République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

---

École supérieure en Sciences et Technologies de l'Informatique et du Numérique

RAPPORT DE PROJET :

Thème :
X.25 et MPLS(Multi protocol label switching)

Ce projet est réalisé par :

- **GUIR Mohamed abdelhai**
- **BAHLOUL Rami**
- **ATOUI Abderahman yakoub**
- **MENAD abdelmadjid**
- **HAMOUDI ahmediyad**
- **MESSAOUDI belkacem**

Encadré par :

- **Mme Sylia ZENADJI**
- **Mme Numidia ZAIDI**

Année universitaire : 2023-2024

REMERCIEMENTS :

En tout premier lieu, nous remercions le bon Dieu, tout puissant, de nous avoir donné la force pour survivre, ainsi que l'audace pour dépasser toutes les difficultés. Permis de mener 'a bien ce projet. Louange à ALLAH le tout puissant.

Nous tenons à remercier chaleureusement toutes les personnes qui ont contribué à la réalisation de ce projet.

Nous adressons nos plus sincères remerciements à nos chères encadreuses Mme Sylia ZENADJI et Mme Numidia ZAIDI pour la richesse et la qualité de leur encadrement , pour tous leurs précieux conseils,pour leurs écoutes actives et leurs disponibilités tout au long de la réalisation de ce projet.

Nous souhaitons également adresser nos remerciements aux membres de l'équipe de ce projet, pour leur disponibilité et leur collaboration tout au long de la réalisation de ce projet. Leur expertise nous a été précieuse et a grandement contribué à la qualité de notre travail.

Enfin, nous tenons à remercier nos familles et nos amis pour leur soutien inconditionnel, leur patience et leur compréhension durant cette période intense de travail.

Nous sommes conscients que ce projet n'aurait pas été possible sans l'implication de chacun de ces acteurs et nous leur exprimons notre sincère gratitude.

Table des matières

Liste des Figures

1 Introduction générale

Dans l'histoire dynamique des télécommunications, l'évolution des protocoles de transmission de données a été marquée par des jalons significatifs, parmi lesquels se distinguent X.25 et MPLS.

D'une part, X.25, standardisé par le CCITT en 1976, a représenté une avancée majeure en permettant la transmission fiable de données à commutation de paquets à travers des réseaux publics. Son déploiement à grande échelle, comme avec le réseau Transpac en France, a été crucial pour l'établissement de connexions informatiques entre terminaux distants et ordinateurs centraux, offrant ainsi une connectivité efficace pour une multitude de services, de l'annuaire électronique via Minitel aux transactions bancaires.

D'autre part, l'avènement de MPLS a répondu aux exigences croissantes de performance et de fiabilité dans les réseaux modernes. Contrairement au processus complexe et potentiellement inefficace de commutation de paquets traditionnel, MPLS propose une approche plus intelligente, basée sur l'étiquetage des données pour faciliter un routage plus rapide et plus efficace. En comprenant le fonctionnement des réseaux Internet et les défis rencontrés lors de la transmission de données, on peut apprécier pleinement le rôle crucial que joue MPLS dans l'amélioration des performances et de la connectivité.

Ce rapport se propose donc d'explorer en détail l'évolution de ces deux protocoles, depuis leur conception jusqu'à leur utilisation contemporaine, en mettant en lumière leurs contributions respectives à l'architecture des réseaux de communication. Nous analyserons également leur impact sur les performances, la sécurité et la satisfaction des utilisateurs, tout en examinant les tendances émergentes qui pourraient façonner l'avenir de ces technologies. Enfin, nous nous attarderons sur les défis et les opportunités qui se présentent dans le paysage en constante évolution des télécommunications.

2 CHAPITRE 01 : Le protocole X.25

2.1 Introduction:

Le protocole X.25 représente un jalon significatif dans l'histoire des télécommunications, émergeant comme une solution novatrice pour la transmission de données à commutation de paquets. Standardisé par le CCITT en 1976, X.25 a été largement déployé dans des réseaux publics à travers le monde, offrant une connectivité fiable et efficace pour les échanges informatiques entre terminaux distants et ordinateurs centraux. En France, par exemple, le réseau Transpac a exploité X.25 pour fournir une gamme de services allant de l'annuaire électronique via Minitel aux transactions bancaires. Malgré son déclin ultérieur face à l'essor des protocoles IP et TCP, X.25 demeure un élément crucial de l'histoire des télécommunications, témoignant de l'évolution constante des technologies de communication.

2.2 Historique:

Le développement du protocole X.25 découle d'efforts collaboratifs entre des représentants des PTT (Poste, Télégraphe et Téléphone) et des entreprises privées à travers l'Europe, l'Amérique du Nord et le Japon. À partir des discussions lors de la réunion du groupe de rapporteurs de l'UIT à Ottawa en mars 1975, les bases ont été posées pour ce qui allait devenir la proposition X.25. Cette initiative était motivée par la nécessité d'un protocole standardisé pour la communication de données à commutation de paquets, une demande qui est apparue à partir de divers projets de réseau de données au milieu des années 1970.

Le processus de normalisation a impliqué des ingénieurs du Canada, de la France, du Japon, du Royaume-Uni et des États-Unis, représentant un mélange de PTT nationales et d'opérateurs privés. Rémi Després a joué un rôle significatif dans la définition de la norme,qui était basée sur un service de circuit virtuel. Des ajustements mineurs ont été apportés pour prendre en compte les contributions des parties prenantes clés, y compris Larry Roberts, renforçant ainsi l'accord.

À travers une série de réunions et de discussions, l'UIT a travaillé à

normaliser les circuits virtuels, explorant la faisabilité des réseaux à commutation de paquets et de l'interface entre les réseaux et les ordinateurs. Des réunions bilatérales et multilatérales entre les opérateurs de réseau, tels que DATAPAC, TRANSPAC et Telenet, ont conduit à l'élaboration de spécifications d'interface communes.

La culmination de ces efforts est survenue lors de la plénière de l'UIT en septembre 1976, où la recommandation X.25, ainsi que d'autres normes connexes, ont été unanimement approuvées. Des révisions ultérieures, y compris l'ajout d'un service de datagramme facultatif, ont contribué à l'affinement continu de X.25.

Les réseaux X.25 accessibles au public, connus sous le nom de réseaux de données publics, se sont multipliés dans le monde entier à la fin des années 1970 et dans les années 1980, facilitant l'accès à des services en ligne tels que Iberpac, TRANSPAC et Tymnet. Cependant, avec l'émergence des technologies Frame Relay et TCP/IP au début des années 1990, les réseaux X.25 ont commencé à décliner en Amérique du Nord, bien qu'ils continuent d'être utilisés dans le monde entier, notamment dans des applications de niche comme la radio amateur et les communications aéronautiques.

En France, le service Minitel basé sur X.25 est resté opérationnel jusqu'en 2012, marquant la fin d'une époque pour les services X.25 destinés aux utilisateurs finaux commerciaux. Malgré son déclin dans l'utilisation grand public, X.25 continue d'être disponible dans certaines régions et industries, soulignant son héritage durable dans le domaine des télécommunications.

2.3 Architecture:

Le protocole X.25 a été conçu dans le but de créer un réseau universel et mondial à commutation de paquets. Une grande partie du système X.25 décrit la rigueur de la correction d'erreurs nécessaire pour atteindre cet objectif, ainsi que le partage plus efficace des ressources physiques coûteuses.

La spécification X.25 ne définit que l'interface entre un abonné (DTE) et un réseau X.25 (DCE). X.75, un protocole très similaire à X.25, définit l'interface entre deux réseaux X.25 pour permettre à des connexions de traverser deux réseaux ou plus. X.25 ne spécifie pas le fonctionnement in-

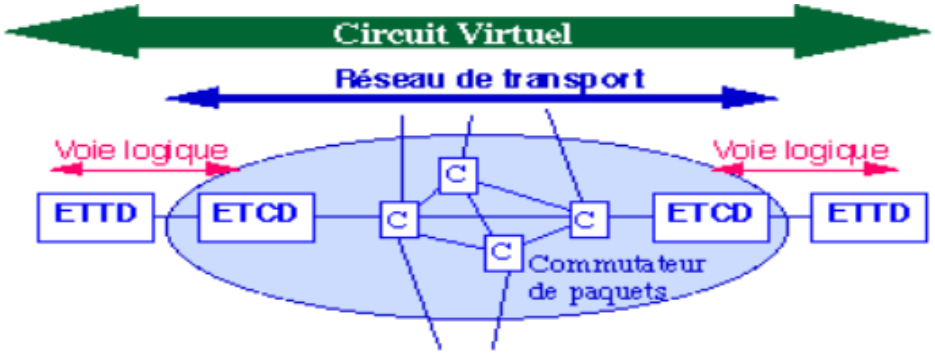


Figure 1: X.25 archi

terne du réseau - de nombreuses implémentations de réseaux X.25 utilisent quelque chose de très similaire à X.25 ou X.75 en interne, mais d'autres utilisent des protocoles très différents. La spécification ISO équivalente à X.25, ISO 8208, est compatible avec X.25, mais inclut également une disposition permettant à deux DTE X.25 d'être directement connectés l'un à l'autre sans réseau intermédiaire.

