

# **Pratique des réseaux**

## **SR200**

**Support de formation**



## Table des matières

Introduction .....	4
• Avant de commencer .....	5
• Objectifs de la formation .....	6
Chapitre 1 – Pourquoi un réseau ? .....	9
• Objectifs du chapitre .....	10
• Ateliers .....	28
• Ce qu'il faut retenir .....	29
Chapitre 2 – Le réseau Ethernet .....	30
• Objectifs du chapitre .....	31
• Ce qu'il faut retenir .....	54
Chapitre 3 – Commutation Ethernet ou « switching » .....	55
• Objectifs du chapitre .....	56
• Atelier .....	62
• Atelier .....	75
• Atelier .....	77
• Atelier .....	89
• Atelier .....	92
• Ateliers .....	96
• Ce qu'il faut retenir .....	97
Chapitre 4 - Wifi .....	98
• Objectifs du chapitre .....	99
• Ce qu'il faut retenir .....	122
Chapitre 5 – TCP/IP .....	123
• Objectifs du chapitre .....	124
• Ce qu'il faut retenir .....	164
Chapitre 6 – DHCP et DNS .....	165
• Objectifs du chapitre .....	166
• Ce qu'il faut retenir .....	181
Chapitre 7 – Administration et SNMP .....	182
• Objectifs du chapitre .....	183

---

• Ce qu'il faut retenir.....	194
Ce qu'il faut retenir de la formation .....	195

## Introduction



• Avant de commencer

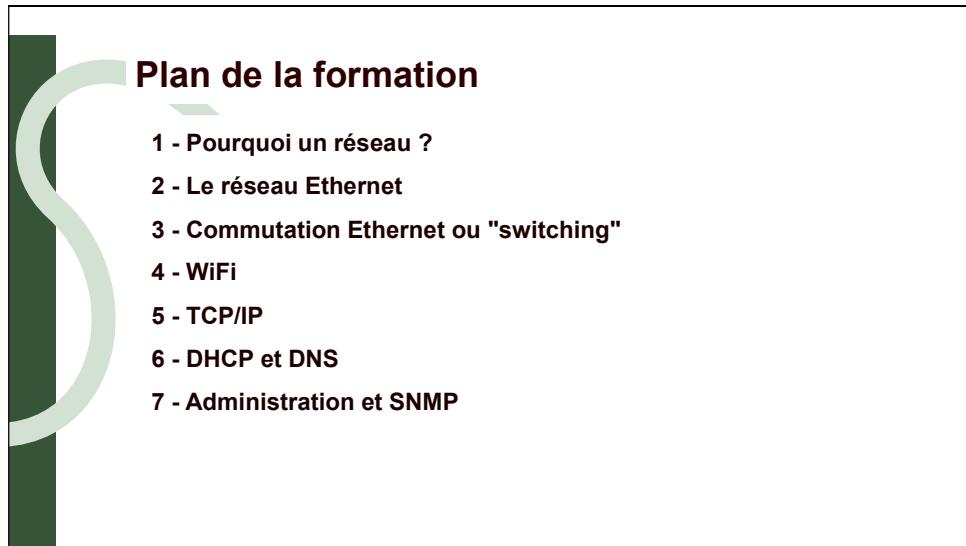


— Priorité aux échanges  
(durant les ateliers également)

— Tour de table :

- ▶Prénom, nom, Société, Titre/fonction  
Dans le tableau blanc Teams :
  - Votre expérience sur le sujet de la formation ?
  - Vos attentes de la formation

- Objectifs de la formation



### **Bienvenue dans notre Formation sur la Pratique des Réseaux !**

Chers participants.

C'est avec un immense plaisir que nous vous accueillons dans cette aventure d'apprentissage conçue pour transformer votre compréhension et votre maîtrise des technologies réseau. Que vous soyez novice désireux de poser les premières pierres de votre parcours dans le domaine des réseaux. ou professionnel cherchant à approfondir vos compétences. cette formation est faite pour vous.

#### **Notre Cheminement Ensemble :**

Nous débuterons par explorer les **fondations des réseaux** - comprendre pourquoi ils existent et comment ils ont évolué pour devenir l'ossature de notre monde numérique. Cette première étape posera les bases nécessaires pour naviguer avec aisance dans le monde complexe des réseaux informatiques.

Ensuite. nous plongerons dans les détails du **réseau Ethernet**. le pilier des connexions filaires. Vous apprendrez comment les données voyagent. comment elles sont dirigées et comment assurer leur transmission efficace et sécurisée.

Le troisième chapitre vous emmènera dans l'univers du **WiFi**. où la liberté rencontre la connectivité. Vous découvrirez comment configurer. sécuriser et optimiser les réseaux sans fil pour répondre aux besoins variés des utilisateurs et des entreprises.

Avec une compréhension solide des infrastructures réseau. nous aborderons ensuite le cœur battant de l'Internet : les protocoles **TCP/IP**. Cette section dévoilera comment les données sont structurées. adressées et routées à travers le vaste réseau mondial.

La gestion dynamique des adresses IP à travers **DHCP** et la résolution des noms de domaine via **DNS** constitueront notre cinquième étape. essentielle pour maintenir les réseaux fluides et accessibles.

Finalement. nous clôturerons notre parcours en explorant **SNMP**. un outil puissant pour administrer et surveiller les réseaux. assurant ainsi leur performance et leur sécurité.

**À l'Issue de cette Formation :**

Vous serez non seulement capables de comprendre les principes fondamentaux qui régissent les réseaux modernes. mais aussi d'appliquer concrètement vos connaissances pour configurer. gérer et résoudre les problèmes réseau. Vous aurez les outils pour faire des choix éclairés sur la sécurité. l'optimisation et la gestion des ressources réseau. contribuant ainsi à la construction d'infrastructures numériques fiables et robustes.

Nous sommes convaincus que cette formation enrichira vos compétences et élargira vos perspectives professionnelles. Ensemble. engageons-nous dans ce voyage d'apprentissage pour débloquer le potentiel illimité des réseaux informatiques.

Bienvenue à bord. et que notre aventure commence !

**Les objectifs pédagogiques de cette formation :****Comprendre les Fondamentaux des Réseaux :**

Expliquer les principes de base et l'évolution des réseaux informatiques.

Identifier les principaux organismes de normalisation (IEEE. OSI. UIT. IETF) et la différence entre normes et RFC.

Classifier les réseaux en fonction de leur étendue (PAN. LAN. MAN. WAN) et comprendre les différents types de communication (unicast. multicast. broadcast. anycast).

Décrire les couches du modèle OSI. leur rôle et le processus d'encapsulation.

Reconnaître et expliquer le rôle des principaux composants d'un réseau.

**Maîtriser le Réseau Ethernet :**

Comprendre les concepts de domaine de collision et de domaine de broadcast.

Expliquer la méthode d'accès CSMA/CD et comment les collisions sont gérées.

Dérypter l'adressage MAC et connaître les circonstances de modification d'une adresse MAC.

Identifier l'évolution des topologies réseau et les standards de câblage.

**Gérer la Commutation Ethernet et les VLANs :**

Comprendre la commutation de niveau 2. y compris l'auto-apprentissage et l'apprentissage statique.

Configurer et résoudre des problèmes sur les VLANs. et comprendre l'importance et le fonctionnement du protocole 802.1q.

Mettre en œuvre et dépanner des architectures réseau redondantes utilisant le Spanning Tree et l'agrégation de liens.

**Déployer et Sécuriser un Réseau WiFi :**

Comprendre les principes de base des réseaux WLAN. y compris les normes 802.11.

Analyser les performances et sécuriser un réseau WiFi en entreprise.

Utiliser des outils de diagnostic pour visualiser et optimiser la couverture WiFi.

**Comprendre et Appliquer le TCP/IP :**

Expliquer le fonctionnement des protocoles au sein de l'empilement TCP/IP.

Configurer et dépanner l'adressage IP. y compris la gestion des sous-réseaux.

Analyser le fonctionnement de TCP et UDP. y compris la gestion des connexions. la transmission de données et les particularités de chaque protocole.

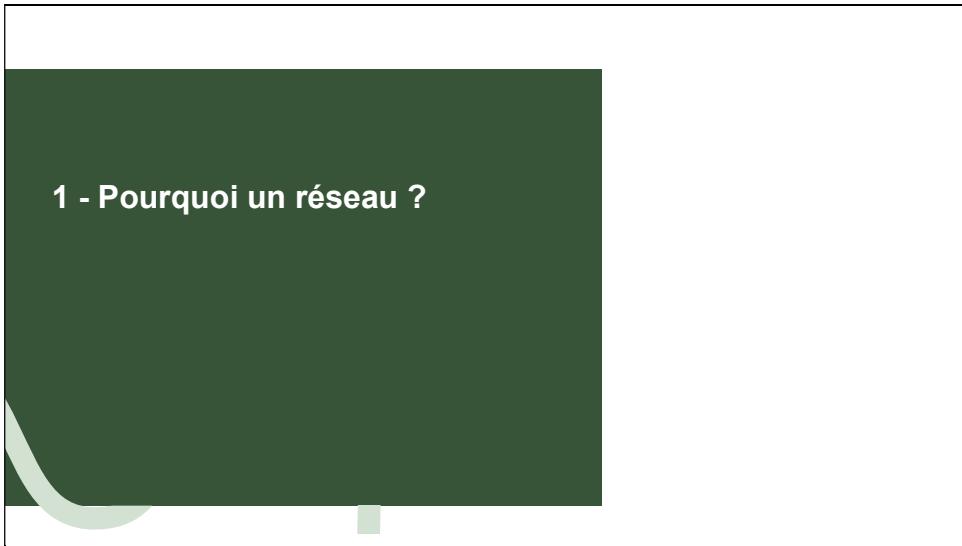
**Configurer DHCP et DNS :**

Comprendre et configurer les services DHCP pour la gestion dynamique des adresses IP.  
Mettre en place et interroger des serveurs DNS pour la résolution de noms.  
Gérer la redondance et la tolérance aux pannes dans les services de noms et d'adressage.

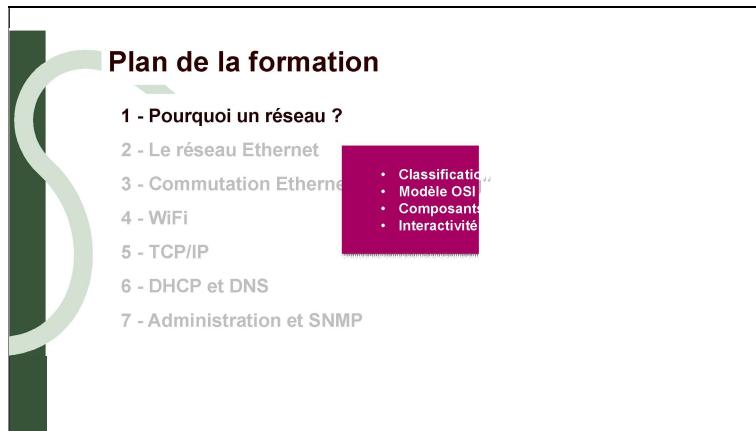
**Administre les Réseaux via SNMP :**

Comprendre les bases de la gestion de réseau via SNMP.  
Configurer et utiliser SNMP pour le monitoring et la gestion des dispositifs réseau.  
Utiliser des outils pour parcourir les MIBs et analyser les échanges SNMP.  
Ces objectifs pédagogiques servent à orienter les participants vers les compétences clés qu'ils acquerront tout au long de la formation. leur permettant ainsi de comprendre, configurer, et dépanner des réseaux informatiques dans divers contextes professionnels.

## Chapitre 1 – Pourquoi un réseau ?



- Objectifs du chapitre



Ce chapitre inaugural pose les bases essentielles pour la compréhension des réseaux informatiques. Il est crucial de contextualiser la pertinence de ce chapitre au début de la formation, car il met en place le cadre conceptuel sur lequel s'appuieront tous les autres modules. Voici quelques consignes pour guider votre **introduction** :

**Établir la Connexion avec le Quotidien :**

Commencez par présenter les réseaux informatiques à travers des exemples concrets tirés de la vie quotidienne des participants, illustrant l'omniprésence et l'importance des réseaux dans le monde moderne.

**Historique et Évolution :**

Offrez un bref aperçu historique montrant l'évolution des réseaux depuis leur création jusqu'aux technologies actuelles, en mettant l'accent sur les innovations majeures qui ont façonné le paysage actuel des réseaux.

**Organismes et Standards :**

Introduisez les principaux organismes de normalisation et expliquez pourquoi il est essentiel de comprendre leur rôle. Discutez de l'importance des normes et des RFC dans le développement et l'interfonctionnement des réseaux.

**Objectifs pédagogiques des sujets :**

**Classification des Réseaux :**

Expliquez la classification des réseaux et sa pertinence pratique. Utilisez des visuels ou des schémas pour clarifier les différences entre PAN, LAN, MAN, et WAN.

**Modes de Communication :**

Illustrer par des analogies ou des scénarios réels les différents types de communication réseau (unicast, multicast, broadcast, anycast), afin de les rendre plus accessibles et compréhensibles.

**Le Modèle OSI :**

Présentez le modèle OSI comme la fondation théorique nécessaire pour comprendre la structure et le fonctionnement interne des réseaux. Soulignez l'importance de chaque couche et le concept d'encapsulation.

**Composants d'un Réseau :**

Faites correspondre les composants matériels du réseau avec leur fonction. Si possible, montrez de réels composants ou des images pour renforcer la compréhension.

**Interactivité et Engagement :**

Encouragez la participation active dès le début. Posez des questions ouvertes pour susciter la curiosité et le dialogue autour des sujets abordés.



