérique de destination peut recevoir les trames sans avoir à comprendre leur identification VLAN.
- Un port trunk a un Port VLAN ID attribué par défaut (PVID) pour un VLAN sur lequel transitera tout le trafic non balisé.

Réseau WAN

Les services fournisseurs



- **Customer premises equipment (CPE)**: L'équipement des locaux du client (CPE) est un équipement qui appartient généralement (mais pas toujours) à l'abonné et situé dans les locaux de l'abonné.
- **Demarcation point**: Le point de démarcation est l'endroit précis où s'achève la responsabilité du prestataire et où commence le CPE. C'est généralement un appareil dans un placard de télécommunications détenu et installé par la société de télécommunications. Il est de la responsabilité de l'abonné de câbler (démarcation étendue) de cette boîte au CPE, qui est généralement une connexion à une interface CSU/DSU ou RNIS.
- **Local loop**: La boucle locale relie la démarcation au central téléphonique le plus proche, appelé central office.
- **Central office (CO)**: Ce point relie le réseau du client au réseau de commutation du fournisseur. Un central office (CO) est parfois appelé **P**oint **O**f **P**resence (**POP**).
- **Toll network**: Le réseau à péage est une ligne principale à l'intérieur du réseau d'un fournisseur WAN. Ce réseau est un ensemble de commutateurs et d'installations appartenant au FAI.

Les équipements

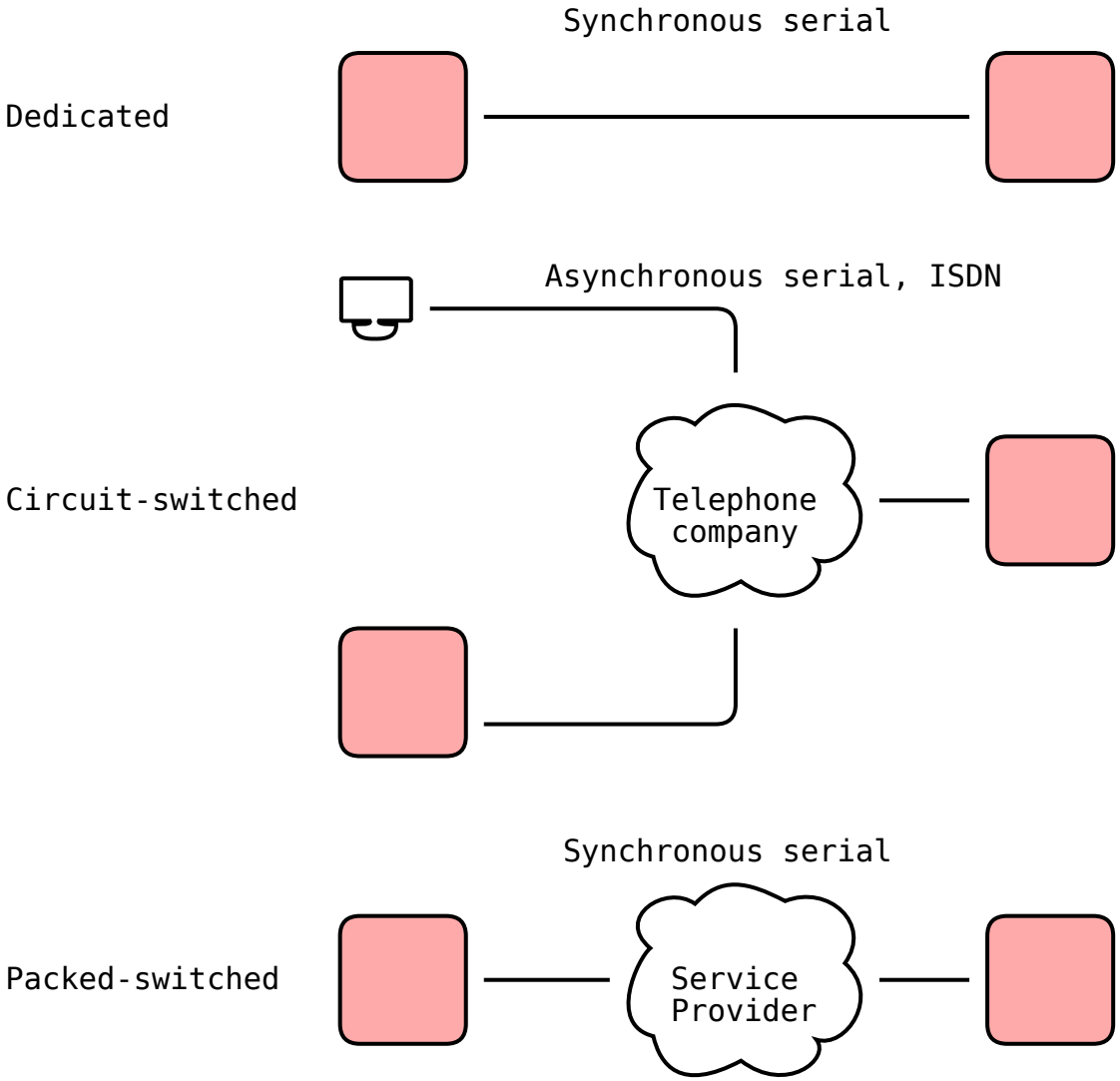
- Un équipement terminal de données (**DTE**) ou **ETTD** est un équipement qui est soit une source, soit une destination pour les données numériques. Les **DTE** ne communiquent généralement