Le modèle X.25 était basé sur le concept téléphonique traditionnel d'établissement de circuits fiables à travers un réseau partagé, mais en utilisant des logiciels pour créer des "appels virtuels" à travers le réseau. Ces appels interconnectent des "équipements terminaux de données" (DTE) fournissant des points d'extrémité aux utilisateurs, qui ressemblent à des connexions point à point. Chaque point d'extrémité peut établir de nombreux appels virtuels distincts vers différents points d'extrémité.

Le modèle X.25 définissait à l'origine trois niveaux ou couches architecturales de protocole de base. Dans les spécifications d'origine, ces niveaux étaient appelés niveaux et avaient également un numéro de niveau, alors que toutes les recommandations X.25 de l'UIT-T et les normes ISO 8208 publiées après 1984 les désignent comme des couches.

Couche physique: Cette couche spécifie les caractéristiques physiques, électriques, fonctionnelles et procédurales pour contrôler la liaison physique entre un DTE et un DCE. Les implémentations courantes utilisent X.21, EIA-232, EIA-449 ou d'autres protocoles série.

Couche liaison de données: La couche liaison de données est composée de la procédure d'accès au lien pour l'échange de données sur le lien entre un DTE et un DCE. Dans son implémentation, la procédure d'accès au

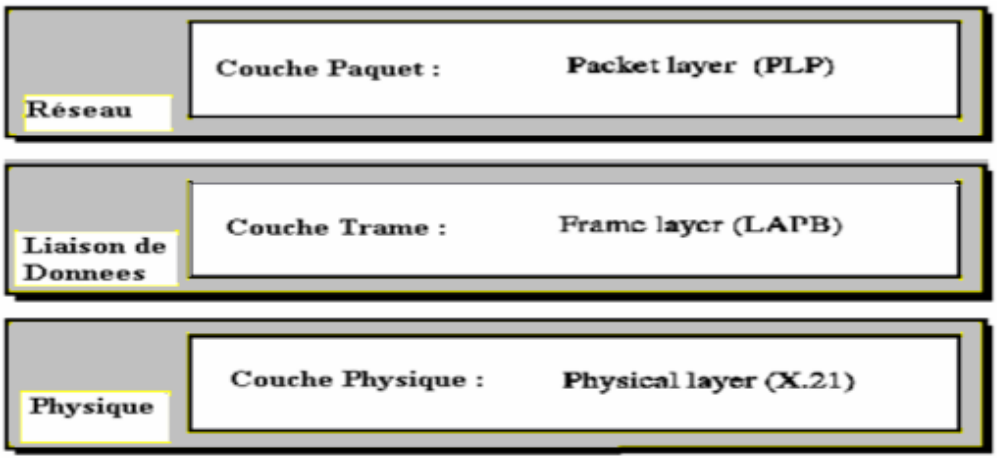


Figure 2: couche paquet

lien, équilibrée (LAPB) est un protocole de liaison de données qui gère une session de communication et contrôle le formatage des paquets. C'est un protocole orienté bits qui fournit une correction d'erreurs et une livraison ordonnée.

Couche de paquet: Cette couche définissait un protocole de couche de paquet pour l'échange de paquets de données de contrôle et d'utilisateur pour former un réseau à commutation de paquets basé sur des appels virtuels, selon le protocole de couche de paquet.

La connexion d'appareils asynchrones (tels que des terminaux idiots et des imprimantes) à un réseau X.25 était gérée par des protocoles tels que X.3, X.28 et X.29. Cette fonctionnalité était réalisée à l'aide d'un assembleur/désassembleur de paquets ou PAD (également appelé dispositif triple-X, faisant référence aux trois protocoles utilisés).

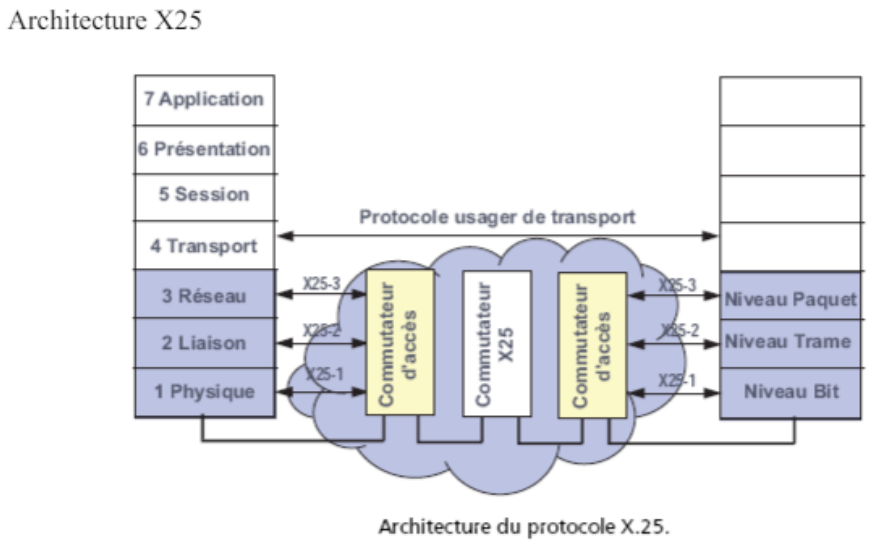


Figure 3: Architecture x.25

2.4 La structure d'une trame X.25:

La structure d'une trame X.25 comporte les champs suivants. Le champ de contrôle indique quel cadre est en cours de transmission. Les trames Information contiennent des données, tandis que les trames Unnumbered et Supervisory contiennent des informations de contrôle.

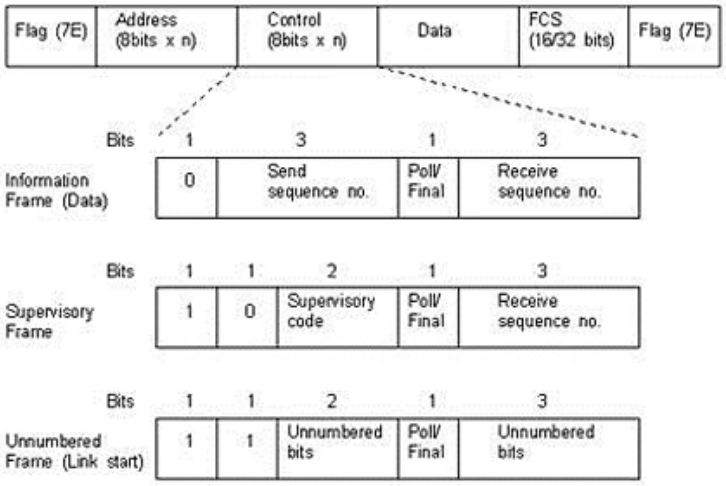


Fig. 3 LAPB frame structure

Figure 4: X.25 trame

2.5 Le format de trame X.25:

Le format de trame X.25 propose trois formats différents, différenciés par la taille du numéro de séquence. La trame de base a une taille de numéro de séquence de 3 bits, de sorte que l'incrémentation du numéro de séquence est une opération modulo 8. Dans le cas de la trame étendue, l'incrémentation est une opération modulo 128, et dans le cas de la trame super, une opération modulo 32768.

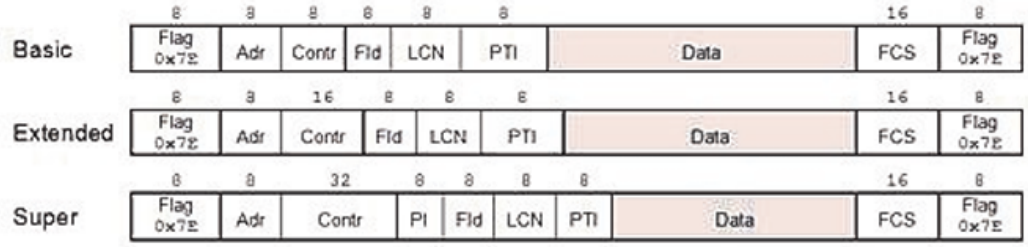


Fig. 4 X.25 Frame format

Figure 5: X.25 format de trame

2.6 La structure d'un paquet X.25:

La structure d'un paquet X.25 comprend le champ de données d'une trame LAPB (HDLC) d'une taille de 64 à 4096 octets. Le champ GFI (General Format Identifier) contient des informations générales sur le format du paquet, le champ LCI (Logical Channel Identifier) contient des informations sur le canal logique, et le champ PTI (Packet Type Identifier) contient des informations sur le type de paquet PLP.