- "Comment la capacité de partager instantanément des informations a-t-elle changé votre environnement de travail ou votre vie personnelle ?"
- "Pouvez-vous penser à une situation où un réseau n'était pas disponible et cela a eu un impact significatif sur votre activité ou votre productivité ? Qu'auriez-vous souhaité améliorer dans cette situation ?"
- "Avez-vous déjà eu besoin d'accéder à des ressources ou des données situées hors de votre emplacement immédiat ? Comment pensez-vous qu'un réseau pourrait faciliter cet accès ?"
- "Dans quelles circonstances est-il crucial pour vous d'avoir une connexion fiable et quels problèmes cela résoudrait-il dans votre quotidien ?"
- "Pourquoi est-il important pour vous que vos données soient sécurisées lors de l'échange d'informations ? Comment pensez-vous qu'un réseau bien conçu peut contribuer à cette sécurité ?"

**Communication et Partage d'Informations :**

"Comment la capacité de partager instantanément des informations a-t-elle changé votre environnement de travail ou votre vie personnelle ?"

**Dépendance aux Réseaux :**

"Pouvez-vous penser à une situation où un réseau n'était pas disponible et cela a eu un impact significatif sur votre activité ou votre productivité ? Qu'auriez-vous souhaité améliorer dans cette situation ?"

**Organisation et Accès aux Ressources :**

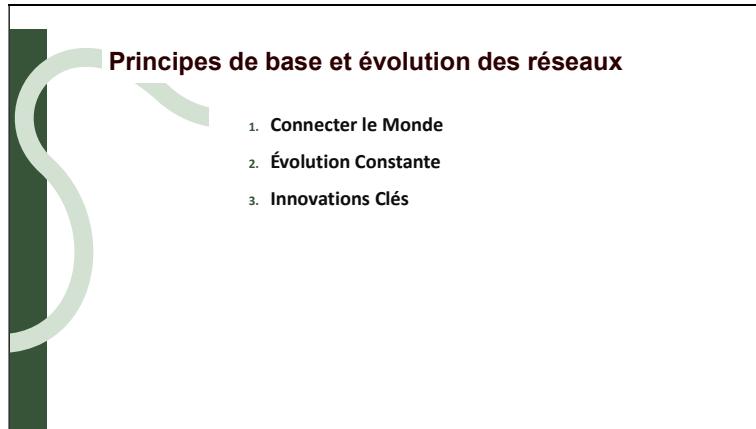
"Avez-vous déjà eu besoin d'accéder à des ressources ou des données situées hors de votre emplacement immédiat ? Comment pensez-vous qu'un réseau pourrait faciliter cet accès ?"

**Fiabilité et Connectivité :**

"Dans quelles circonstances est-il crucial pour vous d'avoir une connexion fiable et quels problèmes cela résoudrait-il dans votre quotidien ?"

**Sécurité des Données et des Échanges :**

"Pourquoi est-il important pour vous que vos données soient sécurisées lors de l'échange d'informations ? Comment pensez-vous qu'un réseau bien conçu peut contribuer à cette sécurité ?"



## Principes de base et évolution des réseaux

1. Connecter le Monde
2. Évolution Constante
3. Innovations Clés

### Principes de base et évolution des réseaux

Les réseaux informatiques ont transformé la manière dont nous vivons, travaillons et communiquons. À la base, un réseau informatique est un ensemble d'ordinateurs, de dispositifs et d'autres équipements connectés qui partagent des ressources, des données et, souvent, une connexion Internet. Les raisons fondamentales de la mise en place d'un réseau informatique incluent le partage d'informations et de ressources, l'amélioration de la communication et l'augmentation de l'efficacité et de la productivité.

### Évolution Historique des Réseaux

L'évolution des réseaux est une histoire fascinante de progrès technologiques et d'innovations. Elle commence avec les premiers systèmes de télécommunication comme le télégraphe et le téléphone, évoluant vers les réseaux de données informatiques dans les années 1960 et 1970. L'introduction d'ARPANET, considéré comme le précurseur de l'Internet, a marqué une étape déterminante, posant les bases de la communication en réseau telle que nous la connaissons aujourd'hui.

Les avancées technologiques majeures qui ont jalonné l'histoire des réseaux comprennent le développement de protocoles de communication standardisés, l'émergence des technologies Ethernet pour les réseaux locaux (LAN), l'avènement du WiFi pour une connectivité sans fil flexible et l'expansion de l'Internet à l'échelle mondiale. Chaque innovation a contribué à augmenter la vitesse, la capacité et la portée des réseaux, permettant l'émergence de nouveaux usages comme le streaming vidéo, les jeux en ligne et les applications cloud. À l'ère numérique actuelle, les réseaux continuent d'évoluer à une vitesse impressionnante, avec le déploiement de la fibre optique, des réseaux 5G, et au-delà, promettant des vitesses de connexion encore plus rapides et une connectivité omniprésente. Cette évolution est propulsée par une demande croissante de bande passante et par les besoins en communication de technologies émergentes comme l'Internet des Objets (IoT), la réalité virtuelle et augmentée, et l'intelligence artificielle.

### Conclusion

Comprendre les principes de base et l'évolution des réseaux est essentiel pour apprécier le rôle central que jouent ces technologies dans notre société. Ils ne se limitent pas à connecter des ordinateurs entre eux, mais sont le fondement de notre monde interconnecté, influençant profondément nos interactions, notre économie et notre culture. En tant que stagiaires de cette formation, vous êtes invités à explorer ces concepts et à envisager comment les avancées futures des réseaux pourraient continuer à transformer notre monde.



**Principaux organismes : IEEE. ISO. UIT. IETF**

1. **Gardiens des Standards :**  
IEEE. ISO. UIT. IETF définissent les règles du jeu en matière de communication réseau. assurant compatibilité et interopérabilité.
2. **Normes vs. RFC :**  
Les normes établissent des protocoles universels. tandis que les RFC encouragent l'innovation et l'adaptation rapide aux nouvelles technologies.
3. **Unification par la Standardisation :**  
La collaboration entre ces organismes facilite un réseau mondial unifié. permettant une communication sans frontières.

## Principaux Organismes de Normalisation des Réseaux

Dans le monde des réseaux. plusieurs organismes jouent un rôle crucial dans la définition des standards qui garantissent l'interopérabilité et la fiabilité des technologies de communication. Comprendre le rôle de chacun de ces organismes vous aidera à naviguer dans l'écosystème complexe des normes de réseau.

•**IEEE (Institute of Electrical and Electronics Engineers)** : Principalement connu pour ses standards relatifs à la technologie Ethernet (IEEE 802.3) et au WiFi (IEEE 802.11). l'IEEE est un acteur majeur dans la définition des normes qui régissent les réseaux locaux et les réseaux sans fil.

•**ISO (International Organization for Standardization)**. il fournit

•**UIT (Union Internationale des Télécommunications)** : Spécialisée dans les standards de communication à l'échelle mondiale. l'UIT se concentre sur les télécommunications et leur intégration dans les réseaux d'information. assurant la cohérence des technologies à travers le globe.

•**IETF (Internet Engineering Task Force)** : L'IETF est responsable de l'élaboration et de la promotion des standards Internet. notamment les protocoles TCP/IP. Les Request for Comments (RFC). bien que non obligatoires comme les normes. jouent un rôle vital dans l'évolution d'Internet en documentant les spécifications. les innovations et les meilleures pratiques.

### Normes vs. RFC

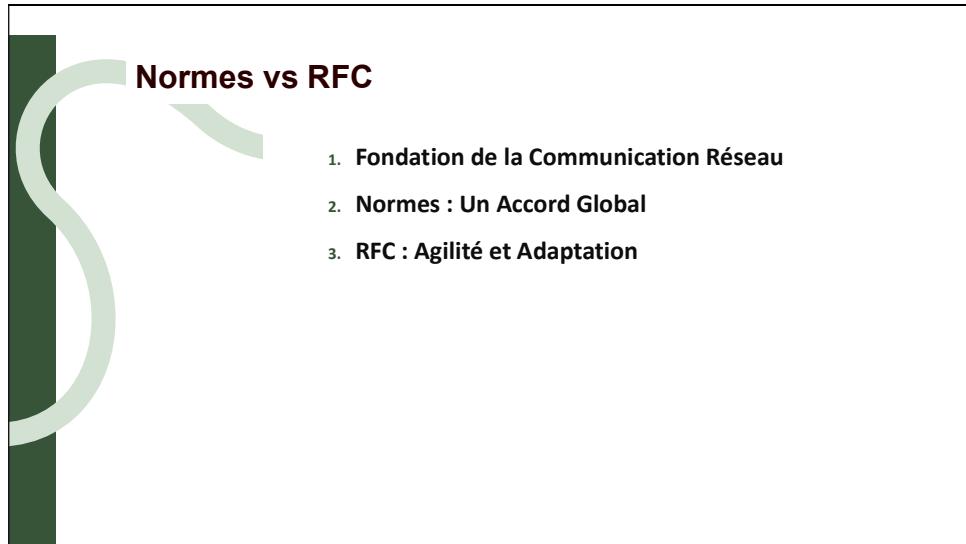
La distinction entre les normes (comme celles développées par l'IEEE) et les RFC (publiées par l'IETF) réside dans leur approche et leur application. Les normes sont généralement des spécifications techniques détaillées conçues pour être suivies à la lettre. assurant ainsi l'interopérabilité entre les équipements et les systèmes. Les RFC. en revanche. sont plus souples. permettant une évolution plus rapide et l'expérimentation dans le développement de nouveaux protocoles et technologies.

### Impact sur l'Interopérabilité

L'adhésion aux normes et l'application des RFC sont fondamentales pour l'interopérabilité des équipements et des protocoles réseau. Elles garantissent que différents dispositifs. souvent développés par différents fabricants. peuvent communiquer efficacement entre eux. formant la base d'un réseau mondial connecté et cohérent.

**Conclusion**

Les organismes de normalisation jouent un rôle indispensable dans l'unification et la standardisation des technologies de réseau. Leur travail assure que les innovations restent compatibles et interopérables, facilitant ainsi une infrastructure réseau mondiale robuste et accessible. En tant que professionnels du réseau, une compréhension approfondie de ces organismes et de leur impact vous permettra de mieux appréhender la complexité des réseaux modernes et de contribuer efficacement à leur développement et leur maintenance.



## Normes vs RFC

1. Fondation de la Communication Réseau
2. Normes : Un Accord Global
3. RFC : Agilité et Adaptation

### Normes vs. RFC : Définir les Règles du Réseau

Dans le domaine des technologies de réseau, la distinction entre normes et Request for Comments (RFC) est fondamentale pour comprendre comment les protocoles et les technologies évoluent pour répondre aux besoins changeants de l'industrie.

#### Normes : Le Langage Universel des Réseaux

Les normes sont des spécifications techniques développées par des organismes de normalisation reconnus, comme l'IEEE ou l'UIT. Elles sont le résultat d'un processus de consensus entre les experts de l'industrie, les universitaires et les gouvernements. Les normes visent à assurer l'interopérabilité entre les dispositifs de réseau, garantissant que les équipements de différents fabricants peuvent travailler ensemble sans problème. Elles couvrent une vaste gamme d'aspects techniques, allant de la transmission physique des données à la manière dont les messages sont structurés et transmis.

#### RFC : Documents Vivants de l'Internet

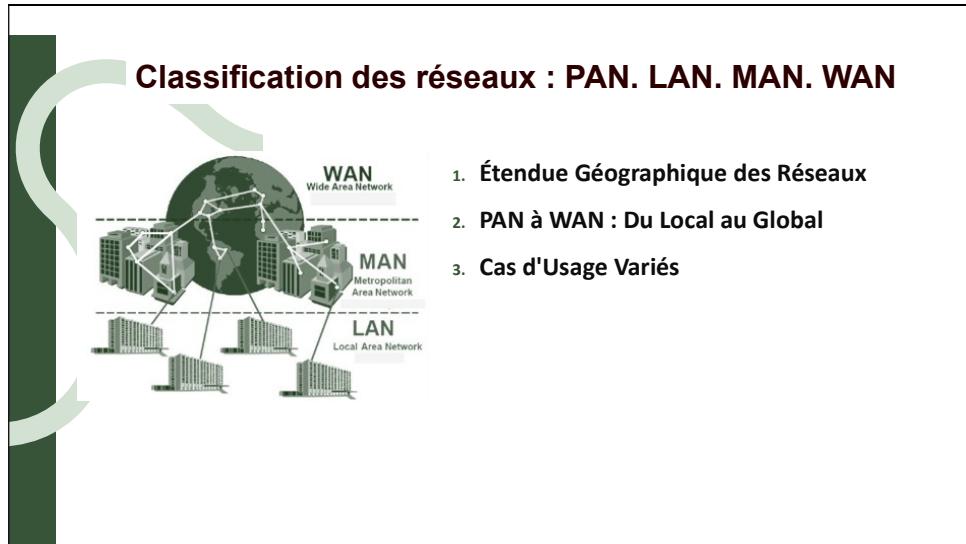
Les Request for Comments, quant à eux, sont une série de documents publiés par l'Internet Engineering Task Force (IETF) et d'autres groupes de travail. Les RFC documentent les spécifications de protocoles, les meilleures pratiques et d'autres informations pertinentes pour le fonctionnement d'Internet et des réseaux en général. Contrairement aux normes, les RFC ne sont pas toujours destinées à devenir des standards obligatoires. Elles servent plutôt de forum pour l'échange d'idées, de propositions techniques et de recommandations. Les RFC permettent une certaine flexibilité et adaptabilité, avec la possibilité de mettre à jour ou de remplacer les documents existants en réponse aux avancées technologiques ou aux changements dans les pratiques de l'industrie.