pas les uns avec les autres, ils doivent donc utiliser **DCE** pour établir la communication. Le **DTE** n'a pas besoin de savoir comment les données sont envoyées ou reçues; les détails de la communication sont laissés au **DCE**. Un exemple typique de DTE est un **ordinateur**.

- Les équipements de communication de données (**DCE**) ou **ETCD** peuvent être classés comme des équipements qui transmettent ou reçoivent des signaux analogiques ou numériques via un réseau. **DCE** travaille au niveau de la couche physique du modèle OSI en prenant les données générées par un équipement terminal de traitement de données (**DTE**) et en les convertissant en un signal pouvant ensuite être transmis sur une liaison de communication. Un exemple courant de **DCE** est un **modem** qui fonctionne comme un traducteur de signaux numériques et analogiques.
- Une unité **CSU/DSU** est une interface numérique - ou parfois deux unités numériques distinctes - qui adapte l'interface physique d'un **DTE** (par exemple, un terminal) à celle d'un **DCE** (par exemple, un commutateur) dans un réseau commuté. Les unités CSU/DSU sont parfois intégrées au routeur.

Types de connexion WAN

Un WAN peut utiliser un certain nombre de types de connexion différents, et on va voir chacun des différents types de connexions WAN qu'on trouve sur le marché aujourd'hui. La figure suivante montre les différents types de connexion WAN qui peuvent être utilisés pour connecter les réseaux locaux (DTE) sur un réseau DCE.



Bande passante de connexion WAN

- **Digital Signal 0 (DS0)**: Il s'agit du débit de signalisation numérique de base de 64 Kbit/s, équivalent à un canal. C'est le circuit numérique de plus petite capacité. 1 DS0 = 1 ligne voix/données.
- **T1** Également appelé DS1, il contient 24 circuits DS0 regroupés avec une bande passante totale de 1,544 Mbps.
- **E1** Équivalent européen du T1. Contient 30 circuits DS0 regroupés avec une bande passante de 2,048 Mbps.
- **T3** Appelé DS3, il comprend 28 DS1 regroupés, ou 672 DS0, avec une bande passante de 44,736 Mbps.
- **OC-3** Optical Carrier (OC) 3, utilise la fibre, est composé de trois DS3 regroupés et contient 2 016 DS0 avec une bande passante totale de 155,52 Mbps.
- **OC-12** Optical Carrier 12 est composé de quatre OC-3 regroupés et contient 8 064 DS0 avec une bande passante totale de 622,08 Mbps.
- **OC-48** Optical Carrier 48 est composé de quatre OC12 regroupés et contient 32 256 DS0 avec une bande passante totale de 2488,32 Mbps.