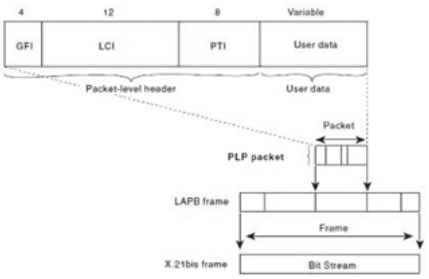


Fig. 4 X.25 PLP encapsulation in a LAPB frame

Figure 6: X.25 structure d'un paquet

2.7 Relation avec le modèle de référence OSI:

Bien que X.25 précède le modèle de référence OSI (OSIRM), la couche physique du modèle OSI correspond à la couche physique de X.25, la couche liaison de données à la couche liaison de données de X.25, et la couche réseau à la couche de paquet de X.25. La couche de liaison de données X.25, LAPB, fournit un chemin de données fiable sur un lien de données (ou plusieurs liens de données parallèles, multiliens) qui peuvent ne pas être fiables eux-mêmes. La couche de paquet X.25 fournit les mécanismes d'appel virtuel, fonctionnant sur X.25 LAPB. La couche de paquet inclut des mécanismes pour maintenir les appels virtuels et signaler les erreurs de données dans le cas où la couche de liaison de données ne peut pas récupérer les erreurs de transmission de données.

2.8 X.25 face à TCP/IP:

Contrairement à TCP/IP, qui ne propose qu'un contrôle d'erreurs et de flux aux deux extrémités d'une liaison, X.25 offre un contrôle d'erreurs au niveau de chaque nœud et une transmission des paquets dans l'ordre d'émission. Le résultat est un service fiable, avec une qualité pratiquement constante. En contrepartie, TCP/IP propose un contrôle de flux et un mécanisme de fenêtrage des données bien plus perfectionné, de manière à compenser un fonctionnement du réseau entièrement passif. Avec X.25, le nombre de connexions simultanées à chaque nœud est limité : il est donc possible de saturer le réseau, mais pas de faire s'écrouler la bande passante comme avec IP. Autre différence importante : les algorithmes de routage ne font pas partie de la norme X.25. On ne cherche pas à connaître le

trajet des données, pour autant qu'il soit fiable. X.25 définit précisément des normes électriques et de connecteurs, ainsi qu'un niveau trame, conformément au modèle OSI,tandis que TCP/IP est conçu pour fonctionner sur un grand nombre de réseaux physiques différents (Ethernet, Frame Relay, ATM, X.25, etc.). Par de nombreux principes de fonctionnement, notamment la gestion des adresses, les deux technologies se révèlent similaires. Le RFC 1236 établit d'ailleurs un pont entre les deux systèmes d'adressage.

2.9 Support des appareils utilisateurs:

X.25 a été développé à l'époque des terminaux informatiques se connectant à des ordinateurs hôtes, bien qu'il puisse également être utilisé pour les communications entre ordinateurs. Au lieu de se connecter directement "au" système hôte - ce qui nécessiterait que le système hôte dispose de son propre pool de modems et de lignes téléphoniques, et nécessiterait que les appelants non locaux effectuent des appels longue distance - le système hôte pourrait avoir une connexion X.25 à un fournisseur de services réseau. Désormais, les utilisateurs de terminaux idiots pouvaient se connecter au "PAD" (installation d'assemblage/désassemblage de paquets) local du réseau, un dispositif passerelle connectant les modems et les lignes série au lien X.25 telque défini par les normes X.29 et X.3.

Une fois connecté au PAD, l'utilisateur du terminal idiot indique au PAD quel hôte se connecter, en fournissant une adresse au format X.121, semblable à un numéro de téléphone (ou en fournissant un nom d'hôte, si le fournisseur de services permet des noms qui se mappent en adresses X.121). Le PAD établit ensuite un appel X.25 vers l'hôte, établissant un appel virtuel. Notez que X.25 prévoit des appels virtuels, il semble donc s'agir d'un réseau à commutation de circuits, même si en réalité les données elles-mêmes sont commutées par paquets en interne, de manière similaire à la manière dont TCP fournit des connexions même si les données sous-jacentes sont commutées par paquets. Deux hôtes X.25 pourraient, bien sûr, s'appeler directement ; aucun PAD n'est impliqué dans ce cas. En théorie, il n'importe pas que l'appelant X.25 et la destination X.25 soient tous deux connectés au même opérateur, mais en pratique, il n'était pas

toujours possible de faire des appels d'un opérateur à un autre.

Dans le but de la régulation du débit, un protocole de fenêtrage coulissant est utilisé avec une taille de fenêtre par défaut de 2. Les accusés de réception peuvent avoir soit une signification locale, soit une signification de bout en bout. Un bit D (bit de livraison de données) dans chaque paquet de données indique si l'expéditeur nécessite une confirmation de réception de bout en bout. Lorsque D = 1, cela signifie que l'accusé de réception a une signification de bout en bout et doit avoir lieu uniquement après que le DTE distant a accusé réception des données. Lorsque D = 0, le réseau est autorisé (mais non obligé) à accuser réception avant que le DTE distant ait accusé réception ou même reçu les données.

Bien que la fonction PAD définie par X.28 et X.29 prenne en charge spécifiquement les terminaux de caractères asynchrones, des équivalents de PAD ont été développés pour prendre en charge une large gamme de dispositifs de communication intelligents propriétaires, tels que ceux pour l'architecture de réseau du système IBM (SNA).

2.10 Contrôle des erreurs:

Le contrôle des erreurs dans le protocole X.25 est un mécanisme qui permet de détecter et de corriger les erreurs qui se produisent pendant la transmission de données. Ce contrôle est effectué à chaque niveau du réseau, ce qui signifie que chaque équipement d'extrémité (ou node) vérifie les données reçues et les corrige si nécessaire avant de les transmettre à l'équipement suivant. Dans le protocole X.25, le contrôle des erreurs est réalisé à l'aide de plusieurs mécanismes, notamment :

- Vérification de la séquence : chaque équipement d'extrémité vérifie la séquence des paquets reçus pour s'assurer qu'ils sont arrivés dans l'ordre correct.

- Vérification de la cohérence : chaque équipement d'extrémité vérifie la cohérence des données reçues pour s'assurer qu'elles sont correctes et cohérentes.

- Réinitialisation des erreurs : si une erreur est détectée, l'équipement d'extrémité peut réinitialiser la transmission pour réessayer de trans-

mettre les données correctement.

Ce contrôle des erreurs permet de garantir une transmission fiable et exempte d'erreurs, ce qui est essentiel pour les applications qui nécessitent une transmission de données précise et sans erreur.

Les procédures de récupération d'erreurs au niveau de la couche de paquet supposent que la couche de liaison de données est responsable de la retransmission des données reçues en erreur. La gestion des erreurs au niveau de la couche de paquet se concentre sur la resynchronisation du flux d'informations dans les appels, ainsi que sur la suppression des appels ayant atteint des états irrécupérables :

- Paquets de réinitialisation de niveau 3, qui réinitialisent le flux sur un appel virtuel (mais ne rompent pas l'appel virtuel).
- Paquet de redémarrage, qui ferme tous les appels virtuels sur la liaison de données et réinitialise tous les circuits virtuels permanents sur la liaison de données.

2.11 Conclusion:

Dans cette étude, nous avons exploré en détail la structure et le fonctionnement du protocole X.25, une norme historique dans le domaine des réseaux de données. Nous avons examiné la structure des trames X.25, mettant en évidence les différents champs de contrôle et leur fonctionnalité dans le processus de transmission. De plus, nous avons analysé les trois formats de trame proposés par X.25, en mettant en lumière leurs caractéristiques distinctives en termes de taille de numéro de séquence et d'opérations d'incrémentation.

Ensuite, nous avons étudié la structure des paquets X.25, soulignant l'importance des champs de données, GFI, LCI et PTI dans la transmission efficace des données sur le réseau. Nous avons également établi des liens entre X.25 et le modèle de référence OSI, mettant en évidence les correspondances entre les différentes couches des deux modèles et soulignant le rôle crucial de X.25 dans la fourniture de services de communication fiables.

En comparant X.25 à TCP/IP, nous avons mis en évidence les avantages

et les inconvénients de chaque protocole en termes de contrôle d'erreurs, de gestion du flux et de performance globale. Enfin, nous avons examiné le support des appareils utilisateurs pour X.25, montrant comment cette norme a facilité la connectivité entre les terminaux et les ordinateurs hôtes à une époque où les technologies de communication étaient encore en développement.

En conclusion, le protocole X.25 a joué un rôle important dans l'histoire des réseaux de données, fournissant un cadre robuste pour la transmission de données dans un environnement réseau en évolution constante. Bien que largement remplacé par des technologies plus récentes, son héritage perdure dans de nombreux aspects des réseaux modernes, témoignant de son importance et de sa pertinence dans le domaine des communications informatiques.