**Impact sur l'Interopérabilité et l'Innovation**

L'interaction entre normes et RFC est cruciale pour l'évolution des réseaux. Les normes fournissent la stabilité et la prévisibilité nécessaires pour construire et maintenir des infrastructures réseau à grande échelle. En parallèle, les RFC stimulent l'innovation en permettant aux ingénieurs et développeurs d'expérimenter de nouvelles idées et technologies qui, une fois éprouvées, peuvent être adoptées comme nouvelles normes ou meilleures pratiques.

**Conclusion**

La compréhension des rôles complémentaires joués par les normes et les RFC est essentielle pour tout professionnel du réseau. Ensemble, elles façonnent le paysage des technologies de communication, équilibrant la nécessité d'un cadre stable et interopérable avec la capacité à innover et à s'adapter aux défis émergents. En tant que participants à cette formation, vous êtes encouragés à explorer et à contribuer à cet écosystème dynamique, où les normes et les RFC continuent de définir les fondations de nos réseaux mondiaux connectés.



### Classification des Réseaux Informatiques : De PAN à WAN

La classification des réseaux informatiques selon leur étendue géographique fournit un cadre pour comprendre comment différents types de réseaux répondent à des besoins spécifiques. qu'ils soient destinés à un usage personnel. professionnel. ou à grande échelle.

#### Types de Réseaux

- **PAN (Personal Area Network)** : Un réseau PAN est conçu pour l'usage personnel dans un espace très restreint. typiquement quelques mètres. Il connecte des dispositifs personnels tels que téléphones. ordinateurs portables. et wearables. Exemple d'utilisation : connexion Bluetooth entre un smartphone et une montre intelligente.
- **LAN (Local Area Network)** : Un LAN couvre une petite zone géographique. comme une maison. une école. ou un petit bureau. Il facilite le partage de ressources comme les fichiers et les imprimantes entre plusieurs utilisateurs. Exemple d'utilisation : un réseau d'entreprise connectant les ordinateurs des employés.
- **MAN (Metropolitan Area Network)** : Un MAN s'étend sur une plus grande zone géographique. typiquement une ville ou une région métropolitaine. Il peut connecter plusieurs LANs entre eux. Exemple d'utilisation : réseau d'une université répartie sur plusieurs campus dans une ville.
- **WAN (Wide Area Network)** : Le WAN a la plus grande portée. couvrant des zones géographiques étendues. souvent à l'échelle nationale ou internationale. Internet est l'exemple le plus connu de WAN. reliant des réseaux du monde entier. Exemple d'utilisation : le réseau d'une multinationale connectant ses bureaux à travers le monde.

**Cas d'Usage**

La classification des réseaux n'est pas juste une question de taille; elle détermine également les technologies et les protocoles les mieux adaptés à chaque type de réseau. Par exemple, les réseaux PAN utilisent souvent des technologies sans fil comme Bluetooth, tandis que les WAN peuvent s'appuyer sur des liaisons satellite ou des câbles sous-marins pour la transmission de données sur de longues distances.

**Conclusion**

Comprendre la classification des réseaux informatiques selon leur étendue géographique et leurs cas d'usage spécifiques est essentiel pour choisir la bonne infrastructure réseau. Que ce soit pour connecter des dispositifs personnels dans un espace restreint ou pour assurer la communication globale entre des bureaux à travers le monde, chaque type de réseau offre des solutions adaptées aux besoins des utilisateurs et des organisations.



## **Les types de communication entre machines : unicast. multicast. broadcast et anycast**

1. Diversité des Communications Réseau
2. Unicast : Communication 1 vers 1
3. Multicast : Communication 1 vers N
4. Broadcast (Diffusion) : Communication 1 vers \*
5. Anycast : Communication 1 vers le plus proche

### **Les Types de Communication Entre Machines : Un Aperçu**

Dans les réseaux informatiques, les données peuvent être transmises entre machines de plusieurs manières, chacune répondant à des besoins spécifiques en termes de portée, de performance et d'utilisation de la bande passante. Comprendre ces modes de communication est essentiel pour concevoir et gérer efficacement des réseaux.

### **Modes de Communication Réseau**

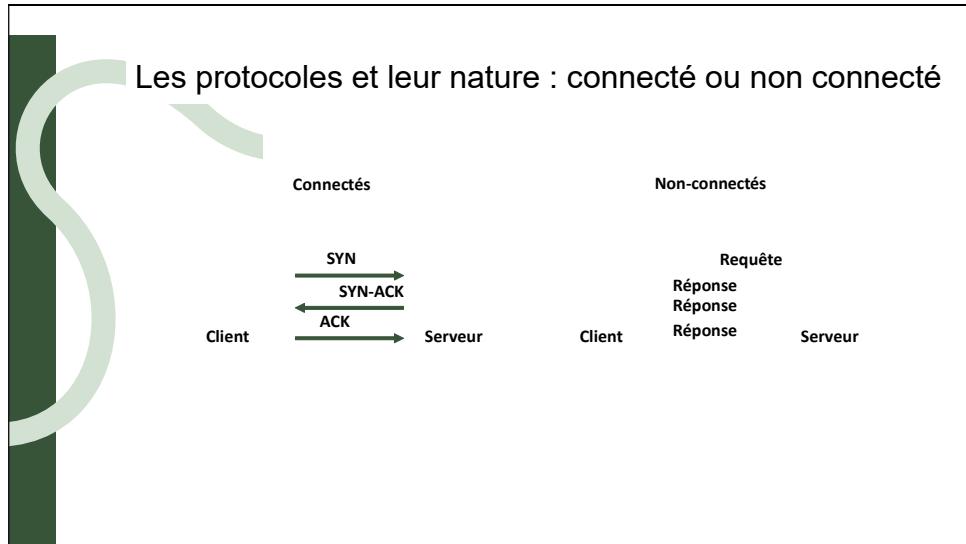
- **Unicast** : Le mode unicast représente la forme de communication la plus courante sur les réseaux, où les données sont envoyées d'un dispositif unique à un autre dispositif unique. Ce mode est utilisé pour la plupart des communications sur Internet, telles que le chargement d'une page web ou l'envoi d'un email.
- **Multicast** : Le multicast permet à une source d'envoyer un message à plusieurs destinataires spécifiques dans un groupe. Ce mode est particulièrement utile pour la diffusion de contenu multimédia, comme la télévision IP (IPTV) ou les conférences vidéo, où les mêmes données doivent être distribuées à plusieurs utilisateurs.
- **Broadcast** : Dans le mode broadcast, les données sont envoyées de manière indifférenciée à tous les dispositifs sur le réseau. Ce mode est souvent utilisé pour la découverte de services sur un réseau local (LAN), comme l'attribution dynamique d'adresses IP par DHCP.
- **Anycast** : L'anycast est un mode de communication où les données sont envoyées à la première machine disponible parmi un groupe de destinataires potentiels, généralement utilisé pour optimiser l'accès aux services répartis géographiquement, comme les serveurs DNS.

**Utilisations Typiques**

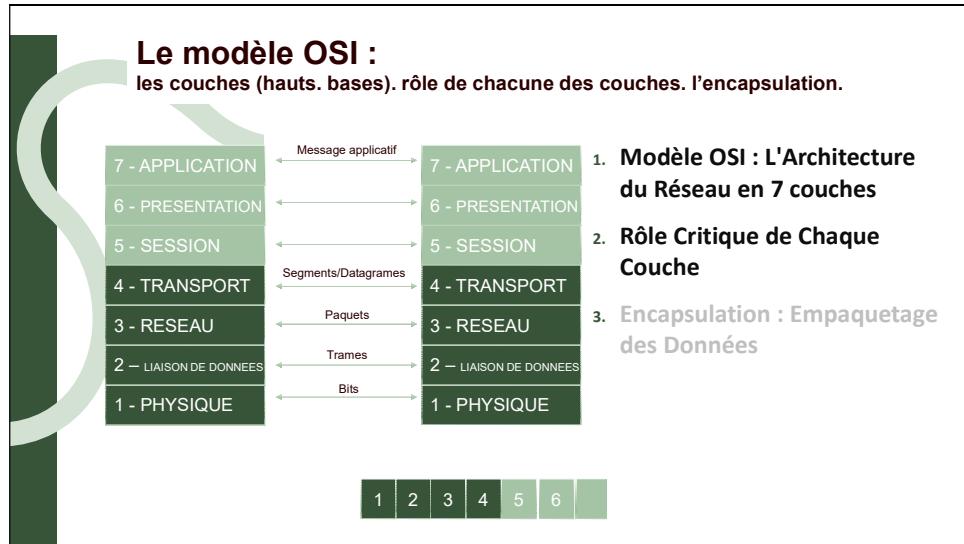
- **Unicast** est préféré pour les communications directes et confidentielles.
- **Multicast** réduit la charge sur la source et optimise l'utilisation de la bande passante pour les diffusions groupées.
- **Broadcast** est utile pour la configuration initiale des réseaux ou pour les annonces globales.
- **Anycast** améliore la répartition de charge et la résilience en dirigeant les requêtes vers le serveur le plus proche ou le plus performant.

**Conclusion**

La sélection du mode de communication adapté est cruciale pour répondre aux exigences spécifiques des applications réseau. En associant judicieusement unicast, multicast, broadcast et anycast à leurs cas d'usage, les professionnels du réseau peuvent optimiser la performance, la sécurité et l'efficacité des systèmes qu'ils administrent.



- Les protocoles réseau sont essentiellement des règles et des conventions qui dictent la manière dont les données sont échangées entre les appareils sur un réseau. Ils déterminent la façon dont les appareils communiquent. Il existe deux types principaux de protocoles : les protocoles connectés et les protocoles non-connectés
- **Protocoles Connectés :**
- **Fiabilité** : Ces protocoles garantissent la fiabilité des données en s'assurant que toutes les informations sont transmises sans perte ni altération.
- **Contrôle de Flux** : Ils gèrent le débit de données pour éviter la congestion du réseau.
- **Ordre de Transmission** : Ils maintiennent l'ordre des paquets de données pour une reconstruction précise de l'information.
- **Applications** : Ils sont adaptés aux applications où la perte de données ou les erreurs de transmission sont critiques. comme le transfert de fichiers. la navigation web. etc.
- **Protocoles Non-connectés :**
- **Latence minimale** : Ces protocoles visent à minimiser la latence en ne nécessitant pas de connexion continue.
- **Moins de surcharge réseau** : Ils n'impliquent pas l'établissement et le maintien d'une connexion. ce qui réduit la charge sur le réseau.
- **Applications** : Ils conviennent aux applications où une latence minimale est plus importante que la fiabilité. comme la diffusion en continu de médias. les jeux en ligne. la surveillance réseau. etc.



## Le Modèle OSI : Fondamentaux de la Communication Réseau

Le modèle Open Systems Interconnection (OSI) est un cadre conceptuel utilisé pour comprendre les interactions complexes au sein des réseaux informatiques. Divisé en sept couches, il décrit les différentes étapes que les données traversent, de l'application de l'utilisateur jusqu'au matériel réseau, et vice versa.

### Exploration des Sept Couches

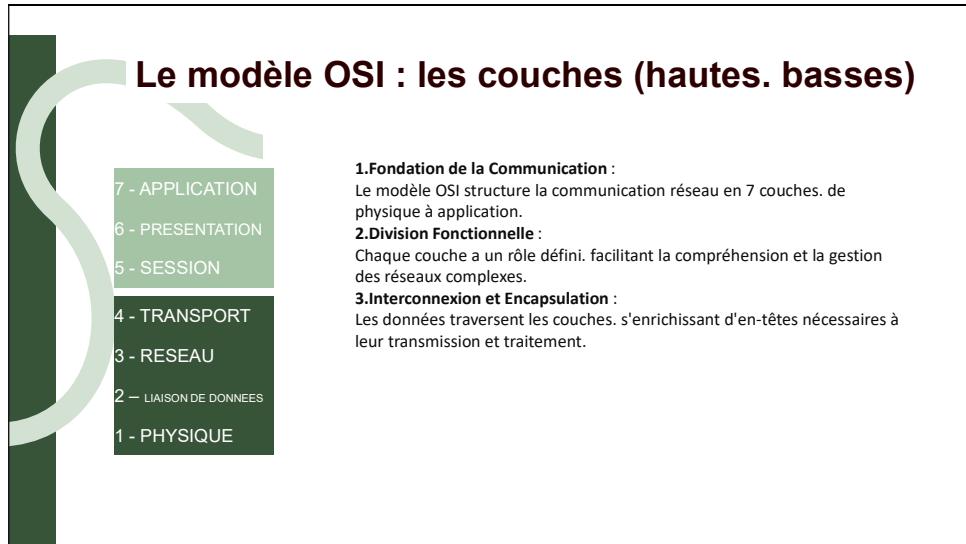
- **Couche Physique (1)** : La fondation du modèle OSI, responsable de la transmission brute des données sur le média physique, comme les câbles ou les ondes radio.
- **Couche de Liaison de Données (2)** : Gère la connexion entre les dispositifs sur le même réseau local (LAN), traitant les adresses physiques (MAC) et les erreurs de transmission.
- **Couche Réseau (3)** : Se concentre sur le routage des paquets à travers différents réseaux, utilisant des adresses logiques (IP) pour trouver le meilleur chemin.
- **Couche Transport (4)** : Assure la livraison fiable et dans le bon ordre des données entre les applications, en gérant le contrôle de flux et la correction d'erreurs.
- **Couche Session (5)** : Permet l'établissement, la gestion et la terminaison des sessions entre applications, facilitant l'échange de données.
- **Couche Présentation (6)** : Traduit les données entre les formats réseau et application, gérant l'encryption et la compression des données.
- **Couche Application (7)** : L'interface avec laquelle les applications logicielles interagissent avec le réseau, fournissant des services réseau spécifiques comme le courrier électronique et le transfert de fichiers.

