Module 1 (Réseau)

Environnement Technologique et Réseautique

- **Architectures de réseau**

  - PSTN
  - Internet
  - Multiprotocol Layer Switching (MPLS)
  - Cellulaires (GSM, GPRS, EDGE, UMTS: 3G, LTE et WiMax Mobile :4G)
  - Wi-Fi
  - WiMAX
  - Bluetooth
  - Réseaux ad hoc

Switched Circuits

- **Internet**
  - Réseau mondial basé sur l'envoi de paquets;
  - Familles de protocoles IP, UDP, TCP, FTP, SMTP, HTTP...
  - Les aspects techniques et architecturaux sont régis par l'Internet Engineering Task Force (IETF);
  - Les protocoles sont documentés dans les Request For Comments (RFC);
  - Réseaux locaux avec routage statique et réseau global avec routage dynamique;
  - Initialement, rien n'était prévu pour assurer la qualité de service, par exemple afin de transmettre la voix ou le vidéo en temps réel.

- **Multiprotocol Label Switching (MPLS)**

  - Le principe du MPLS consiste à générer une étiquette courte, d'une longueur fixe, correspondant, en fait, à un bref résumé de tout l'en-tête du datagramme IP.

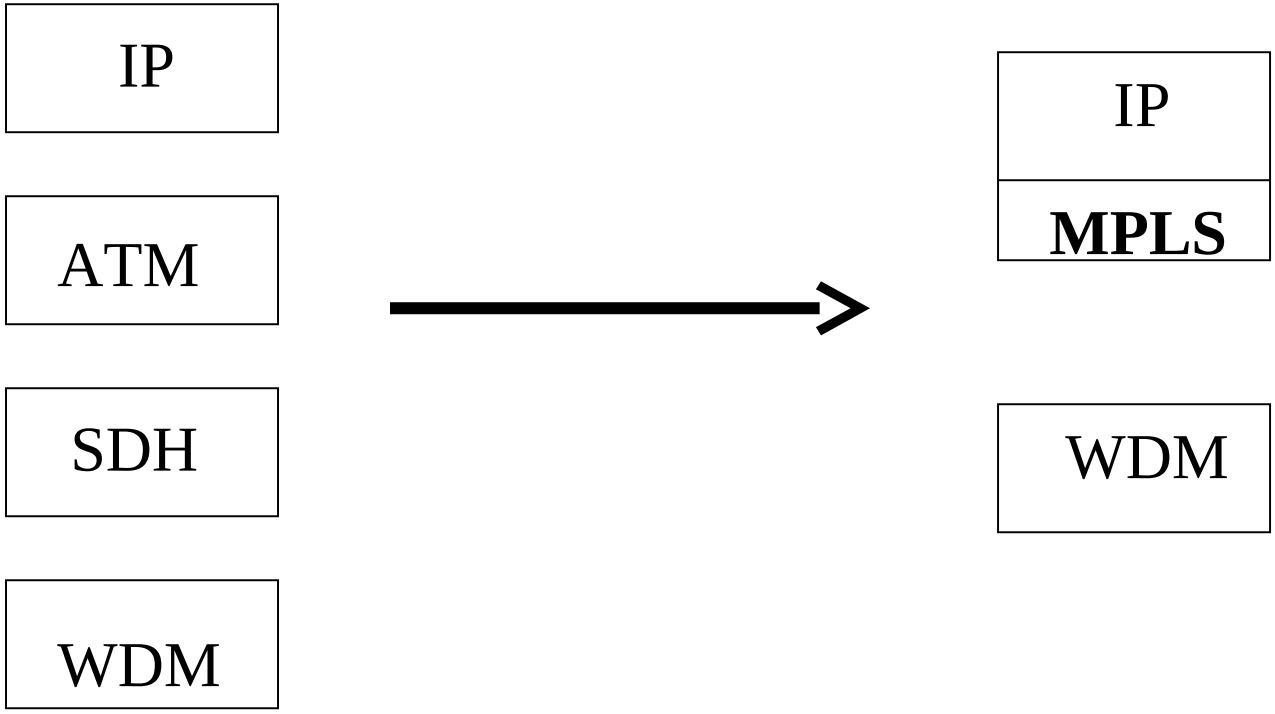
  - Le premier routeur MPLS que le datagramme rencontrera apposera une telle étiquette et le datagramme pourra être envoyé très rapidement dans le réseau MPLS en fonction de cette étiquette.