3 CHAPITRE 02 : Multiprotocol Label Switching (MPLS)

3.1 Introduction:

Avant de plonger dans MPLS, permettez-moi de vous expliquer comment les données voyagent à travers Internet. Lorsque vous envoyez un e-mail ou participez à un appel vidéo, vos données traversent différents routeurs Internet pour atteindre leur destination. À chaque routeur, il y a un processus complexe d'ouverture des paquets et de récupération des adresses réseau pour déterminer le meilleur chemin pour vos données. Ce processus peut être lent et inefficace, entraînant des retards et de la frustration pour les utilisateurs. Non seulement cela affecte les individus, mais cela impacte également les performances globales du réseau pour les organisations. Heureusement, il existe une solution appelée Multiprotocol Label Switching (MPLS). MPLS offre une façon plus intelligente aux données de voyager, rendant les réseaux plus rapides et plus fiables. Pour les entreprises et les organisations visant à améliorer les performances du réseau et la satisfaction des utilisateurs, MPLS présente une solution prometteuse.

3.2 Historique:

Le développement de la technologie MPLS a été marqué par plusieurs étapes clés depuis ses débuts dans les années 1990. En 1994, Toshiba présente les premières idées de routeur de commutation de cellules lors de l'IETF BOFF, jetant ainsi les bases de ce qui allait devenir MPLS. Deux ans plus tard, en 1996, Ipsilon, Cisco et IBM annoncent leurs plans pour la commutation par étiquettes, une évolution significative qui conduira à la création du groupe de travail MPLS de l'IETF l'année suivante. Dans les années qui suivent, MPLS connaît une série de développements majeurs, notamment le déploiement des VPN MPLS et de l'ingénierie du trafic (TE) en 1999, ainsi que la publication du premier Request for Comments (RFC) dédié à MPLS en 2001. L'introduction des VPN de couche 2 (L2VPN) avec AToM en 2002 et la montée en puissance de la TE à grande échelle en 2006 marquent également des avancées importantes. Au fil des

ans, MPLS continue de s'étendre pour prendre en charge de nouvelles fonctionnalités telles que le multicast avec le Label Switching Multicast en 2009 et le profil de transport MPLS en 2011. Cette évolution constante témoigne de l'importance croissante de MPLS dans le paysage des réseaux de communication.

3.3 Evolution:

L'évolution de MPLS a été marquée par plusieurs phases importantes, chaque étape apportant des améliorations significatives à la technologie et étendant ses capacités. Voici un aperçu des principales évolutions de MPLS :

1. Origines et développement initial :
   - MPLS a été introduit pour la première fois dans les années 1990 comme une solution pour améliorer les performances et la qualité de service des réseaux IP.
   - Sa conception originale visait à fournir un mécanisme de commutation de paquets plus efficace en utilisant des étiquettes pour acheminer le trafic.
2. Intégration de la qualité de service (QoS) :
   - Une évolution majeure de MPLS a été l'intégration de la qualité de service (QoS) dans la gestion du trafic.
   - Cela a permis aux fournisseurs de services de différencier les niveaux de service pour différents types de trafic, garantissant une expérience utilisateur optimale pour des applications sensibles à la latence comme la voix sur IP (VoIP) ou la vidéo en streaming.
3. Extension aux réseaux privés virtuels (VPN) :
   - Une autre étape importante dans l'évolution de MPLS a été son extension pour prendre en charge les réseaux privés virtuels (VPN).
   - Cette fonctionnalité a permis aux entreprises de créer des réseaux privés virtuels sécurisés et rentables, en utilisant l'infrastructure MPLS existante des fournisseurs de services.

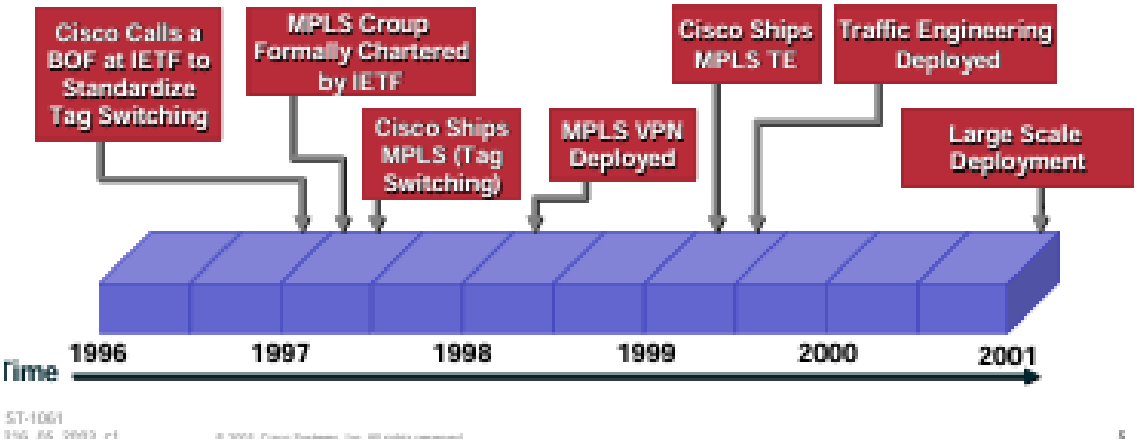


Figure 7: mpls

4. MPLS-TE (Traffic Engineering) :
   - L'introduction de MPLS Traffic Engineering a permis aux opérateurs de réseaux de contrôler plus précisément le flux de trafic à travers leurs réseaux.
   - Cela leur a donné la capacité de configurer des chemins de trafic spécifiques pour optimiser l'utilisation des ressources du réseau et améliorer les performances globales.
5. Évolutivité et automatisation :
   - Les récentes évolutions de MPLS se concentrent sur l'amélioration de l'évolutivité et de l'automatisation des réseaux.
   - Cela comprend des techniques telles que l'intégration de protocoles SDN (Software-Defined Networking) pour simplifier la gestion et l'orchestration du réseau, ainsi que des mécanismes d'évolutivité pour prendre en charge des réseaux de plus en plus vastes et complexes.

En résumé, l'évolution de MPLS a été caractérisée par l'ajout de fonctionnalités telles que la QoS, les VPN, le Traffic Engineering, ainsi que des améliorations continues de la performance, de la sécurité et de la gestion des réseaux. Ces développements ont fait de MPLS une technologie fondamentale pour les fournisseurs de services de télécommunications et les entreprises cherchant à optimiser leurs infrastructures réseau.

3.4 Architecture:

La structure de MPLS comprend deux composants principaux : le plan de contrôle et le plan de données.

Le plan de contrôle est responsable de l'échange d'informations de routage de couche 3 et d'étiquettes entre les périphériques adjacents. Il comprend des mécanismes complexes pour échanger des informations de routage (OSPF, EIGRP, IS-IS, BGP, etc.) et des étiquettes (Protocole de distribution de tag [TDP], Protocole de distribution de label [LDP], BGP, RSVP, etc.). En outre, il maintient le contenu de la table de commutation d'étiquettes (base d'information de commutation d'étiquettes ou LFIB).

Le plan de données, quant à lui, assure le transfert des paquets basé sur les étiquettes. Il dispose d'un moteur de transfert simple qui se base sur les étiquettes pour acheminer les paquets, indépendamment du type de protocole de routage ou de protocole d'échange d'étiquettes. Une table de base d'information de commutation d'étiquettes (LFIB) est utilisée pour transférer les paquets en se basant sur les étiquettes. Cette table est remplie par les protocoles d'échange d'étiquettes utilisés dans le plan de contrôle.

Un réseau MPLS simple implémente un transfert basé sur les destinations qui utilise des étiquettes pour prendre des décisions de transfert. Un protocole de routage de couche 3 est toujours nécessaire pour propager les informations de routage de couche 3. Le mécanisme d'échange d'étiquettes est simplement un complément pour propager les étiquettes qui sont utilisées pour les destinations de couche 3.

En résumé, le plan de contrôle gère l'échange d'informations de routage et d'étiquettes, tandis que le plan de données assure le transfert des paquets basé sur les étiquettes. Ces deux composants travaillent ensemble pour permettre un acheminement efficace des données à travers le réseau MPLS.