Les protocoles WAN

- **Frame Relay**: Est une technologie à commutation de paquets. C'est une liaison de données hautes performances et spécification de la couche physique qui fournit des fonctionnalités pour l'allocation dynamique de bande passante et contrôle des encombrements. **Taux d'accès**: La vitesse maximale à laquelle l'interface **Frame Relay** peut transmettre, **Taux d'information engagé (CIR)**: La bande passante maximale des données dont la livraison est garantie. En réalité, c'est le montant moyen que le prestataire permettra de transmettre, **circuits virtuels permanents (PVC)**, **circuits virtuels commutés (SVC)**, **Identifiants de connexion de liaison de données (DLCI)**: les **PVC Frame Relay** sont identifiés auprès des terminaux **DTE** par des identificateurs de connexion de liaison de données (**DLCI**), ils sont localement significatif, utilisés par les opérateurs de télécommunications pour « trouver » l'autre extrémité d'un **PVC**, **ARP inverse (IARP)**: **IARP** est un peu similaire à ARP dans le fait qu'il mappe un **DLCI** à une adresse IP, **Interface de gestion locale (LMI)**: sont glomalement significatis
- **ISDN**: Le réseau numérique à intégration de services **RNIS** (Integrated Services Digital Network **ISDN**) est un ensemble de services numériques qui transmettent la voix et les données sur les lignes téléphoniques existantes.
- **LAPB**: Link Access Procedure, Balanced (**LAPB**) est un protocole orienté connexion au niveau de la couche de liaison de données à utiliser avec X.25, mais il peut également être utilisé comme simple transport de liaison de données. Une caractéristique moins bonne du LAPB est qu'il a tendance à créer une énorme surcharge en raison de ses techniques strictes de temporisation et de fenêtrage.
- **LAPD**: La procédure d'accès au lien D-Channel(Link Access Procedure, D-Channel) est utilisé avec le RNIS au niveau de la couche de liaison de données (couche 2) en tant que protocole pour le canal D (signalisation). LAPD a été dérivé du protocole Link Access Procedure, Balanced (**LAPB**) et est conçu principalement pour satisfaire aux exigences de l'accès de base **RNIS**.
- **HDLC**: Le contrôle de liaison de données de haut niveau (High-Level Data-Link Control) fonctionne au niveau de la couche de liaison de données et crée très peu de surcharge par rapport à LAPB. **HDLC** générique n'était pas destiné à encapsuler plusieurs protocoles de couche réseau sur le même lien - l'en-tête **HDLC** ne contient aucune identification du type de protocole transporté à l'intérieur de l'encapsulation **HDLC**. Pour cette raison, chaque fournisseur qui utilise HDLC a sa propre façon d'identifier le protocole de couche réseau, ce qui signifie que le HDLC de chaque fournisseur est propriétaire en ce qui concerne son équipement spécifique.
- **PPP**: Point-to-Point Protocol (PPP) est un protocole standard utilisé pour créer des liens point à point entre les équipements de différents fournisseurs. Il utilise un champ **N**etwork **C**ontrol **P**rotocol (**NCP**) dans l'en-tête Data Link pour identifier le protocole de couche réseau transporté et permettre l'exécution de connexions d'authentification et de liaisons multiples sur des connexions asynchrones et des liaisons synchrones.
- **PPPoE**: Point-to-Point Protocol over Ethernet encapsule les trames **PPP** dans des trames Ethernet et est généralement utilisé en conjonction avec une prestations de service xDSL.
- **Cable**: Dans un réseau HFC hybride fibre-coaxial moderne, généralement 500 à 2 000 abonnés de données actifs sont connectés à un segment de réseau câblé, tous partageant la bande passante en amont et en aval. HFC est un terme de l'industrie des télécommunications pour un réseau qui intègre fibre optique et câble coaxial pour créer un réseau à large bande. La bande passante réelle du service Internet sur une ligne de télévision par câble (CATV) peut être jusqu'à environ 27 Mbps sur le chemin de téléchargement vers l'abonné, avec environ 2,5 Mbps de bande passante sur le chemin de téléchargement. En général, les utilisateurs obtiennent une vitesse d'accès de 256Kbps à 6Mbps.
- **DSL**: La ligne d'abonné numérique (Digital subscriber line) est une technologie utilisée par les