  - De l'autre côté du réseau, le datagramme IP sera de nouveau 'déballé' et acheminé de la manière classique.

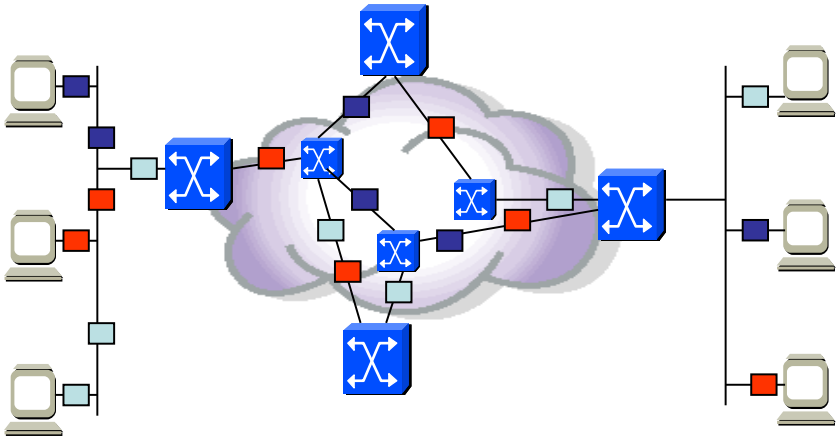
  - L'étiquette n'est pas seulement créée en fonction de l'adresse de destination, mais aussi à partir des caractéristiques de qualité de service et de gestion de l'encombrement.

  - Cette méthode peut être comparée à celle utilisée par la Poste. En mettant un code postal sur une lettre, il n'est pas nécessaire d'interpréter toute l'adresse. Ce n'est que lorsque la lettre arrive dans la ville de destination que l'on regarde toute l'adresse pour déterminer le dernier trajet d 'une lettre.