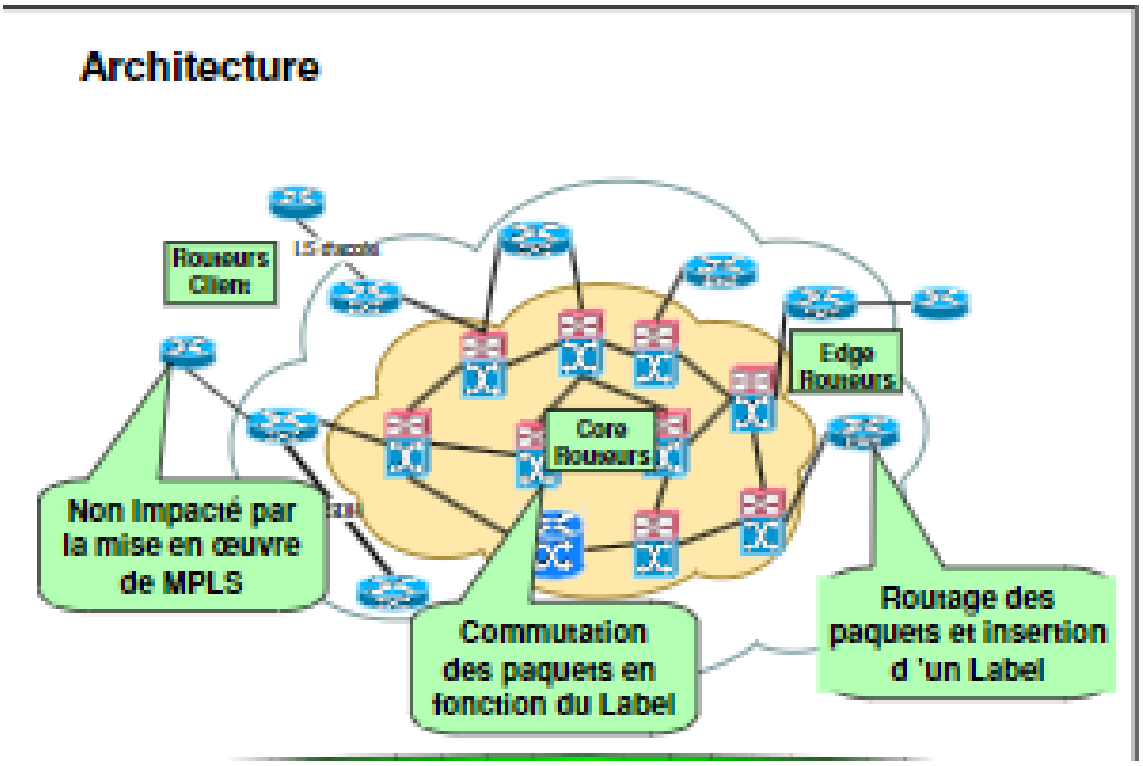


Figure 8: mpls architecture

3.5 Rôle et fonctionnement de MPLS :

1. Étiquetage des paquets : MPLS attribue des étiquettes aux paquets de données. Les décisions de transfert de paquets sont basées uniquement sur ces étiquettes, ce qui élimine le besoin d'examiner le contenu des paquets. Cette approche simplifie le processus de transfert des données et permet un acheminement plus rapide et efficace à travers le réseau.

2. Positionnement en couche : MPLS fonctionne entre la couche OSI 2 et la couche 3, souvent appelée un protocole de couche 2.5. Cela signifie qu'il opère au-dessus des protocoles de liaison de données de la couche 2 (comme Ethernet) mais en dessous des protocoles de routage de la couche 3 (comme IP). Cette position intermédiaire lui confère une grande flexibilité et lui permet de travailler avec une variété de technologies réseau.

3. Polyvalence : MPLS est capable d'encapsuler des paquets de divers protocoles réseau, notamment des paquets IP, ATM, Frame Relay, SONET et Ethernet. Cette polyvalence en fait un outil puissant

pour l'intégration de différents types de réseaux et la fourniture de services de communication convergents. En encapsulant ces paquets dans des étiquettes MPLS, il devient possible de les router efficacement à travers un réseau MPLS, indépendamment de leur protocole d'origine.

En combinant ces caractéristiques, MPLS offre une solution robuste pour le routage de données dans les réseaux de télécommunications. Son approche basée sur les étiquettes, son positionnement en couche intermédiaire et sa polyvalence en font un choix attrayant pour les opérateurs réseau cherchant à optimiser les performances de leur infrastructure et à fournir des services de communication avancés à leurs clients.

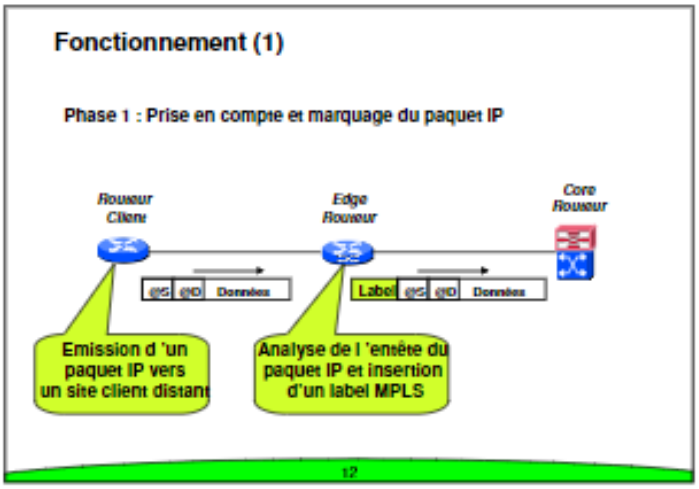


Figure 9: fonctionnement

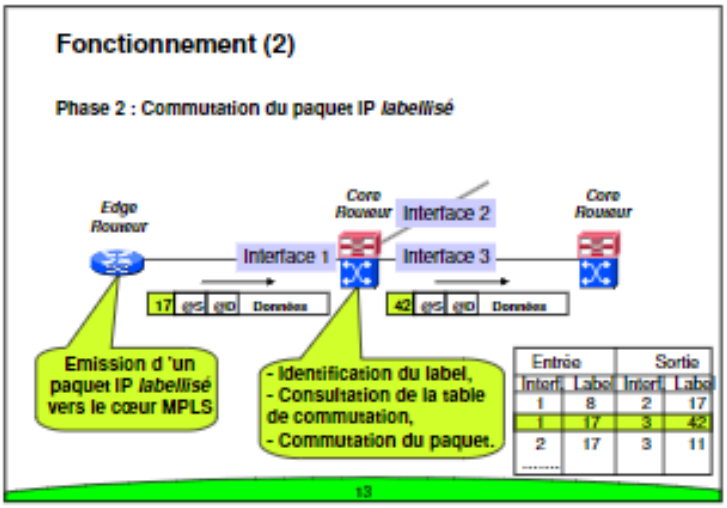


Figure 10: fonctionnement 2

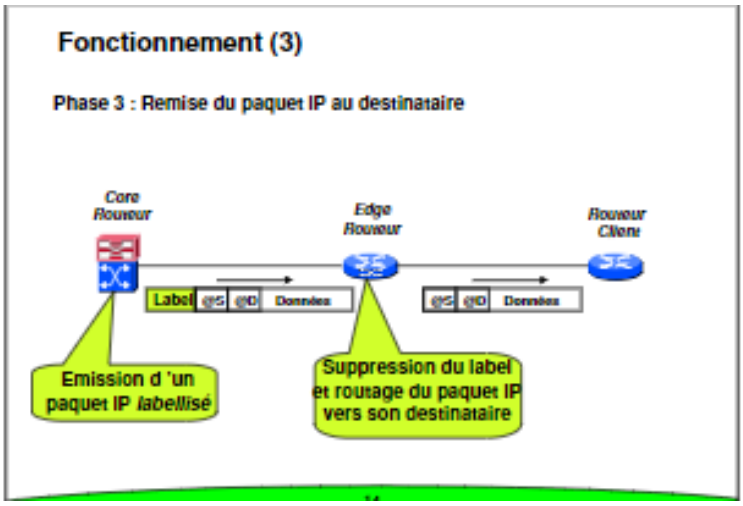


Figure 11: fonctionnement 3

3.6 Label :

Un label a une signification locale entre 2 LSR adjacents et mappe le flux de trafic entre le LSR amont et la LSR aval. A chaque bond le long du LSP, un label est utilisé pour chercher les informations de routage (next hop, lien de sortie, encapsulation, queueing et scheduling) et les actions à réaliser sur le label : insérer, changer ou retirer. La figure ci-dessous, décrit la mise en œuvre des labels dans les différentes technologies ATM, Frame Relay, PPP, Ethernet et HDLC. Pour les réseaux Ethernet, un champ appelé shim a été introduit entre la couche 2 et la couche 3. Sur 32 bits, il a une signification d'identificateur local d'une FEC. 20 bits contiennent le label, un champ de 3 bits appelé Classe of Service (CoS) sert actuellement pour la QoS, un bit S pour indiquer s'il y a empilement de labels et un dernier champ, le TTL sur 8 bits (même signification que pour IP). L'empilement des labels permet en particulier d'associer plusieurs contrats de service à un flux au cours de sa traversé du réseau MPLS.