### Le Processus d'Encapsulation

L'encapsulation est un processus clé dans la communication réseau, où les données sont empaquetées à chaque couche du modèle OSI avec les informations nécessaires à leur transmission et leur traitement. En descendant les couches, chaque couche enveloppe les données de la couche précédente avec un en-tête contenant des informations spécifiques à sa fonction. Ce processus garantit que les données peuvent être transmises efficacement sur le réseau et correctement interprétées à leur destination.

### Conclusion

Le modèle OSI et le processus d'encapsulation sont fondamentaux pour comprendre comment les données sont transmises à travers les réseaux informatiques. En décomposant la communication réseau en couches distinctes avec des fonctions spécifiques, le modèle OSI fournit un cadre permettant de diagnostiquer et résoudre les problèmes réseau, ainsi que de concevoir et implémenter de nouvelles technologies réseau.



## Le modèle OSI : les couches (hautes. basses)

1. **Fondation de la Communication :**  
Le modèle OSI structure la communication réseau en 7 couches. de physique à application.
2. **Division Fonctionnelle :**  
Chaque couche a un rôle défini. facilitant la compréhension et la gestion des réseaux complexes.
3. **Interconnexion et Encapsulation :**  
Les données traversent les couches. s'enrichissant d'en-têtes nécessaires à leur transmission et traitement.

### Le Modèle OSI : Exploration des Couches Hautes et Basses

Le modèle Open Systems Interconnection (OSI) est un cadre conceptuel qui décrit les fonctions de communication réseau en sept couches distinctes. Chaque couche du modèle OSI sert un but spécifique. facilitant la modularité et le diagnostic des problèmes de réseau. En divisant la communication réseau en ces couches. le modèle OSI aide à standardiser les interactions entre les logiciels et le matériel réseau. permettant leur interopérabilité.

#### Couches Basses : Les Fondations de la Communication

Les couches basses du modèle OSI concernent principalement les aspects physiques et la transmission des données :

- **Couche 1 - Physique** : Gère la transmission brute des données sur le support physique. qu'il s'agisse de câbles. de fibres optiques ou de signaux sans fil. Cette couche s'occupe des aspects comme les voltages. la modulation et la connectivité physique.
- **Couche 2 - Liaison de Données** : Assure une transmission de données fiable entre deux appareils directement connectés. Elle s'occupe de l'adressage physique (MAC). de la détection et de la correction d'erreurs qui peuvent survenir au niveau physique.
- **Couche 3 - Réseau** : Responsable du routage des paquets à travers différents réseaux et de la gestion de l'adressage logique (comme les adresses IP). Cette couche détermine le chemin optimal que les données doivent emprunter pour atteindre leur destination.

#### Couches Hautes : Vers l'Utilisateur

Les couches hautes traitent des aspects de la communication plus proches de l'utilisateur final et des applications :

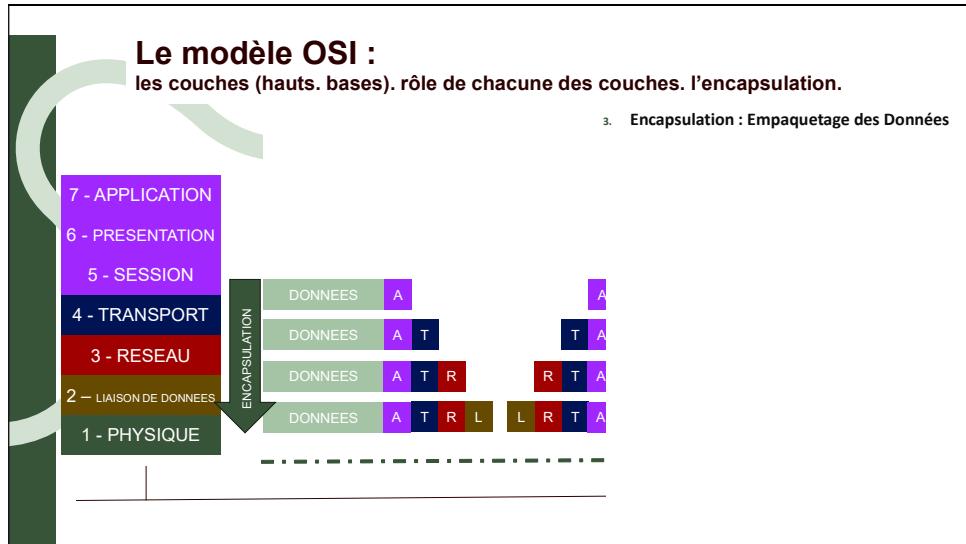
- **Couche 4 - Transport** : Fournit une transmission de données fiable. orientée connexion ou non. entre deux points terminaux. Elle gère le contrôle de flux. la correction d'erreurs et la retransmission.
- **Couche 5 - Session** : Permet l'établissement. la gestion et la terminaison de sessions entre applications. Cette couche gère les dialogues et les synchronisations entre les applications.
- **Couche 6 - Présentation** : Traduit les données entre le format du réseau et le format que l'application peut comprendre. Elle s'occupe de l'encryption. la compression et la conversion de données.
- **Couche 7 - Application** : L'interface avec laquelle les applications accèdent aux services de réseau. Cette couche fournit des services réseau aux applications de l'utilisateur. comme le transfert de fichiers. la messagerie électronique et d'autres services de réseau.

**Encapsulation et Interconnexion**

Au cœur du modèle OSI se trouve le processus d'encapsulation. Les données de l'utilisateur sont emballées à chaque couche avec des en-têtes pertinents avant d'être transmises à travers le réseau. puis déballées à la destination. Ce processus permet une gestion efficace et sécurisée des données à travers les diverses couches de communication.

**Conclusion**

Le modèle OSI demeure un outil essentiel pour comprendre et enseigner les concepts de réseau. En décomposant la communication en couches distinctes. avec des fonctions clairement définies. le modèle OSI offre une vue d'ensemble de la manière dont les réseaux fonctionnent et interagissent. facilitant la résolution de problèmes. la conception de réseaux et le développement de nouvelles technologies.



### Le Processus d'Encapsulation

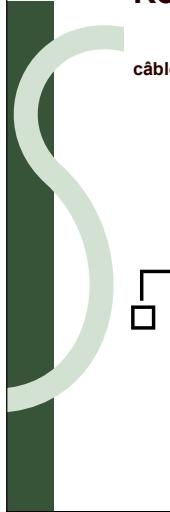
L'encapsulation est un processus clé dans la communication réseau, où les données sont empaquetées à chaque couche du modèle OSI avec les informations nécessaires à leur transmission et leur traitement. En descendant les couches, chaque couche enveloppe les données de la couche précédente avec un en-tête contenant des informations spécifiques à sa fonction. Ce processus garantit que les données peuvent être transmises efficacement sur le réseau et correctement interprétées à leur destination.

### Conclusion

Le modèle OSI et le processus d'encapsulation sont fondamentaux pour comprendre comment les données sont transmises à travers les réseaux informatiques. En décomposant la communication réseau en couches distinctes avec des fonctions spécifiques, le modèle OSI fournit un cadre permettant de diagnostiquer et résoudre les problèmes réseau, ainsi que de concevoir et implémenter de nouvelles technologies réseau.

### Rôle des composants d'un réseau (et leur logo) :

câbles. cartes réseau (connecteurs. débit des interfaces). switch. accès point. routeur. firewall



**1. Composants Clés du Réseau**

**1. Infrastructure du Réseau :**  
Comprendre le rôle des câbles. cartes réseau. switchs. points d'accès. routeurs et firewalls dans l'architecture réseau.

**2. Connectivité et Communication :**  
Chaque composant contribue à la performance. la sécurité et la fiabilité du réseau.

**3. Spécificités Techniques :**  
Les caractéristiques comme les types de connecteurs et les débits des interfaces sont clés pour optimiser l'infrastructure réseau.

### Rôle des Composants dans un Réseau

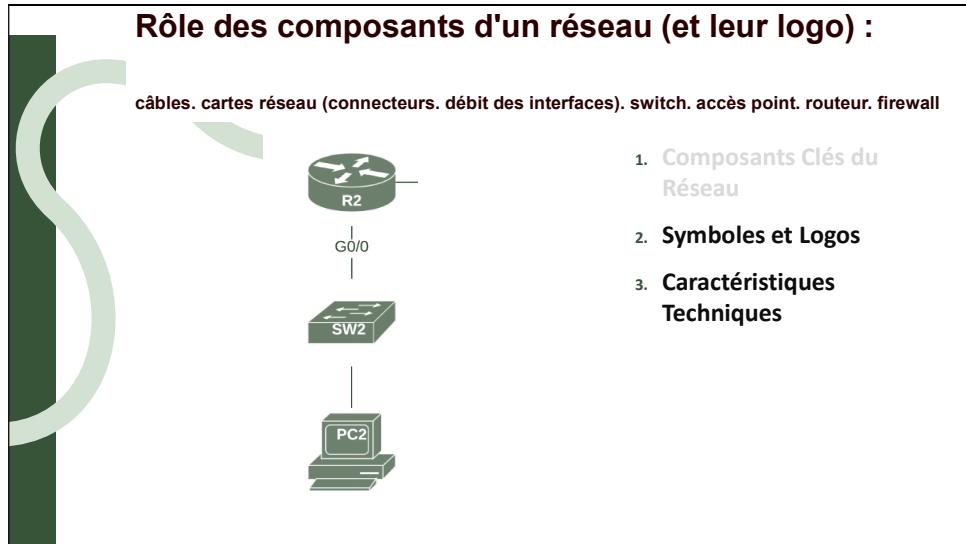
La construction et le maintien d'un réseau informatique impliquent une variété de composants physiques. chacun jouant un rôle crucial dans la facilitation de la communication et le transfert de données. La compréhension de ces éléments et de leurs fonctions spécifiques est essentielle pour tout professionnel des réseaux.

#### Comprendre les Composants de Base

- Câbles et Connecteurs** : Les câbles sont les artères d'un réseau. transportant les signaux entre les dispositifs. Selon l'environnement. vous pourriez utiliser du câblage en cuivre (ex. Cat5e. Cat6 pour Ethernet) ou de la fibre optique pour des connexions à longue distance et haute vitesse. Les connecteurs (comme RJ45 pour Ethernet ou LC pour la fibre optique) jouent également un rôle crucial dans la connexion physique des dispositifs.
- Cartes Réseau** : Elles permettent aux ordinateurs et autres appareils de se connecter au réseau. Les caractéristiques importantes incluent le type de connecteur et le débit de l'interface. qui peut varier de 10/100/1000 Mbps pour Ethernet à beaucoup plus pour les connexions fibre.
- Switchs** : Ces dispositifs opèrent principalement à la couche de liaison de données (couche 2) du modèle OSI. dirigeant les données entre les appareils sur un LAN. Ils jouent un rôle vital dans la gestion du trafic et la prévention des congestions sur le réseau.
- Points d'Accès** : Les points d'accès étendent la connectivité réseau aux appareils sans fil. agissant comme des ponts entre le réseau câblé et les utilisateurs sans fil.
- Routeurs** : Fonctionnant à la couche réseau (couche 3). les routeurs connectent différents segments de réseau et dirigent le trafic entre eux. Ils utilisent des adresses IP pour déterminer le meilleur chemin pour les données à travers un réseau étendu (WAN).
- Firewalls** : Les firewalls surveillent et contrôlent l'entrée et la sortie du trafic réseau basé sur un ensemble de règles de sécurité. Ils sont essentiels pour protéger le réseau contre les accès non autorisés et les cyberattaques.

#### Conclusion

Les composants d'un réseau travaillent ensemble pour créer une infrastructure solide et sécurisée. capable de supporter les communications et les échanges de données. Chaque élément. des câbles et cartes réseau aux switchs. points d'accès. routeurs et firewalls. est vital pour le fonctionnement efficace et sécurisé d'un réseau. La sélection appropriée et la configuration de ces composants sont cruciales pour atteindre les performances désirées et maintenir la sécurité et la fiabilité du réseau.



## Manuel pour les Stagiaires

### Symboles et Logos

Chaque composant réseau est souvent représenté dans les schémas de réseau par des symboles ou logos standardisés. facilitant leur identification et la compréhension des architectures réseau. Par exemple. un switch peut être représenté par un symbole ressemblant à un éventail de lignes convergeant en un point. tandis qu'un point d'accès peut être symbolisé par des ondes radio émanant d'un point central.

### Conclusion

La connaissance des composants d'un réseau. de leurs rôles spécifiques. de leurs caractéristiques techniques. et de leur représentation symbolique est fondamentale pour concevoir. construire et maintenir des réseaux efficaces et sécurisés. Cette compréhension permet non seulement d'optimiser les performances et la fiabilité des réseaux mais aussi de faciliter le dépannage et l'amélioration continue des infrastructures réseau.

• Ateliers



**ATELIER 1**

**Activité**



— **Objectifs :**

- ▶ Réaliser une première utilisation de la commande « ping » en testant la présence d'une machine sur le réseau

— **Enoncé : voir livret d'ateliers**



**ATELIER 2**

**Activité**



— **Objectifs :**

- ▶ Situer une machine distante dans un réseau.
- ▶ Visualiser le chemin emprunté par les paquets.
- ▶ Savoir interpréter le résultat de la commande (perte de paquet, goulot d'étranglement, présence d'un firewall).