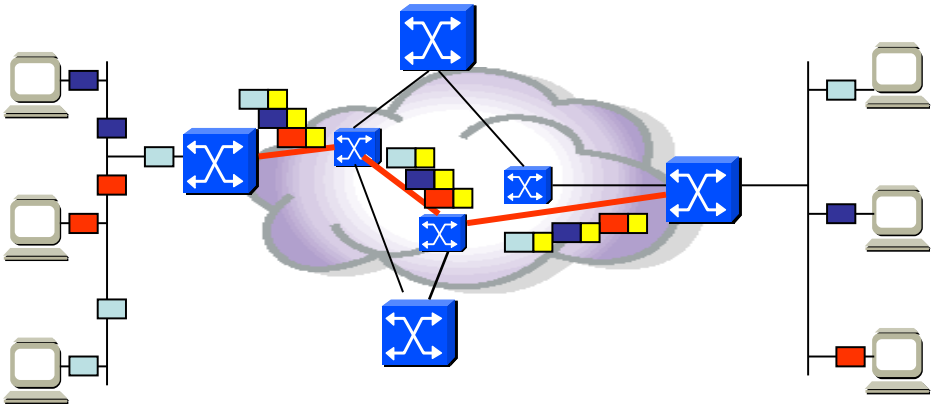
Simplification de l'Internet



Routage MPLS

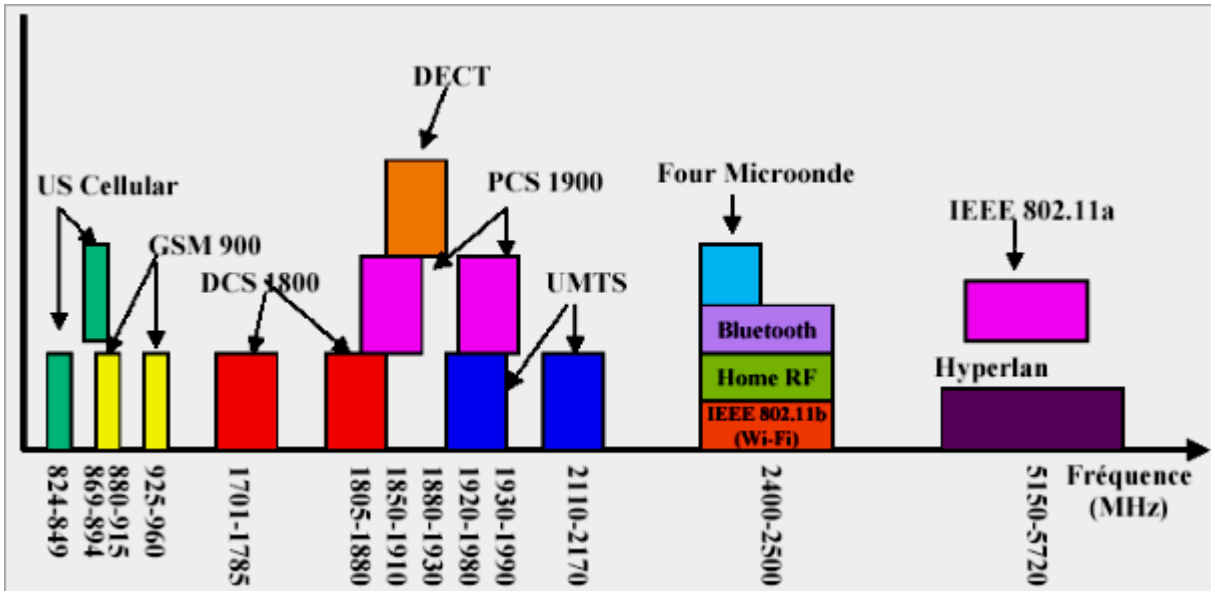


Routage classique IP

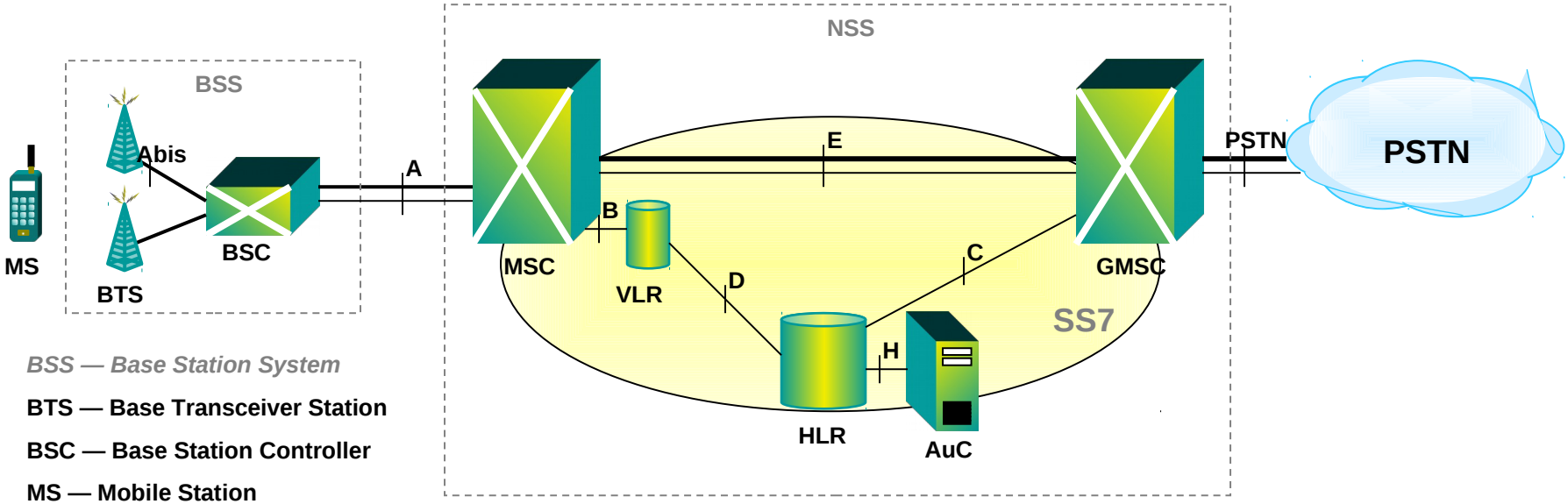


Routage MPLS

- **Les réseaux sans fil, fixes ou mobiles**



Architecture GSM



BSS — Base Station System

BTS — Base Transceiver Station

BSC — Base Station Controller

MS — Mobile Station