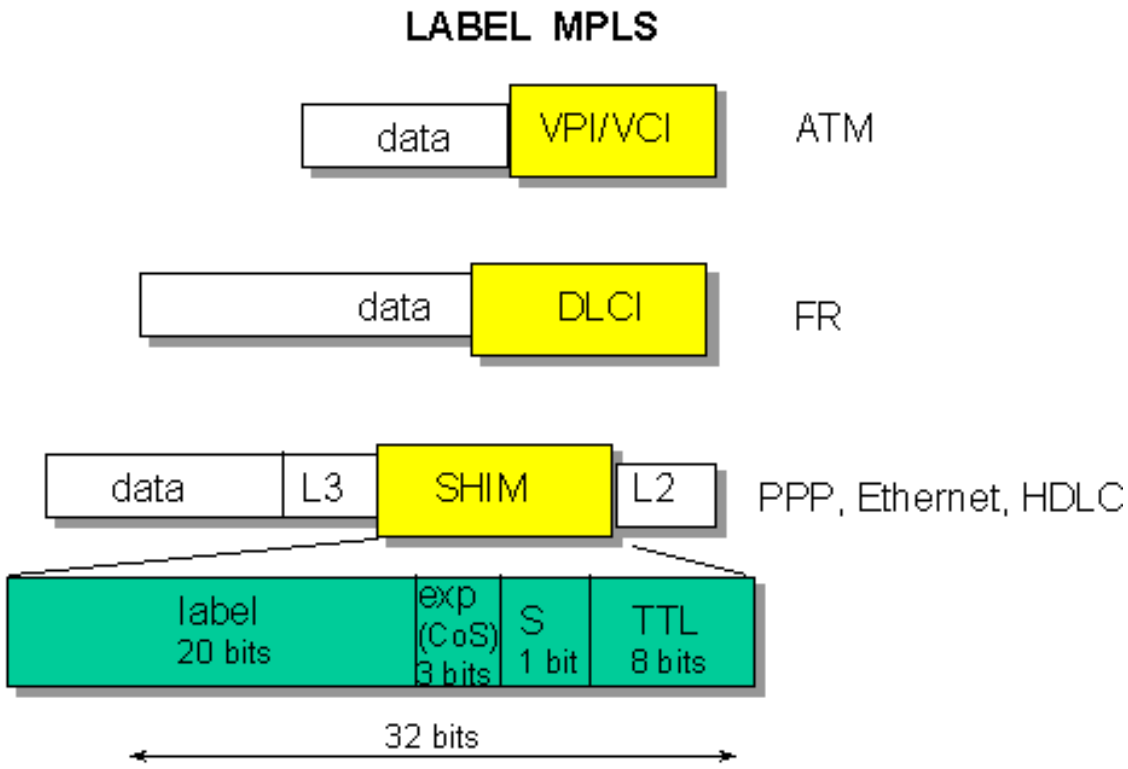


Figure 12: label mpls

3.7 Relation avec le protocole Internet (IP) :

1. Intégration avec IP : Le MPLS fonctionne avec IP et ses protocoles de routage, généralement les protocoles de passerelle intérieure (IGP).

2. Réseaux Virtuels Dynamiques : Les LSP MPLS fournissent des réseaux virtuels dynamiques et transparents prenant en charge l'ingénierie du trafic et les VPN de couche 3 (IP) avec des espaces d'adresses superposés.

3. Pseudowires de Couche 2 : Le MPLS prend en charge les pseudofils de couche 2 en utilisant l'émulation de pseudofils de bord à bord (PWE3), capable de transporter diverses charges utiles de transport.

4. Routage et Configuration : Les dispositifs compatibles MPLS sont des LSR. Les définitions de chemin peuvent être configurées explicitement ou dynamiquement en utilisant des algorithmes comme le Constrained Shortest Path First (CSPF).

3.8 Étapes clés :

1. Formation du Groupe de Travail MPLS : L'Internet Engineering Task Force (IETF) a formé le groupe de travail MPLS en 1997 pour développer un protocole de consensus.

2. Déploiement des VPN MPLS et de l'Ingénierie du Trafic : Les premiers déploiements de VPN MPLS (L3VPN) et d'ingénierie du trafic ont eu lieu en 1999.

3. Publication des Premiers RFCs MPLS : Les premiers Request for Comments (RFCs) MPLS ont été publiés en 2001.

4. Avancées : Le MPLS a connu des avancées telles que AToM (L2VPN), GMPLS, les VPN MPLS à grande échelle et la commutation d'étiquettes multicast.

3.9 Gestion des chemins :

1. Protocoles Standardisés : Les chemins MPLS sont gérés à l'aide de protocoles tels que le Protocole de Distribution d'Étiquettes (LDP) et RSVP-TE.

2. Protection de Liaison : Les LSP peuvent être catégorisés en tant que primaires (opérationnels), secondaires (de secours) et tertiaires (LSP de dernier recours) pour fournir une protection de liaison et une fiabilité réseau.

3.10 Adressage Multicast :

1. Prise en charge du Multicast : La prise en charge du Multicast dans le MPLS a été introduite pour répondre aux besoins des fournisseurs de services en matière de transport de vidéos à large bande sur les réseaux MPLS.

2. LSP HSMP : Le LSP multipoint en étoile (LSP HSMP) facilite le multicast, la synchronisation temporelle et d'autres objectifs.

3.11 Composants MPLS :

1. Routeurs de commutation d'étiquettes (LSRs) : Ce sont les routeurs au sein d'un réseau MPLS qui effectuent l'opération de commutation d'étiquettes. Les LSRs maintiennent une table de routage qui fait correspondre les étiquettes d'entrée aux interfaces de sortie.

2. Routeurs de bordure d'étiquettes (LERs) : Les LERs sont les points d'entrée et de sortie d'un réseau MPLS. Ils attribuent des étiquettes aux paquets entrants et suppriment les étiquettes des paquets sortants, marquant ainsi les limites des domaines MPLS.

3. Protocole de distribution d'étiquettes (LDP) : Le LDP est utilisé par les LSRs pour distribuer les informations de mappage des étiquettes entre les routeurs voisins, assurant une attribution cohérente des étiquettes dans tout le réseau.

4. Classe d'équivalence de transfert (FEC) : La FEC définit un groupe de paquets traités de manière similaire au sein du réseau MPLS. Les paquets avec la même FEC reçoivent la même étiquette et suivent le même chemin de transfert

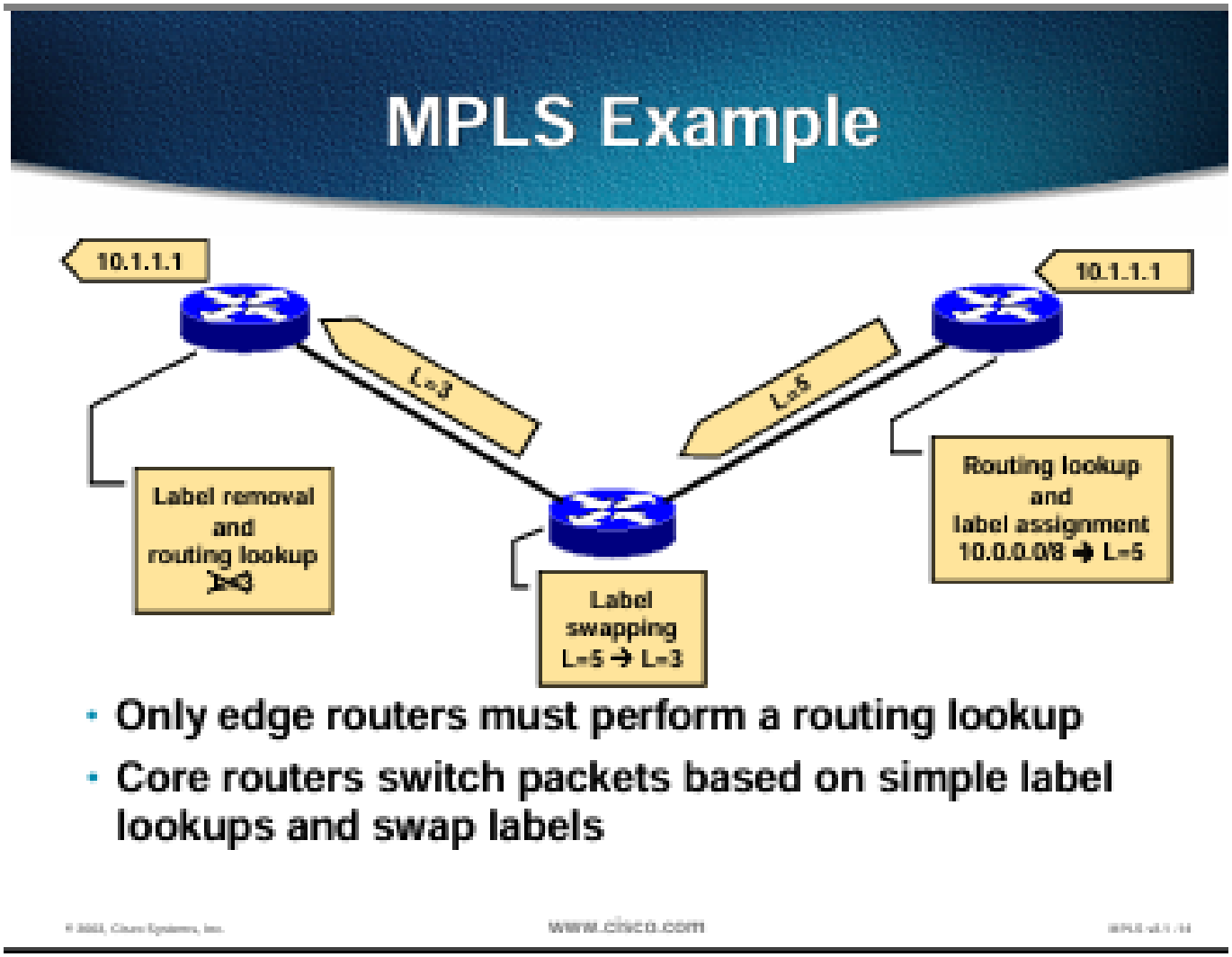


Figure 13: mpls ex

3.12 Applications MPLS :

Les applications les plus courantes du MPLS sont les suivantes :