— **Enoncé : voir livret d'ateliers**

- Ce qu'il faut retenir



1. **La Fondation des Réseaux**
2. **Interconnexion Mondiale**
3. **Avancées Technologiques**
4. **Compréhension du Modèle OSI**
5. **Importance des Standards et Protocoles**

**La Fondation des Réseaux :** Comprendre les principes de base et l'évolution des réseaux est essentiel pour saisir comment les technologies de communication ont façonné notre monde connecté.

**Interconnexion Mondiale :** Les réseaux permettent de connecter des individus et des dispositifs à travers le globe, facilitant le partage d'informations et la collaboration sans précédent entre les personnes.

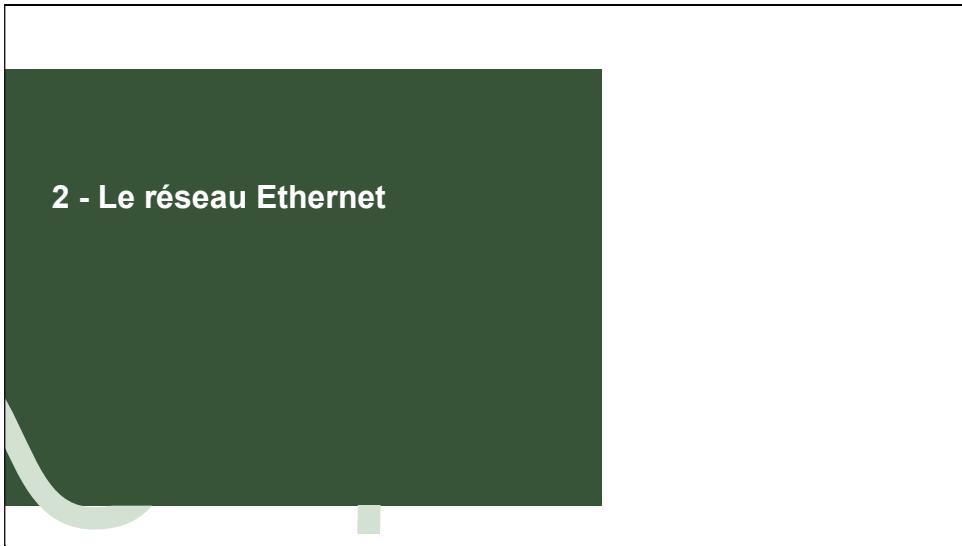
**Avancées Technologiques :** L'histoire des réseaux est marquée par des innovations continues qui ont amélioré la vitesse, la sécurité et la capacité des connexions, permettant l'émergence de nouvelles applications et services.

**Compréhension du Modèle OSI :** Le modèle OSI décompose la communication réseau en sept couches distinctes, offrant un cadre pour comprendre et résoudre les problèmes de réseau.

**Importance des Standards et Protocoles :** Les standards et protocoles définis par des organismes tels que l'IEEE, OSI, UIT et IETF assurent l'interopérabilité et la fiabilité des communications sur les réseaux.

Ces messages clés fournissent une synthèse du chapitre, soulignant l'importance de la connectivité réseau dans le monde moderne, les progrès technologiques qui ont permis cette connectivité, et l'importance des cadres et standards qui régissent le fonctionnement des réseaux.

## Chapitre 2 – Le réseau Ethernet



- Objectifs du chapitre

## Plan de la formation

- 1 - Pourquoi un réseau ?
- 2 - Le réseau Ethernet
- 3 - Commutation Ethernet ou "switching"
- 4 - WiFi
- 5 - TCP/IP
- 6 - DHCP et DNS
- 7 - Administration et SNMP

- Com
- Maîtr
- Ethe
- Com
- Com
- Déco
- App
- Impl
- Envi

Le chapitre sur le réseau Ethernet constitue le cœur technique de notre formation. Après avoir posé les bases théoriques des réseaux. nous allons maintenant plonger dans les détails spécifiques de la technologie Ethernet. qui est l'épine dorsale de la plupart des réseaux locaux (LAN). Pour préparer les participants à cette session. voici quelques lignes directrices :

**Transition et Cohérence :**

Faites le lien avec le chapitre précédent en montrant comment les fondamentaux des réseaux préparent à une compréhension plus approfondie des réseaux Ethernet.

Soulignez que ce chapitre est un pont entre la théorie générale des réseaux et des modules plus avancés. qui s'appuieront sur ces connaissances pour explorer des concepts de réseau plus complexes.

**Engagement des Apprenants :**

Encouragez les questions et la participation active tout au long de la session pour garantir la compréhension et l'engagement.

Prévoyez des activités interactives ou des études de cas qui permettront aux participants de mettre en pratique les concepts abordés.

Les objectifs pédagogiques du chapitre 2. axé sur le "réseau Ethernet". pourraient inclure :

**•Comprendre les Fondamentaux d'Ethernet :**

- Expliquer ce qu'est Ethernet et son rôle comme technologie de réseau local (LAN) la plus répandue.
- Identifier les caractéristiques clés d'Ethernet. y compris ses méthodes d'accès au média et son évolution au fil du temps.

**•Maîtriser les Concepts de Base du Réseau Ethernet :**

- Distinguer les différentes versions d'Ethernet. notamment Fast Ethernet. Gigabit Ethernet. et 10 Gigabit Ethernet. et leurs domaines d'application.
- Décrire les types de câblage utilisés dans les réseaux Ethernet (par exemple. câblage en cuivre vs. fibre optique) et les normes associées.

**•Comprendre le Fonctionnement des Commutateurs Ethernet (Switches) :**

- Expliquer comment les switches Ethernet améliorent les performances du réseau en réduisant les collisions et en segmentant le trafic.
- Identifier les fonctions avancées des switches, comme le VLAN (Virtual Local Area Network) et la QoS (Quality of Service).

**•Découvrir les Protocoles et Standards Ethernet :**

- Se familiariser avec les protocoles et les standards qui régissent les réseaux Ethernet, y compris IEEE 802.3.
- Comprendre l'importance des normes dans l'assurance de l'interopérabilité et la fiabilité des connexions réseau.

**•Appréhender les Applications et les Implications d'Ethernet dans les Environnements Réseaux Actuels :**

- Reconnaître comment Ethernet s'adapte aux besoins des réseaux modernes, y compris dans les contextes de data centers et de cloud computing.
- Évaluer l'impact de l'évolution d'Ethernet sur la planification et la gestion des infrastructures réseau.

Ces objectifs visent à offrir une compréhension complète d'Ethernet en tant que technologie fondamentale dans les réseaux d'entreprise et personnels, couvrant à la fois les principes théoriques et les aspects pratiques de sa mise en œuvre et de sa gestion.



- **Performance et Agilité des Connexions :**  
"Avez-vous déjà remarqué une différence de vitesse ou de stabilité entre une connexion sans fil et une connexion filaire ? Dans quel contexte la performance est-elle particulièrement importante pour vous ?"
- **Organisation et Structure du Travail :**  
"Comment l'organisation de votre espace de travail ou de votre environnement domestique pourrait-elle être influencée par la nécessité d'une connexion réseau filaire ?"
- **Expérience avec le Matériel de Réseau :**  
"Quelle a été votre expérience avec le matériel physique de réseau, comme les câbles ou les switchs, même si ce n'était que pour brancher un ordinateur ou un appareil similaire ?"
- **Sécurité et Fiabilité des Connexions :**  
"Dans quelles situations estimatez-vous qu'une connexion filaire pourrait être plus sécurisée ou fiable qu'une connexion sans fil ? Pourquoi ?"
- **Dépannage des Connexions Réseau :**  
"Si vous avez déjà eu à résoudre un problème de connexion à Internet, quels éléments avez-vous considérés ou vérifié en premier lieu ?"

**Performance et Agilité des Connexions :**

"Avez-vous déjà remarqué une différence de vitesse ou de stabilité entre une connexion sans fil et une connexion filaire ? Dans quel contexte la performance est-elle particulièrement importante pour vous ?"

**Organisation et Structure du Travail :**

"Comment l'organisation de votre espace de travail ou de votre environnement domestique pourrait-elle être influencée par la nécessité d'une connexion réseau filaire ?"

**Expérience avec le Matériel de Réseau :**

"Quelle a été votre expérience avec le matériel physique de réseau, comme les câbles ou les switchs, même si ce n'était que pour brancher un ordinateur ou un appareil similaire ?"

**Sécurité et Fiabilité des Connexions :**

"Dans quelles situations estimatez-vous qu'une connexion filaire pourrait être plus sécurisée ou fiable qu'une connexion sans fil ? Pourquoi ?"

**Dépannage des Connexions Réseau :**

"Si vous avez déjà eu à résoudre un problème de connexion à Internet, quels éléments avez-vous considérés ou vérifié en premier lieu ?"

## Présentation

### 1. Piliers des Réseaux Modernes :

Ethernet. fondation de l'infrastructure réseau. adapté aux besoins changeants de la communication.

### 2. Caractéristiques Clés :

Fiabilité. vitesse. et simplicité définissent Ethernet. facilitant la connectivité dans divers environnements.

### 3. Évolution Continue :

Depuis son introduction. Ethernet a évolué. soutenant l'expansion des réseaux d'entreprise et personnels.



Collision

## Introduction au Réseau Ethernet

### Contextualisation et Importance du Réseau Ethernet

Depuis sa création dans les années 1970 par Robert Metcalfe et son équipe chez Xerox PARC. la technologie Ethernet s'est imposée comme la colonne vertébrale des réseaux informatiques à travers le monde. Initialement conçu pour relier quelques ordinateurs sur de courtes distances. Ethernet est devenu le standard dominant pour les réseaux locaux (LAN) et a évolué pour répondre aux besoins croissants en matière de vitesse. de sécurité et de fiabilité des infrastructures de réseau modernes.

### Caractéristiques Fondamentales d'Ethernet

Ethernet se caractérise par sa simplicité. son efficacité et sa capacité d'adaptation. Voici quelques-unes de ses caractéristiques fondamentales :

• **Topologie de Réseau** : Ethernet permet une grande flexibilité dans la configuration des réseaux. avec des topologies en étoile. en bus ou en anneau. facilitant l'intégration et l'expansion des réseaux existants.

• **Méthode d'Accès** : Ethernet utilise une méthode d'accès au média appelée CSMA/CD (Carrier Sense Multiple Access with Collision Detection) pour les environnements filaires. permettant aux dispositifs de communiquer sur un même segment de réseau tout en minimisant les collisions de données.

• **Débits** : Au fil du temps. Ethernet a évolué de débits initiaux de 10 Mbps à des vitesses bien supérieures. avec des standards actuels supportant 10 Gbps. 40 Gbps. et même 100 Gbps. répondant ainsi aux exigences des applications de données intensives.

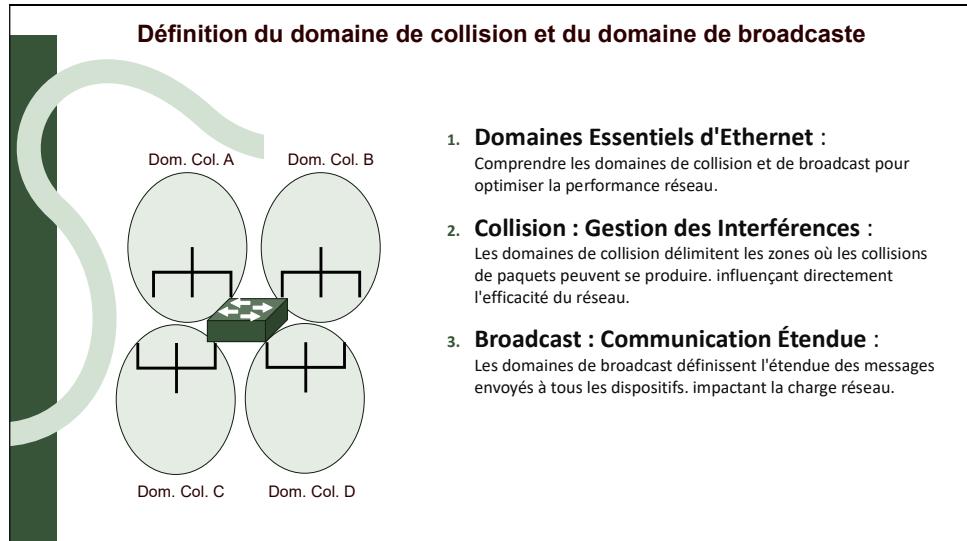
• **Support Physique** : Ethernet peut utiliser divers types de câbles. y compris coaxial. à paire torsadée (non blindée ou blindée). et la fibre optique. offrant ainsi une grande variété d'options pour différentes exigences de distance et de qualité de signal.

### Rôle d'Ethernet dans les Infrastructures Réseau Modernes

Ethernet joue un rôle crucial dans l'interconnexion des dispositifs informatiques. des serveurs. des dispositifs de stockage. et d'autres équipements réseau au sein des entreprises. des data centers. et des réseaux domestiques. Sa standardisation assure l'interopérabilité entre les équipements de différents fabricants. tandis que sa robustesse et sa fiabilité le rendent indispensable pour la mise en œuvre de solutions réseau critiques.

**Conclusion**

La technologie Ethernet constitue la fondation sur laquelle reposent les infrastructures de réseau modernes. Comprendre ses caractéristiques, son évolution et son application pratique est essentiel pour tout professionnel des réseaux. Ethernet continue d'évoluer, offrant des solutions innovantes pour répondre aux défis de la communication et de la connectivité dans le monde numérique d'aujourd'hui.



### Définition et Impact des Domaines de Collision et de Broadcast

Dans le contexte des réseaux Ethernet, comprendre les concepts de domaines de collision et de broadcast est crucial pour la conception et la gestion d'une infrastructure réseau performante.