compagnies de téléphone traditionnelles pour fournir des services avancés (données à haut débit et parfois vidéo) sur des câbles téléphoniques en cuivre à paire torsadée. Il a généralement une capacité de transport de données inférieure à celle des réseaux HFC et des vitesses de données peuvent être limité en portée par la longueur et la qualité des lignes. La ligne d'abonné numérique n'est pas une solution complète de bout en bout mais plutôt une technologie couche physique de transmission comme l'accès commuté, le câble ou le sans fil. Les connexions DSL sont déployées dans le dernier kilomètre d'un réseau téléphonique local—la boucle. La connexion est établie entre une paire de modems DSL à chaque extrémité d'un fil de cuivre qui se trouve entre les locaux du client (**CPE**) et le multiplexeur d'accès de ligne d'abonné numérique (**DSLAM**). Un **DSLAM** est l'appareil situé au bureau central du fournisseur (**CO**) et concentre les connexions de plusieurs abonnés DSL. **DSL symétrique**: Les vitesses des connexions en aval et en amont sont égales ou symétriques, **DSL asymétrique**: Des vitesses de transmission différentes se produisent entre les deux extrémités d'un réseau, la vitesse en aval est toujours plus rapide.

- **MPLS**: MultiProtocol Label Switching (**MPLS**) est un mécanisme de transport de données qui émule certaines propriétés d'un réseau à commutation de circuits sur un réseau à commutation de paquets. **MPLS** est un mécanisme de commutation qui impose des étiquettes (numéros) aux paquets, puis utilise ces étiquettes pour transférer les paquets. Les étiquettes sont attribuées à la périphérie du réseau **MPLS** et le transfert à l'intérieur du réseau **MPLS** se fait uniquement sur la base des étiquettes. Les étiquettes correspondent généralement à un chemin vers les adresses de destination de la couche 3 (égal au routage basé sur la destination IP). **MPLS** a été conçu pour prendre en charge la transmission de protocoles autres que TCP/IP. Pour cette raison, la commutation d'étiquettes au sein du réseau est effectuée de la même manière quelle que soit le protocole de couche 3. Dans les grands réseaux, le résultat de l'étiquetage **MPLS** est que seuls les routeurs de périphérie (edge routers) effectuent une recherche de routage, tous les routeurs centraux font faire suivre les paquets sur la base des étiquettes, ce qui accélère le transfert des paquets via le réseau du fournisseur de services.
- **ATM**: Le mode de transfert asynchrone **ATM** (Asynchronous Transfer Mode) a été créé pour le trafic sensible au temps, offrant une transmission simultanée de la voix, de la vidéo et des données. **ATM** utilise des cellules d'une longueur fixe de 53 octets au lieu de paquets. Il peut également utiliser une synchronisation isochrone (horloge externe) pour aider les données à se déplacer plus rapidement. En règle générale, si on exécute **Frame Relay** aujourd'hui, on utilisera **Frame Relay** sur **ATM**.
- **DWDM** Le multiplexage par répartition en longueur d'onde dense (Dense Wavelength Division Multiplexing) est une technologie optique utilisée pour augmenter la bande passante à l'aide de dorsales en fibre. **DWDM** fonctionne pour combiner et transmettre plusieurs signaux simultanément à différentes longueurs d'onde sur le même lien de fibre, créant un type de multilien avec les signaux descendant la fibre. En théorie, un lien de 1,5 Gbs pourrait avoir une capacité de 10 Mbps. Un avantage de **DWDM** est qu'il est à la fois un protocole indépendant du débit binaire et peut fonctionner avec IP sur ATM, SONET et même Ethernet.