NSS — Network Sub-System

MSC — Mobile-service Switching Controller

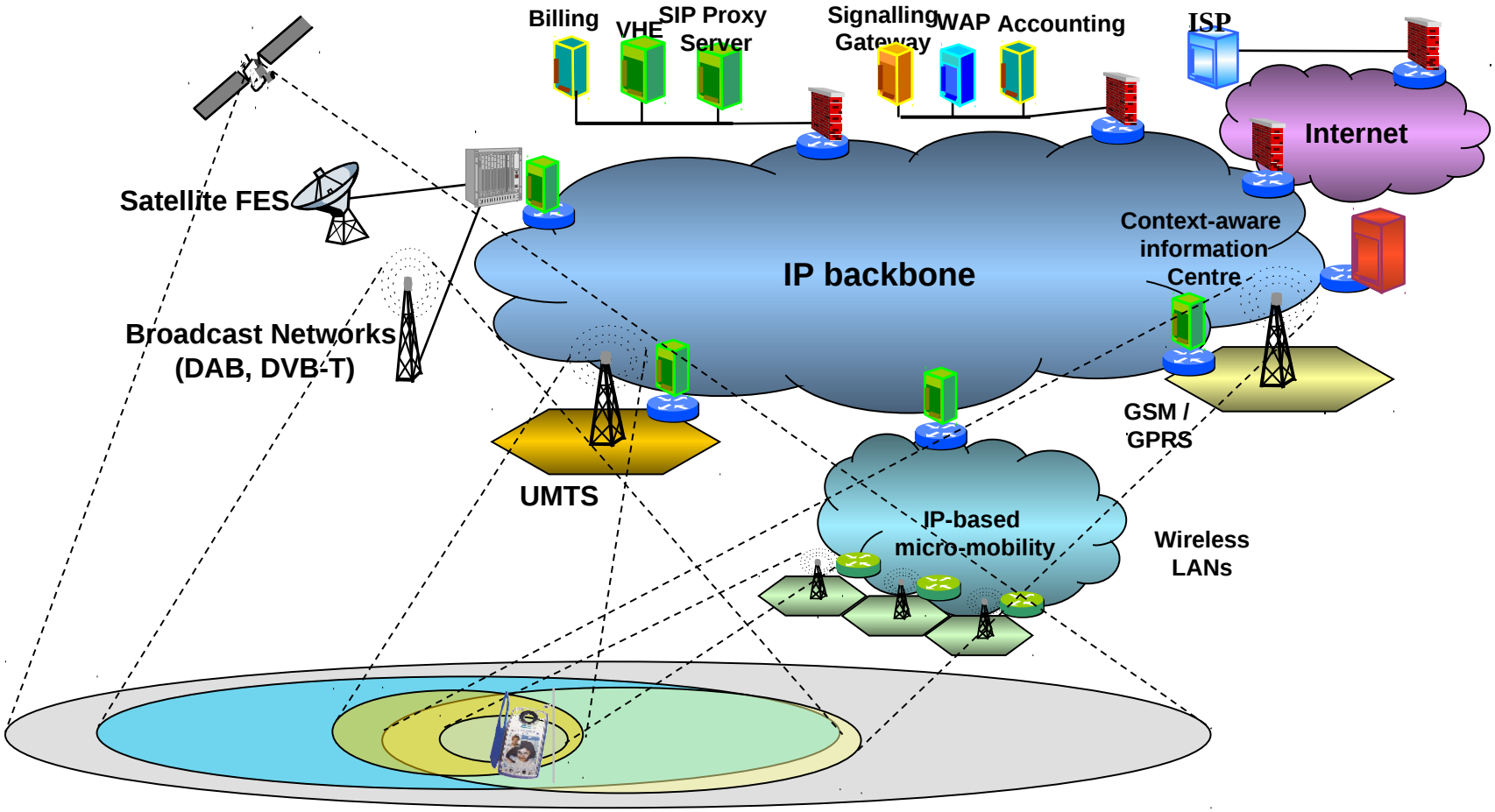
VLR — Visitor Location Register

HLR — Home Location Register

AuC — Authentication Server

GMSC — Gateway MSC

Vision tout-IP (‘ALL-IP Networks’)



Norme IEEE 802.11 (Wi-Fi)

- Wi-Fi : Wireless Fidelity

- Originellement IEEE 802.11b (11 Mbps) mais il y a eu aussi 802.11a (54 Mbps).