#### Domaine de Collision : Principe et Gestion

Un domaine de collision est un segment de réseau où les trames envoyées par deux dispositifs ou plus peuvent entrer en collision, car ils partagent le même médium physique. Dans les réseaux Ethernet traditionnels utilisant un hub ou une topologie en bus, une collision se produit lorsque deux dispositifs tentent de communiquer simultanément, entraînant une interférence qui nécessite la retransmission des données.

• **Impact sur le Réseau :** Les collisions réduisent l'efficacité du réseau, car elles provoquent des retards et augmentent la charge sur le réseau en raison des retransmissions nécessaires. La gestion efficace des domaines de collision, notamment par l'utilisation de switchs et la segmentation du réseau, est essentielle pour minimiser ces interférences et améliorer la performance globale.

#### Domaine de Broadcast : Fonctionnement et Conséquences

Un domaine de broadcast représente la portée à l'intérieur de laquelle un message de broadcast envoyé par un dispositif sera reçu par tous les autres dispositifs du réseau. Les messages de broadcast sont utilisés pour diverses fonctions, telles que la résolution d'adresses ou les annonces de service.

• **Considérations de Performance :** Bien que nécessaires, les broadcasts peuvent surcharger le réseau, surtout dans les grands domaines de broadcast, car chaque dispositif doit traiter le message, même s'il n'est pas le destinataire final. La limitation de la taille des domaines de broadcast, par exemple à l'aide de VLANs, peut réduire cette charge et améliorer la performance du réseau.

### Conclusion

Les domaines de collision et de broadcast ont des implications significatives sur la performance et l'efficacité des réseaux Ethernet. Une compréhension approfondie de ces concepts permet aux professionnels des réseaux de concevoir des infrastructures plus robustes, sécurisées et efficaces, en minimisant les interférences et en optimisant la distribution des données. La gestion adéquate de ces domaines est essentielle pour répondre aux exigences croissantes des applications modernes en termes de bande passante et de fiabilité.

**Méthode d'accès CSMA/CD : impacte des collisions. éviter les collisions**

Hmmm.... J'ai besoin d'envoyer quelque chose. Est-ce que tout se passe bien sur le réseau ?

- CSMA/CD : Clé de l'Ethernet :**  
Comprendre CSMA/CD est essentiel pour gérer efficacement les réseaux Ethernet et minimiser les collisions.
- Impact des Collisions :**  
Les collisions réduisent la performance du réseau en nécessitant la retransmission des données, augmentant ainsi la latence et diminuant le débit.
- Prévention des Collisions :**  
Des stratégies efficaces, incluant la segmentation du réseau et l'usage de switchs modernes, peuvent considérablement réduire le risque de collisions.

## Méthode d'Accès CSMA/CD et Gestion des Collisions dans les Réseaux Ethernet

### Fonctionnement de CSMA/CD

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) est une méthode d'accès au média conçue pour minimiser les collisions de paquets sur les réseaux Ethernet. Le principe est relativement simple mais efficace : un dispositif vérifie d'abord si le média de transmission (le câble, par exemple) est libre avant d'envoyer des données. Si le média est occupé, le dispositif attend une période aléatoire avant de vérifier à nouveau. Si une collision est détectée après l'envoi des données, le dispositif cesse de transmettre, attend un intervalle de temps aléatoire, puis tente de retransmettre les données.

### Impact des Collisions sur le Réseau

Les collisions sont inévitables dans tout réseau partageant un médium commun, surtout dans les réseaux Ethernet traditionnels utilisant des hubs. Chaque collision nécessite la retransmission des données, ce qui peut conduire à une congestion du réseau, augmenter la latence et réduire le débit global. Dans les environnements à fort trafic, l'impact des collisions peut devenir significatif, affectant négativement la performance du réseau.

### Stratégies pour Éviter les Collisions

- Utilisation de Switchs** : Remplacer les hubs par des switchs peut éliminer les collisions sur les réseaux Ethernet. Les switchs créent des domaines de collision séparés pour chaque port, isolant ainsi les dispositifs et réduisant les chances de collision.
- Segmentation du Réseau** : Diviser un grand réseau en segments plus petits (sous-réseaux ou VLANs) limite la taille des domaines de broadcast et de collision, réduisant ainsi le nombre potentiel de dispositifs impliqués dans une collision.

### Conclusion

La compréhension et l'application efficaces de la méthode d'accès CSMA/CD sont cruciales pour le diagnostic, la gestion et l'optimisation des réseaux Ethernet. Bien que la technologie Ethernet ait évolué et que l'utilisation de switchs ait réduit l'importance des collisions dans les réseaux modernes, la connaissance de CSMA/CD reste essentielle pour tout professionnel des réseaux. Elle souligne l'importance de concevoir des réseaux qui non seulement minimisent les collisions mais sont également résilients, performants et adaptés aux besoins actuels de communication et de connectivité.

## Adressage MAC : Compréhension et Application

## Structure et Rôle de l'Adresse MAC

L'adresse MAC (Media Access Control) est une adresse physique unique attribuée à chaque interface réseau par son fabricant. Cette adresse de 48 bits, représentée en notation hexadécimale (par exemple, 00:1A:2B:3C:4D:5E), joue un rôle crucial dans le processus de communication au sein des réseaux locaux (LANs), notamment Ethernet.

La structure de l'adresse MAC se divise en deux parties principales :

- **Identifiant du Fabricant** : Les 24 premiers bits, également connus sous le nom d'oui (Organizationally Unique Identifier), identifient le fabricant du dispositif.
  - **Numéro de Série** : Les 24 bits restants servent de numéro de série ou d'identifiant unique attribué par le fabricant, garantissant l'unicité de chaque adresse MAC au sein d'un réseau.

## Cas de Modification d'une Adresse MAC

Bien que chaque dispositif réseau possède une adresse MAC unique attribuée en usine, il existe des situations où modifier cette adresse peut s'avérer nécessaire ou utile :

- **Politiques de Sécurité** : Pour se protéger contre le suivi ou l'identification non autorisée, les utilisateurs peuvent modifier l'adresse MAC de leurs dispositifs.
  - **Contrôle d'Accès au Réseau** : Certains réseaux limitent l'accès aux dispositifs autorisés via leur adresse MAC. Modifier l'adresse MAC peut permettre à un dispositif de contourner ces restrictions.
  - **Tests de Réseau** : Les administrateurs réseau peuvent modifier les adresses MAC pour tester la réponse du réseau à différents scénarios, comme les changements d'équipement ou la simulation de dispositifs supplémentaires.
  - **Remplacement de Matériel Défectueux** : Si un composant réseau est remplacé, la modification de l'adresse MAC peut être nécessaire pour maintenir les configurations réseau existantes, notamment dans les systèmes où les permissions et les configurations sont liées à l'adresse MAC spécifique d'un dispositif.

**Considérations Importantes**

Il est crucial de noter que, bien que la modification d'une adresse MAC puisse être utile dans certaines circonstances, elle doit être effectuée avec prudence et dans le respect des politiques réseau et des considérations légales. La "spoofing" d'adresse MAC peut entraîner des conflits réseau, des problèmes de sécurité et des violations de politique réseau.

**Conclusion**

La compréhension de l'adresse MAC et de sa structure est fondamentale pour quiconque travaille avec des réseaux Ethernet. Reconnaître quand et pourquoi modifier une adresse MAC peut aider dans des situations de réseau complexes.

## Démonstration



– Objectifs :  
Montrer la possibilité de  
changer l'adresse mac  
sur un PC windows  
(évoquer les impacts)

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

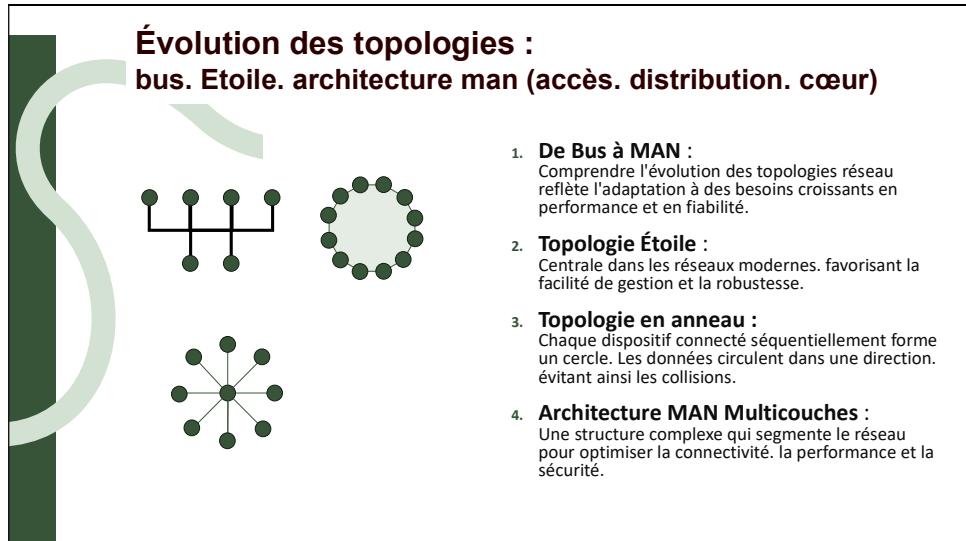
---

---

---

---

---



## Évolution des Topologies Réseau : Du Bus à l'Architecture MAN

L'architecture des réseaux a considérablement évolué depuis les premières implémentations, s'adaptant aux besoins changeants des utilisateurs et des organisations. Comprendre cette évolution aide à saisir les principes sous-jacents de la conception de réseau et à choisir la meilleure configuration pour une application donnée.

### Topologie Bus

La topologie en bus, l'une des plus anciennes formes d'architecture réseau, connecte tous les dispositifs sur un seul câble (le bus). Tous les signaux passent par ce câble, et chaque dispositif écoute pour détecter les messages qui lui sont destinés. Bien que simple et économique, la topologie en bus présente des inconvénients significatifs, notamment en termes de collisions de données et de difficultés de dépannage.

### Topologie Étoile

L'évolution vers la topologie en étoile a répondu à plusieurs limitations de la topologie en bus. Dans une topologie étoile, chaque dispositif est connecté à un point central, comme un switch ou un hub. Cette configuration simplifie le câblage, améliore la gestion du réseau et renforce la fiabilité, car une défaillance sur un seul câble n'affecte que le dispositif connecté à ce câble, sans impacter les autres.

### Topologie en Anneau : Compréhension Approfondie

La topologie en anneau est un arrangement de réseau dans lequel chaque dispositif est connecté à deux autres dispositifs, formant un circuit fermé ou un anneau. Cette configuration permet aux données de circuler dans une direction prédéfinie (soit dans le sens des aiguilles d'une montre, soit dans le sens inverse), de nœud en nœud jusqu'à atteindre leur destination.

### **Architecture MAN Multicouches**

Les réseaux à grande échelle, tels que les réseaux métropolitains (MAN), adoptent une architecture multicouche complexe, typiquement divisée en couches d'accès, de distribution et de cœur.

•**Couche d'Accès** : La première étape de connexion pour les dispositifs utilisateurs au réseau. Elle permet l'accès aux ressources de communication.

•**Couche de Distribution** : Agit comme un intermédiaire entre la couche d'accès et la couche de cœur, acheminant le trafic de manière efficace et appliquant des politiques de réseau.

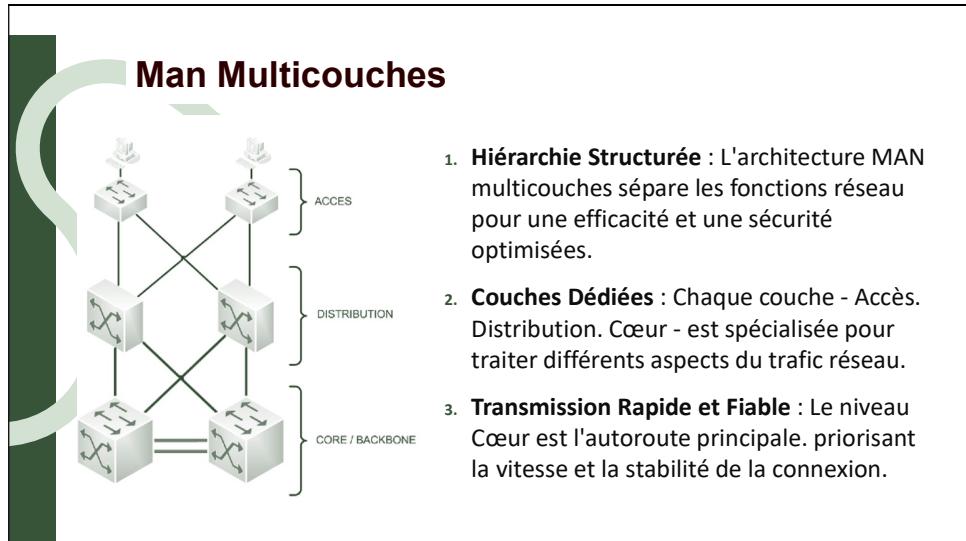
•**Couche de Cœur** : Le cœur du réseau, assurant une haute capacité de transport entre différentes zones du réseau. Elle est conçue pour maximiser la fiabilité et la performance.

### **Applications et Configurations Spécifiques**

Chaque topologie et architecture réseau a des applications et des configurations spécifiques pour lesquelles elle est la mieux adaptée. La topologie en bus peut encore être trouvée dans certains environnements industriels, tandis que l'étoile est prédominante dans les réseaux d'entreprise et domestiques. L'architecture MAN multicouches est utilisée pour les réseaux de grande taille nécessitant une hiérarchie claire pour gérer efficacement le trafic et assurer la qualité de service (QoS).