1. Ingénierie du Trafic : Le MPLS permet aux opérateurs réseau de contrôler le flux de trafic en définissant des chemins explicites à travers le réseau en fonction de facteurs tels que la disponibilité de la bande passante, l'utilisation des liens et la congestion du réseau.

2. Qualité de Service (QoS) : Le MPLS permet de prioriser le trafic en attribuant différentes étiquettes ou chemins de transfert aux paquets en fonction de leurs besoins en QoS. Cela garantit que les applications critiques reçoivent un traitement préférentiel par rapport au trafic moins sensible au temps.

3. Réseaux Privés Virtuels (VPN) : Les VPN basés sur le MPLS offrent une solution sécurisée et évolutive pour connecter des sites géographiquement dispersés sur une infrastructure partagée. En créant des superpositions de réseau virtualisées, le MPLS permet aux organisations de maintenir l'isolation et la confidentialité de leur trafic de données.

4. La bande passante garantie: La bande passante garantie constitue une amélioration à forte valeur ajoutée par rapport aux mécanismes d'ingénierie de trafic traditionnels. MPLS permet aux fournisseurs de services d'allouer des largeurs de bande passante et des canaux garantis. La bande passante garantie permet également la comptabilité des ressources QoS (qualité de service) de manière à organiser le trafic 'prioritaire' et 'au mieux', tels que la voix et les données.

5. Le reroutage rapide: il permet une reprise très rapide après la défaillance d'une liaison ou d'un nœud. Une telle rapidité de reprise empêche l'interruption des applications utilisateur ainsi que toute perte de données.

6. La fonction Classe de service (CoS): MPLS assure que le trafic important est traité avec la priorité adéquate sur le réseau et que les exigences de latence sont respectées. Les mécanismes de qualité de service IP peuvent être mis en oeuvre de façon transparente dans un environnement MPLS.

3.13 Avantages du MPLS :

1. Scalabilité : Le MPLS s'adapte efficacement pour prendre en charge de

grands réseaux avec des milliers de nœuds et des schémas de trafic diversifiés. Son architecture flexible permet une expansion sans heurts au fur et à mesure de l'évolution des besoins du réseau. Le MPLS peut accommoder l'augmentation des volumes de trafic réseau, les changements dynamiques de la topologie du réseau et l'ajout de nouveaux services ou applications sans compromettre les performances ou la fiabilité.

2. Ingénierie du trafic : Le MPLS facilite l'optimisation des ressources réseau et améliore les performances globales du réseau en ajustant dynamiquement les flux de trafic. Avec les capacités d'ingénierie du trafic du MPLS, les opérateurs réseau peuvent mettre en œuvre des politiques pour prioriser le trafic critique, équilibrer la charge sur les liens réseau et atténuer les points de congestion.Cette gestion proactive du trafic assure une utilisation efficace des ressources réseau et améliore l'expérience utilisateur finale.

3. Sécurité :Les VPN MPLS offrent un moyen sécurisé de transmettre

4. Qualité de service :Le MPLS permet un contrôle granulaire sur la priorisation du trafic et l'allocation des ressources, assurant une expérience utilisateur cohérente pour les applications critiques.

5. Hautes performances : L'infrastructure dédiée du MPLS garantit des performances de haute qualité, à faible latence et à faible gigue.

3.14 Défis et considérations :

Malgré ses nombreux avantages, le déploiement et la gestion du MPLS nécessitent une planification minutieuse et une expertise. Voici quelques considérations clés :

des données sensibles sur les réseaux publics, en exploitant l'isolation inhérente et les capacités de chiffrement du MPLS. En établissant des réseaux privés virtuels sur l'infrastructure MPLS, les organisations peuvent créer des canaux de communication sécurisés qui protègent les informations sensibles contre l'accès ou l'interception non autorisés.Les VPN MPLS fournissent des mécanismes de confidentialité, d'intégrité et d'authentification pour sécuriser la transmission des données, en en faisant une solution idéale pour les applications nécessitant des mesures de sécurité strictes.

Grâce aux mécanismes de Qualité de Service (QoS) du MPLS, les opérateurs réseau peuvent définir des accords de niveau de service (SLA) et appliquer des politiques de trafic pour répondre à des exigences de performances spécifiques. Le MPLS permet la classification, le marquage et la priorisation du trafic en fonction de facteurs tels que le type d'application, la sensibilité à la latence et les besoins en bande passante.

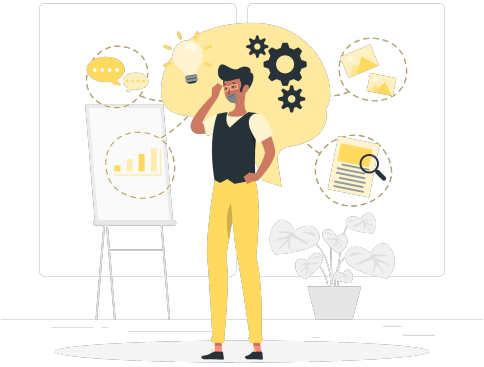
Ce contrôle QoS précis garantit que le trafic à haute priorité reçoit un traitement préférentiel, maintenant la qualité de service et la satisfaction des utilisateurs sur l'ensemble du réseau.

Contrairement aux réseaux publics, le MPLS offre des performances fiables et constantes, ce qui est essentiel pour les applications critiques et la communication en temps réel. Les faibles latences et la stabilité de la connexion du MPLS sont particulièrement précieuses pour les applications telles que la voix sur IP (VoIP), la vidéoconférence et les échanges de données en temps réel. Ces applications nécessitent une transmission rapide et fiable des données pour assurer une expérience utilisateur fluide et sans interruption. Ainsi, le MPLS se distingue par sa capacité à fournir des performances supérieures, offrant une base solide pour les environnements exigeants en termes de performances et de réactivité.

1. Coût : Bien que le MPLS offre des avantages significatifs, ses coûts

de déploiement et de maintenance peuvent être substantiels, notamment pour les petites organisations disposant de budgets limités. Les dépenses initiales liées à la mise en place, les frais de maintenance continus et les coûts de licence pour l'équipement et les logiciels MPLS peuvent contribuer à la charge financière globale. De plus, le MPLS peut nécessiter des investissements dans du matériel spécialisé et une formation pour le personnel informatique, ce qui accroît encore l'engagement financier.

2. Complexité : Les configurations MPLS peuvent être complexes et nécessitent des connaissances et des compétences spécialisées pour être conçues, mises en œuvre et gérées efficacement. La configuration des réseaux MPLS implique des politiques de routage complexes, des configurations de Qualité de Service (QoS) et des paramètres d'ingénierie du trafic, ce qui peut être un défi pour les équipes informatiques sans expertise suffisante. De plus, le dépannage des problèmes liés au MPLS nécessite une compréhension approfondie des protocoles et des technologies MPLS, ce qui accroît la complexité de la maintenance et du support réseau.



3. Dépendance au fournisseur:Les organisations qui dépendent fortement du MPLS peuvent être confrontées à une dépendance au fournisseur, où elles deviennent dépendantes des solutions et technologies propriétaires d'un fournisseur spécifique. Cette dépendance peut limiter leur flexibilité à adopter d'autres technologies réseau ou à changer de fournisseur à l'avenir.

La dépendance au fournisseur peut également entraîner des coûts plus élevés pour les mises à niveau, les expansions ou les services supplémentaires, car les organisations peuvent être liées aux tarifs et offres de produits de leur fournisseur existant.