- Maintenant 802.11g (54 Mbps) et 802.11n (600 Mbps) sont très répandus et 802.11ac (6930 Mbps) est aussi disponible.

- Rayon de 50 mètres approximativement pour chaque point d’accès selon les obstacles.

WiMax

- WiMax (Worldwide Interoperability for Microwave Access) est une une famille de normes techniques permettant de livrer une connectivité haute vitesse sur le dernier kilomètre;
- Haut débit;
- Grande couverture;
- Alternative à ADSL.

Équipements WiMax

Station de base

Récepteur chez le client

Le récepteur est une antenne chez le client. L'antenne peut être connecté à partir d'une liaison Wi-Fi à l'équipement du client ou à un modem WiMax chez le client.

Bluetooth

- Technologie ayant évolué des principes de conception des réseaux cellulaires (basé sur 802.11 en mode ad hoc)
- Norme de communication de courte portée (jusqu'à 10 m mais peut être étendue à 100 m)
- Fonctionne à 3.4 GHz, près de la fréquence micro-onde, dans la part de la bande de fréquence qui ne requiert pas de licence d'opération (ISM - Industrial, Scientific and Medical)
- Effectue des sauts de fréquence rapides (1600 sauts/seconde) entre 79 fréquences de manière à éviter les interférences
- Technologie full-duplex (canal de communication dans les deux sens) en utilisant le TDD (Time Division Duplex)

Réseaux ad hoc

- La topologie change fréquemment, nœuds entrent, sortent, bougent;
- Découverte des voisins par diffusion de message;
- Capacités réduites en mémoire, calcul et puissance
- Pas d'identificateur global
- Déployés en grand nombre (10^3, 10^6)
- Réseaux de capteurs
- Exemple: Zigbee et Z-Wave pour la domotique

La sécurité

- Intégrité de l'information;
- Confidentialité de l'information;
- Disponibilité du service, coût, réputation;

- Authentification: garantie de l’identité du correspondant;
- Somme de contrôle cryptographique: intégrité et non répudiation
- Encryption: confidentialité;
- Contrôle d'accès: usager, groupe, administrateur, rôle, délégation...

- Attaques en déni de service, virus, cheval de troie, exploitation de vulnérabilité réseau, clé USB, accès physique...

La sécurité avec un réseau non fiable

- Un message peut être vu, intercepté, modifié, ajouté, retardé ou rejoué;
- Systèmes de clés publiques pour initier une connexion; des clés symétriques peuvent être communiquées et utilisées par la suite.
  - Paire de clés, une publique, l'autre privée;
  - Chaque utilisateur a deux paires, l'une avec chiffrement publique (déchiffrement secret) permettant à chacun d'écrire un message que seul cet utilisateur peut lire, l'autre avec déchiffrement publique (chiffrement secret) permettant à cet utilisateur d'envoyer un message que lui seul peut avoir envoyé mais tous peuvent lire.
- Avoir un message avec temps, date, numéro de séquence chiffré avec la clé publique du destinataire et la clé privée de l'envoyeur.

La sécurité d'un système

- Sécurité physique: accès au serveur, à l'ordinateur utilisé par l'administrateur de système, au courrier contenant les logiciels à installer...
- Sécurité humaine: persuader un employé de donner un accès...
- Les vulnérabilités dans les logiciels existent;
- Mise à jour de sécurité fréquentes;
- Multiples lignes de défense, pare-feu, détection d'intrusion, vérification d'intégrité, monitoring réseau, contrôle fin des accès, vérification des log...
- Analyse des risques, plan de contingence.