### **Conclusion**

L'évolution des topologies réseau de la simple topologie en bus à des architectures en étoile et MAN multicouches illustre la recherche constante d'efficacité, de performance et de fiabilité dans la conception des réseaux. Choisir la topologie appropriée nécessite une compréhension des avantages et des inconvénients de chaque option, ainsi qu'une analyse des besoins spécifiques du réseau en question.



## Architecture MAN Multicouches : Compréhension et Applications

### Principes de l'Architecture MAN Multicouches

L'architecture de réseau métropolitain (MAN) multicouches représente une approche structurée pour organiser et gérer les réseaux étendus sur une zone métropolitaine. Cette architecture est divisée en trois niveaux hiérarchiques. chacun ayant un ensemble de fonctions spécifiques :

- **Couche d'Accès (Access Layer)** : Ce niveau est le point d'entrée pour les utilisateurs et leurs dispositifs dans le réseau. Il permet la connexion des ordinateurs, des serveurs, et des téléphones IP, fournissant un accès direct aux ressources réseau. La couche d'accès est également le terrain où les politiques de réseau, telles que les VLANs, sont mises en œuvre pour organiser et contrôler le trafic utilisateur.
- **Couche de Distribution (Distribution Layer)** : Servant de médiateur entre les couches d'accès et de cœur, la couche de distribution gère le routage, le filtrage des paquets, la qualité de service (QoS) et les mesures de sécurité. Elle dirige le trafic réseau, applique des politiques de sécurité et prend des décisions de routage qui affectent la performance globale du réseau.
- **Couche Cœur (Core Layer)** : Le niveau cœur, également connu sous le nom de backbone, est conçu pour transporter rapidement les données à travers le réseau. Sa fonction principale est d'offrir une transmission efficace et fiable des données sur de longues distances avec une latence minimale. Ce niveau utilise des dispositifs réseau à haute performance pour gérer des volumes de trafic importants et fournir une connectivité entre les couches de distribution.

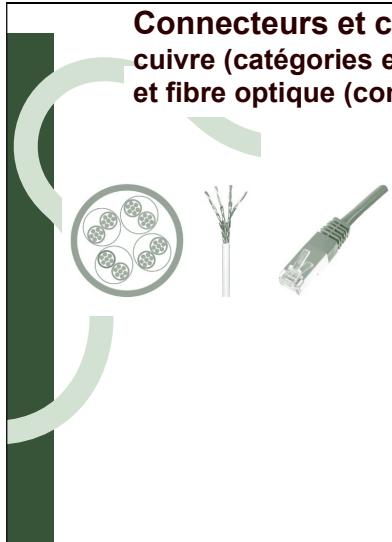
### Applications et Configurations Spécifiques

Dans une architecture MAN multicouches, chaque niveau est optimisé pour des performances spécifiques :

- La **couche d'Accès** est souvent composée de switchs et de points d'accès qui connectent directement les dispositifs des utilisateurs.
- La **couche de Distribution** peut inclure des switchs multicouches et des routeurs qui appliquent des politiques de réseau et facilitent le trafic entre les sous-réseaux.
- La **couche Cœur** se compose de routeurs et de switchs à haute capacité pour gérer le trafic de données à grande vitesse à travers le réseau étendu.

**Conclusion**

L'architecture MAN multicouches est fondamentale pour les réseaux étendus qui nécessitent un contrôle minutieux du trafic, une haute disponibilité, et une sécurité renforcée. La distinction claire entre les niveaux d'accès, de distribution et de cœur permet aux administrateurs de réseaux de concevoir des infrastructures capables de gérer le trafic efficacement, tout en maintenant une qualité de service élevée et en assurant la sécurité des données transmises.



**Connecteurs et câblage :**  
**cuivre (catégories et standard de câblage)**  
**et fibre optique (connecteurs, les fibre OSM, OM)**

1. **Câblage Réseau : Fondation de la Connectivité :**  
Comprendre les types de câbles et catégories pour optimiser la performance réseau.
2. **Cuivre vs. Fibre :**  
Identifier les avantages et applications spécifiques du câblage en cuivre et de la fibre optique dans les infrastructures réseau.
3. **Standards et Connecteurs :**  
Chaque type de câble a des standards définis et des connecteurs spécifiques, cruciaux pour une installation réussie et performante.

### Connecteurs et Câblage dans les Réseaux Ethernet : Comprendre les Options

La sélection du câblage approprié est cruciale pour la performance, la fiabilité et l'évolutivité des réseaux Ethernet. Les deux principaux types de câbles - cuivre et fibre optique - offrent différentes caractéristiques et sont adaptés à divers besoins et environnements réseau.

#### Câblage en Cuivre

Les câbles en cuivre sont largement utilisés dans les réseaux Ethernet pour les connexions LAN grâce à leur coût relativement faible et leur facilité d'installation. Ils se déclinent en plusieurs catégories, chacune offrant des niveaux de performance différents :

- **Catégorie 5e (Cat5e)** : Supporte des débits jusqu'à 1 Gbps sur des longueurs jusqu'à 100 mètres.
- **Catégorie 6 (Cat6)** : Conçu pour des débits jusqu'à 10 Gbps sur des distances jusqu'à 55 mètres dans des conditions de crosstalk élevé.
- **Catégorie 6a (Cat6a)** et supérieures : Supportent des débits de 10 Gbps sur 100 mètres et sont adaptées aux environnements à haute performance.

Les connecteurs RJ45 sont le standard pour les câbles en cuivre Ethernet, assurant une compatibilité universelle entre les équipements.

#### Fibre Optique

La fibre optique, transportant des données sous forme de lumière, offre des vitesses et des distances supérieures par rapport au cuivre, en plus d'être immunisée contre les interférences électromagnétiques. Il existe deux types principaux :

- **Fibre Monomode (OSM)** : Permet des transmissions sur de longues distances (jusqu'à plusieurs kilomètres) avec un seul mode de propagation de la lumière, idéale pour les backbones de réseau et les connexions WAN.
- **Fibre Multimode (OM)** : Utilisée pour des distances plus courtes, comme à l'intérieur d'un bâtiment ou entre des bâtiments proches, avec plusieurs modes de propagation de la lumière.

Les connecteurs pour la fibre optique varient, incluant les types SC, LC, et ST, chacun ayant des applications et une compatibilité spécifiques.

#### Conclusion

La sélection du type de câble et du connecteur approprié dépend de plusieurs facteurs, dont la distance de transmission, l'environnement du réseau, les besoins en bande passante et le budget. Comprendre les caractéristiques et les applications des différents types de câbles et connecteurs est essentiel pour concevoir et maintenir des réseaux Ethernet performants et fiables.

## Tableaux comparatif - Cuivre

Catégorie/Classe	Fréquence maximale	Débit maximal	Applications typiques
Catégorie 1	< 100 kHz	N/A	
Catégorie 2	1 MHz	4 Mbps	
Catégorie 3	16 MHz	16 Mbps	
Catégorie 4	20 MHz	20 Mbps	
Catégorie 5	100 MHz	100 Mbps	Voix analogique 10Base-T (Ethernet)
Catégorie 5e	100 MHz	1000 Mbps	10Base-T, 100Base-TX (Fast Ethernet)
Catégorie 6	250 MHz	1000 Mbps	Token Ring, 100Base-T4 (Fast Ethernet)
Catégorie 6A	500 MHz	10 Gbps	100Base-TX, 1000Base-T (Gigabit Ethernet)
Catégorie 7	600 MHz	10 Gbps	Gigabit Ethernet
Catégorie 7A	1000 MHz	10 Gbps	Gigabit Ethernet
Catégorie 8	2000 MHz	40 Gbps	10 Gigabit Ethernet
Catégorie 8.1	2000 MHz	40 Gbps	10 Gigabit Ethernet

## Dénomination Officielle actuelle : XX/YZZ

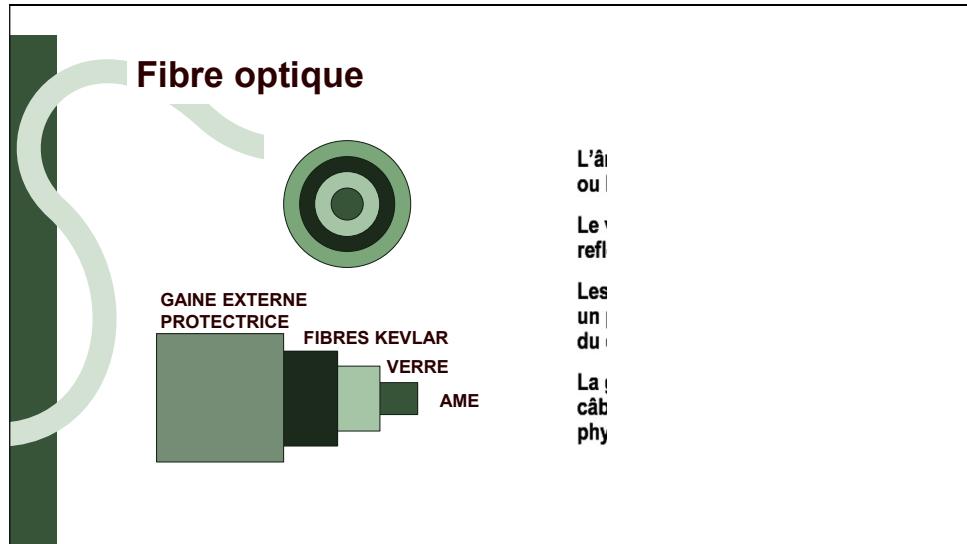
Dénomination officielle actuelle : XX / Y Z Z (voir exemple)

Blindage général

<b>U</b>	<i>Unshielded</i> Aucun blindage
<b>F</b>	<i>Foiled</i> Blindage écran
<b>S</b>	<i>Shielded</i> Blindage tresse
<b>SF</b>	Tresse + écran

Blindage par paire

<b>U</b>	<i>Unshielded</i> Aucun blindage
<b>F</b>	<i>Foiled</i> Blindage écran



- **Gaine externe protectrice** : La gaine externe est une couche protectrice qui entoure les fibres optiques pour les protéger des dommages mécaniques, de l'humidité et d'autres facteurs environnementaux. Elle est généralement fabriquée en plastique ou en PVC pour offrir une protection physique et préserver l'intégrité des fibres optiques à l'intérieur.
- **Fibres Kevlar** : Les fibres Kevlar, également connues sous le nom d'éléments de traction, sont des fils renforcés en aramide qui sont tressés autour des fibres optiques pour leur fournir une résistance à la traction. Le Kevlar aide à prévenir la rupture ou la déformation des fibres optiques dues à une tension excessive lors de l'installation ou de la manipulation.
- **Verre (ou fibre optique)** : La fibre optique elle-même est généralement fabriquée en verre ou en plastique. Elle constitue le cœur de la transmission optique en guidant la lumière le long de son chemin. Le verre offre une faible atténuation et une grande bande passante, ce qui en fait un matériau idéal pour la transmission de signaux optiques sur de longues distances.
- **Âme (ou cœur)** : L'âme, également appelée cœur, est la partie centrale de la fibre optique à travers laquelle la lumière est propagée. Elle est fabriquée en verre ou en plastique de haute pureté et est entourée d'une gaine protectrice. L'âme guide la lumière à travers la fibre en utilisant la réflexion interne totale pour assurer une transmission efficace des signaux optiques.



Caractéristique	Fibre OM
Type de fibre	Multimode
Diamètre du noyau	Plus grand (50 µm ou 62.5 µm)
Indice de réfraction	Plusieurs chemins de propagation
Bande passante	Inférieure à la fibre OS
Distance de transmission maximale	Plus courte (jusqu'à quelques centaines de mètres)
Applications typiques	Réseaux locaux (LAN), courtes distances
Connecteurs courants	SC, LC, ST

#### • Type de fibre :

- **Fibre OM (Multimode)** : La fibre multimode permet à plusieurs modes de lumière de se propager à travers le noyau de la fibre. Elle est principalement utilisée pour les réseaux locaux (LAN) et les applications sur de courtes distances.
- **Fibre OS (Monomode)** : La fibre monomode permet à un seul mode de lumière de se propager à travers le noyau de la fibre. Elle est principalement utilisée pour les réseaux étendus (WAN) et les applications sur de longues distances.

#### • Diamètre du noyau :

- **Fibre OM** : Le diamètre du noyau de la fibre multimode est plus grand. généralement de 50 µm ou 62.5 µm. ce qui permet à plusieurs modes de lumière de se propager.
- **Fibre OS** : Le diamètre du noyau de la fibre monomode est plus petit. généralement de 9 µm. ce qui permet à un seul mode de lumière de se propager avec précision.

#### • Indice de réfraction :

- **Fibre OM** : En raison de son diamètre de noyau plus grand. la fibre multimode a un indice de réfraction plus bas. ce qui permet à plusieurs modes de lumière de se propager.
- **Fibre OS** : Avec un diamètre de noyau plus petit. la fibre monomode a un indice de réfraction plus élevé. ce qui permet à un seul mode de lumière de se propager avec précision sur de longues distances.

#### • Bande passante :

- **Fibre OM** : La bande passante de la fibre multimode est généralement inférieure à celle de la fibre monomode en raison de la dispersion modale et de l'atténuation sur de longues distances.
- **Fibre OS** : La bande passante de la fibre monomode est généralement supérieure à celle de la fibre multimode en raison de sa capacité à supporter des longueurs d'onde plus élevées et à minimiser la dispersion.