4. Scalabilité : Bien que le MPLS soit intrinsèquement scalable et puisse prendre en charge des réseaux à grande échelle, des problèmes de scalabilité peuvent En tenant compte de ces facteurs et en abordant

survenir dans certains scénarios. À mesure que les volumes de trafic réseau augmentent ou que les besoins commerciaux évoluent, les organisations peuvent rencontrer des défis de scalabilité liés à l'infrastructure MPLS, tels que des limitations de capacité matérielle, de taille des tables de routage ou de capacités de débit. Pour résoudre ces problèmes de scalabilité, des investissements supplémentaires peuvent être nécessaires pour mettre à niveau l'équipement MPLS ou revoir la conception et l'architecture du réseau.

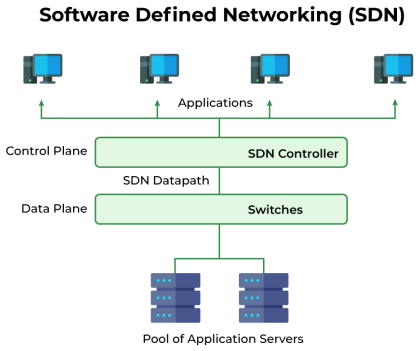
les défis potentiels de manière proactive, les organisations peuvent maximiser les avantages du MPLS tout en atténuant les risques et en garantissant des performances réseau optimales et rentables.

3.15 Tendances futures :

Alors que le MPLS reste une technologie fondamentale pour de nombreux fournisseurs de services et entreprises,

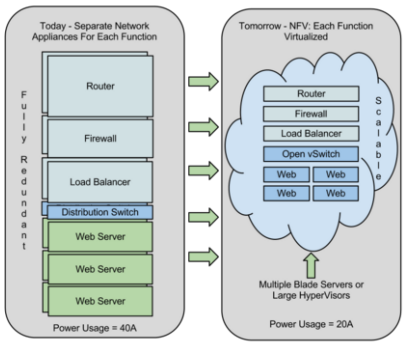
Ces avancées dans le SDN et la NFV viennent compléter les déploiements MPLS en améliorant leurs capacités et en étendant leur portée. Par exemple, le SDN peut être utilisé pour orchestrer l'ingénierie du trafic et les politiques de QoS basées sur le MPLS, tandis que la NFV peut virtualiser

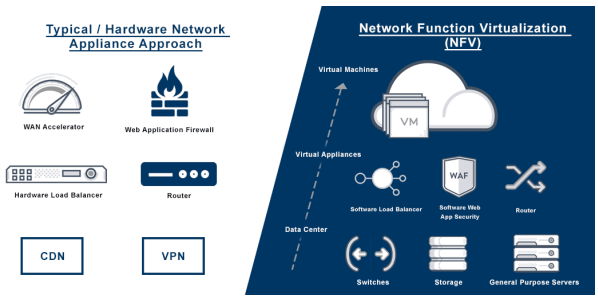
les technologies émergentes telles que le Réseau Défini par Logiciel (SDN) et la Virtualisation des Fonctions Réseau (NFV) sont en train de façonner le paysage des réseaux. Ces tendances stimulent l'innovation dans des domaines tels que l'automatisation du réseau, la programmabilité et l'agilité du service. Le SDN, par exemple, permet la gestion et le contrôle centralisés des



ressources réseau, permettant des configurations réseau plus dynamiques et adaptables. La NFV virtualise les fonctions réseau, telles que les pare-feu et les équilibreurs de charge, ce qui entraîne une plus grande flexibilité et une plus grande évolutivité.

les fonctions réseau MPLS, réduisant ainsi la dépendance matérielle et les coûts opérationnels.





À mesure que les organisations adoptent ces technologies transformatrices, l'évolution future des architectures MPLS est susceptible d'être influencée par les synergies entre le MPLS, le SDN et la NFV. Ensemble, ils offrent une boîte à outils puissante pour construire des infrastructures de communication agiles, efficaces et évolutives capables de répondre aux exigences évolutives des entreprises numériques modernes.

4 CHAPITRE 03 : Comparaison entre X.25 et MPLS

Caractéristique	X.25	MPLS
Type de protocole	Protocole de commutation de paquets	Protocole de commutation de paquets
Utilisation	Principalement utilisé dans les réseaux anciens ou hérités	Utilisé dans les réseaux modernes et IP-centric
Fonctionnalités principales	Commutation de paquets, contrôle de flux, détection d'erreurs	Routage, commutation, qualité de service (QoS), VPN
Efficacité	Moins efficace en termes de vitesse et de bande passante comparé à MPLS	Plus efficace en termes de vitesse et de bande passante par rapport à X.25
Qualité de service (QoS)	Peut offrir une QoS limitée	Peut offrir une QoS améliorée
Support VPN	Peu de support natif pour les VPN	Supporte nativement les VPN
Complexité	Moins complexe que MPLS	Plus complexe que X.25, mais offre une flexibilité accrue
Déploiement	Déploiement en déclin, remplacé par des technologies plus modernes	De plus en plus largement déployé dans les réseaux IP

Table 1: Tableau de comparaison entre X.25 et MPLS

5 CHAPITRE 04 : Relations entre X.25 et MPLS

1. Protocoles de Commutation de Paquets : Les deux sont des protocoles de commutation de paquets, ce qui signifie qu'ils sont conçus pour transférer des données de manière efficace à travers un réseau en les divisant en paquets.

2. Évolution Technologique : X.25 était largement utilisé dans les réseaux plus anciens, tandis que MPLS est une technologie plus récente et est préféré dans les réseaux modernes centrés sur IP, illustrant ainsi l'évolution des technologies réseau au fil du temps.

3. Complexité et Fonctionnalités : MPLS est plus complexe que X.25, mais offre une gamme étendue de fonctionnalités telles que le routage, la commutation, la qualité de service (QoS) et le support VPN. Cela montre comment les réseaux ont évolué pour offrir plus de fonctionnalités et de flexibilité.

4. Efficacité et Performance : MPLS est généralement considéré comme plus efficace en termes de vitesse et de bande passante par rapport à X.25, soulignant les améliorations apportées dans les performances réseau au fil du temps.

5. Déploiement et Adoption : Alors que X.25 est en déclin et est remplacé par des technologies plus modernes, MPLS est de plus en plus largement déployé dans les réseaux IP, ce qui montre comment les nouvelles technologies remplacent progressivement les anciennes pour répondre aux besoins croissants des réseaux.

En résumé, bien que X.25 et MPLS soient tous deux des protocoles de commutation de paquets, leur relation met en évidence l'évolution des technologies réseau, passant des réseaux plus anciens à des infrastructures plus modernes, avec des fonctionnalités et des performances améliorées.

6 Conclusion Générale

La comparaison entre X.25 et MPLS met en lumière l'évolution constante des technologies réseau et l'adaptation aux besoins changeants des infrastructures de communication. X.25, une technologie plus ancienne, a été largement utilisée dans les réseaux hérités, offrant une commutation de paquets mais avec des fonctionnalités limitées et des performances relativement modestes. Cependant, avec l'avènement de MPLS, une technologie plus moderne, les réseaux ont pu bénéficier d'une gamme étendue de fonctionnalités, notamment le routage, la commutation, la qualité de service et le support VPN, offrant ainsi une flexibilité et des performances accrues.

MPLS a également démontré une efficacité supérieure en termes de vitesse et de bande passante par rapport à X.25, ce qui en fait un choix privilégié pour les réseaux modernes centrés sur IP. De plus, avec sa complexité accrue, MPLS offre une meilleure adaptabilité aux exigences changeantes des réseaux d'aujourd'hui.

En fin de compte, la relation entre X.25 et MPLS reflète l'évolution dynamique des technologies de réseau, passant des anciens protocoles de commutation de paquets à des solutions plus modernes et sophistiquées, répondant ainsi aux besoins croissants de performances, de flexibilité et de sécurité dans les infrastructures de communication contemporaines.

RESSOURCES

- X.25 - LAPB — MLP — HDLC — Terminology (archive.org)
- X.25 Packet Layer Protocol (PLP) Overview (archive.org)
- ITU-T Recommendation X.28
- ITU-T Recommendation X.3
- "X.25 within the Payment Card Industry"
- ITU-T Recommendation X.25
- TU-T Recommendation X.25 (1993) White Book
- ITU-T Recommendation X.25 (1996) Grey Book
- Running X.25 over TCP/IP on Cisco routers"
- Understanding MPLS Explicit and Implicit Null Labels [archive]
- lire en ligne [archive]
- Multiprotocol Label Switching (MPLS) on Cisco Routers [archive]
- Request for comments no 7274 [archive]
- Request for comments no 3032 [archive]
- Time to Live (TTL) Processing in MPLS Networks
- IETF - Tag Distribution Protocol (draft-doolan-tdp-spec-00)
- Ipsilon Flow Management Protocol Specification for IPv4 Version 1.0
- Multiprotocol Label Switching Architecture