• **Distance de transmission maximale :**

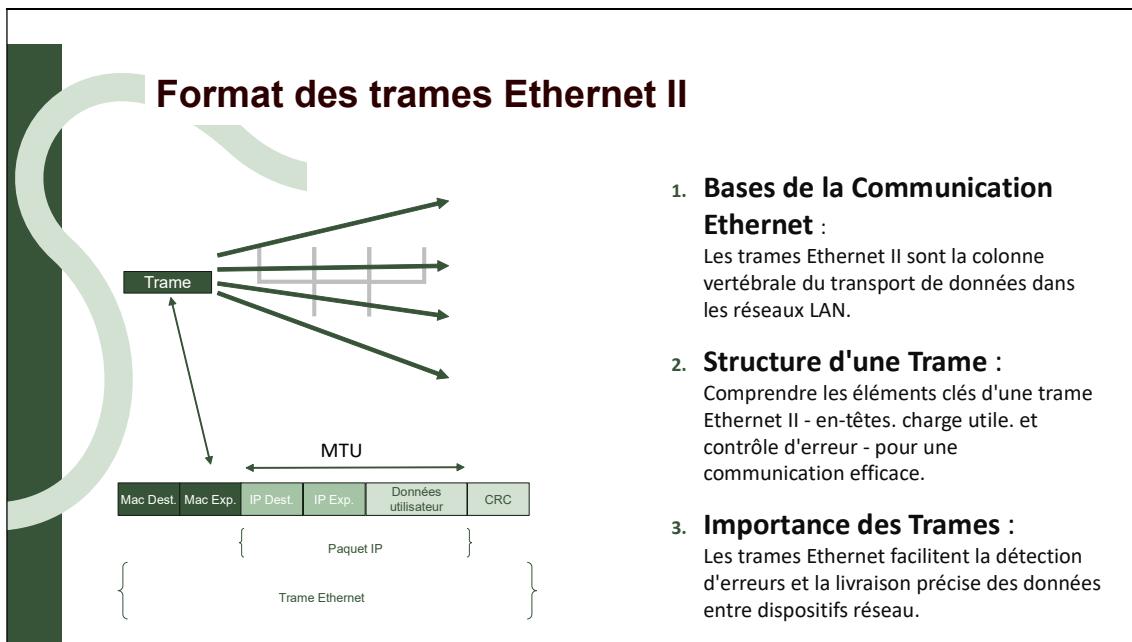
- **Fibre OM** : En raison de la dispersion modale et de l'atténuation, la distance de transmission maximale de la fibre multimode est généralement plus courte, allant jusqu'à quelques centaines de mètres.
- **Fibre OS** : La fibre monomode peut prendre en charge des distances de transmission beaucoup plus longues, allant jusqu'à plusieurs kilomètres, en raison de sa capacité à minimiser la dispersion et l'atténuation.

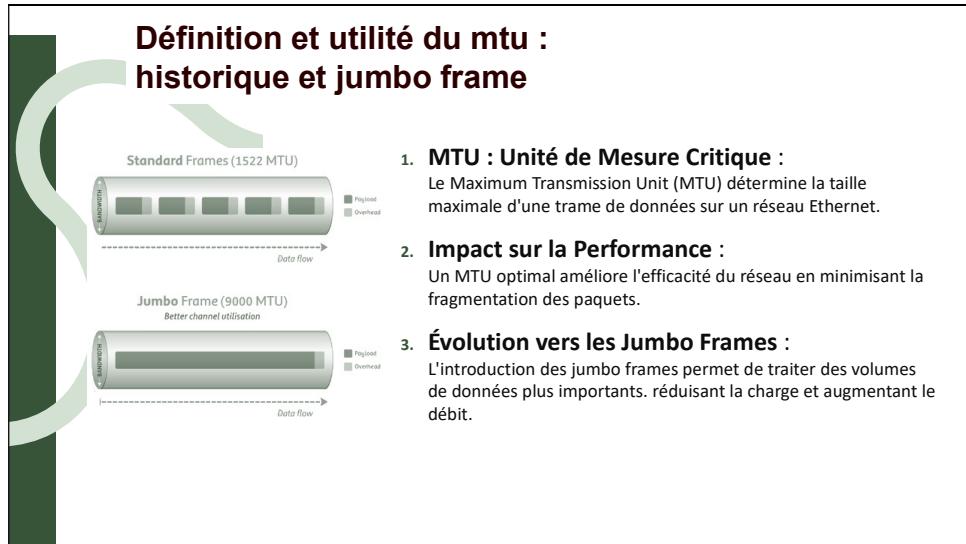
• **Applications typiques :**

- **Fibre OM** : La fibre multimode est couramment utilisée dans les réseaux locaux (LAN), les centres de données et les applications sur de courtes distances.
- **Fibre OS** : La fibre monomode est préférée pour les réseaux étendus (WAN), les liaisons interurbaines, les réseaux métropolitains et les applications sur de longues distances.

• **Connecteurs courants :**

- Les connecteurs couramment utilisés pour les deux types de fibre comprennent SC (Subscriber Connector), LC (Lucent Connector), ST (Straight Tip) et FC (Ferrule Connector), entre autres. Ces connecteurs sont utilisés pour relier les câbles de fibre optique aux équipements réseau.





## L'Émergence des Jumbo Frames

Les jumbo frames sont des paquets Ethernet plus grands que le MTU standard de 1500 octets, pouvant atteindre jusqu'à 9000 octets dans certains cas. L'utilisation des jumbo frames permet de réduire le nombre total de paquets transmis sur le réseau, diminuant ainsi la charge sur les dispositifs réseau et améliorant l'efficacité du transfert de données. Les jumbo frames sont particulièrement utiles dans les environnements réseau à haut débit, comme les data centers et les applications de stockage en réseau (NAS/SAN).

## Considérations et Applications

La mise en œuvre des jumbo frames nécessite que tous les composants du réseau (cartes réseau, switchs, routeurs) supportent cette fonctionnalité, car l'utilisation de tailles de trame incompatibles peut entraîner une perte de données ou des erreurs de transmission. La configuration du MTU doit donc être effectuée avec prudence, en tenant compte des capacités de l'infrastructure réseau existante et des besoins spécifiques des applications.

## Conclusion

Le MTU est un aspect fondamental de la configuration réseau qui influence directement la performance et l'efficacité de la communication Ethernet. La compréhension du MTU et l'adaptation aux besoins en évoluant vers l'utilisation de jumbo frames lorsque c'est possible et pertinent peuvent significativement améliorer le traitement des données dans les réseaux modernes.



**Objectifs :**  
**Découvrir l'utilisation de**  
**Wershark**

## **Démonstration**

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---



## Démonstration

— **Objectifs :**

- Découvrir l'analyse de trames Ethernet en utilisant Wireshark.
- Visualiser l'encapsulation des données à travers les différentes couches du modèle OSI et interpréter les divers champs d'une trame Ethernet.

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---



## Démonstration

- Objectif :
  - Observer des numéros d’OUI avec wireshark

- Ce qu'il faut retenir



1. **Ethernet**
2. **Flexibilité et Évolution des Topologies Réseau**
3. **CSMA/CD et la Gestion des Collisions**
4. **Adressage MAC et Sécurité**
5. **Importance de l'Adressage et du Câblage Ethernet**

•**Ethernet** : Le Standard Dominant pour les Réseaux Locaux :

"Ethernet est la technologie de réseau local (LAN) la plus largement utilisée, offrant une méthode fiable et standardisée pour connecter des appareils dans des environnements filaires."

•**Flexibilité et Évolution des Topologies Réseau** :

"Les topologies de réseau Ethernet, telles que les configurations en bus, étoile et architecture maillée, démontrent la flexibilité et l'évolutivité d'Ethernet pour répondre aux besoins changeants des organisations."

•**CSMA/CD et la Gestion des Collisions** :

"Le protocole d'accès au média CSMA/CD (Carrier Sense Multiple Access with Collision Detection) permet à Ethernet de gérer efficacement les collisions sur le réseau, assurant une communication fluide même dans des environnements à forte densité de trafic."

•**Adressage MAC et Sécurité** :

"L'adressage MAC (Media Access Control) fournit une méthode unique d'identification des appareils sur un réseau Ethernet, jouant un rôle crucial dans la gestion du réseau et la sécurité."

•**Importance de l'Adressage et du Câblage Ethernet** :

"La sélection appropriée des câbles Ethernet et la compréhension des catégories de câblage, ainsi que le rôle des connecteurs et des standards de câblage, sont essentiels pour maximiser les performances et la fiabilité du réseau."

## Chapitre3 – Commutation Ethernet ou « switching »

### **3 - Commutation Ethernet ou « switching »**

- Objectifs du chapitre

## Plan de la formation

- 1 - Pourquoi un réseau ?
- 2 - Le réseau Ethernet
- 3 - Commutation Ethernet ou "switching"**
- 4 - WiFi
- 5 - TCP/IP
- 6 - DHCP et DNS
- 7 - Administration

- Comprendre la Commutation
- Identifier les Différentes Gammes de Switch
- Analyser l'Impact de la Commutation sur le Trafic Réseau
- Explorer les Architectures de Réseau et leur Impact
- Expliquer l'Utilité et les Avantages de la Commutation
- Assurer l'Homogénéité et la Fonctionnalité des Réseaux

Le troisième chapitre de notre formation représente un approfondissement des connaissances techniques en réseau. Après avoir exploré la structure et la classification des réseaux, ainsi que les spécificités du réseau Ethernet, les participants sont désormais prêts à entrer dans le vif du sujet avec la commutation Ethernet. Voici quelques points à aborder pour une introduction complète :

Rappel des Notions Antérieures :

Commencez par un bref rappel des concepts de réseau Ethernet pour ancrer la commutation de niveau 2 dans le contexte déjà appris.

L'Importance de la Commutation :

Soulignez l'importance cruciale de la commutation dans la gestion du trafic réseau et la façon dont elle contribue à l'efficacité et la stabilité d'un réseau.

Présentation des Objectifs du Chapitre :

Introduisez les principaux sujets et objectifs du chapitre, en insistant sur la manière dont la commutation Ethernet est centrale pour le design et la maintenance des réseaux modernes.

Pour le chapitre 3, intitulé "Commutation Ethernet ou « switching »", les principaux objectifs pédagogiques pourraient être :

• **Comprendre la Commutation de Niveau 2 :**

- Appréhender le fonctionnement de la commutation au niveau de la couche de liaison de données (couche 2).
- Expliquer les principes de l'auto-apprentissage des adresses MAC et de l'apprentissage statique (sticky).

• **Identifier les Différentes Gammes de Switch :**

- Distinguer les différents types de switches utilisés dans les réseaux, y compris les switches d'accès, de distribution, et de cœur.
- Comprendre les fonctions et les applications propres à chaque type de switch dans l'architecture réseau.

**Analyser l'Impact des Boucles de Niveau 2 :**

- Examiner les conséquences des boucles de niveau 2 sur la performance du réseau.
- Discuter des méthodes de prévention des boucles. notamment l'importance des techniques de débouclage.

**• Explorer les Architectures Redondantes :**

- Étudier l'utilisation et le fonctionnement du protocole Spanning Tree (STP) et de ses variantes (RSTP, MSTP) pour la gestion de la redondance et l'élimination des boucles.
- Comprendre la mise en œuvre de l'agrégation de liens (Link Aggregation Groups - LAG) pour augmenter la bande passante et la tolérance aux pannes.

**• Expliquer l'Utilité et la Configuration des VLANs :**

- Discuter de l'intérêt des VLANs pour segmenter les réseaux. améliorer la qualité de service (QoS) et renforcer la sécurité.
- Étudier le protocole 802.1Q pour le marquage VLAN et apprendre comment configurer les VLANs sur les switches et les routeurs (avec des ports en mode accès, tronc, taggé ou non taggé).

**• Assurer l'Homogénéité de la Base de Données VLAN :**

- Comprendre les protocoles tels que le VTP (VLAN Trunking Protocol) ou le GVRP (Generic VLAN Registration Protocol) et leur rôle dans la gestion des VLANs dans un réseau étendu.



- **Optimisation de la Connexion :**  
"Avez-vous déjà vécu une situation où plusieurs appareils devaient être connectés ensemble dans un petit espace ? Comment avez-vous géré cette situation ?"
- **Expérience de Latence ou de Perte de Signal :**  
"Pouvez-vous décrire un moment où vous avez rencontré des problèmes de latence ou de perte de signal pendant que vous étiez connecté à un réseau ? Qu'avez-vous pensé qui pourrait être la cause ?"
- **Gestion des Ressources en Réseau :**  
"Dans votre expérience, y a-t-il eu un moment où vous deviez prioriser certains appareils ou services sur votre réseau pour optimiser la performance ? Comment avez-vous décidé quels appareils ou services prioriser ?"
- **Sécurité et Accès au Réseau :**  
"Avez-vous déjà eu à restreindre ou à contrôler l'accès à votre réseau pour des raisons de sécurité ou de gestion de la bande passante ? Quelles mesures avez-vous prises ?"
- **Configuration et Extension du Réseau :**  
"Si vous avez déjà été impliqué dans l'ajout de nouveaux appareils ou services à un réseau existant, quelles étaient vos principales considérations pour assurer une intégration réussie ?"

**Optimisation de la Connexion :**

"Avez-vous déjà vécu une situation où plusieurs appareils devaient être connectés ensemble dans un petit espace ? Comment avez-vous géré cette situation ?"

**Expérience de Latence ou de Perte de Signal :**

"Pouvez-vous décrire un moment où vous avez rencontré des problèmes de latence ou de perte de signal pendant que vous étiez connecté à un réseau ? Qu'avez-vous pensé qui pourrait être la cause ?"

**Gestion des Ressources en Réseau :**

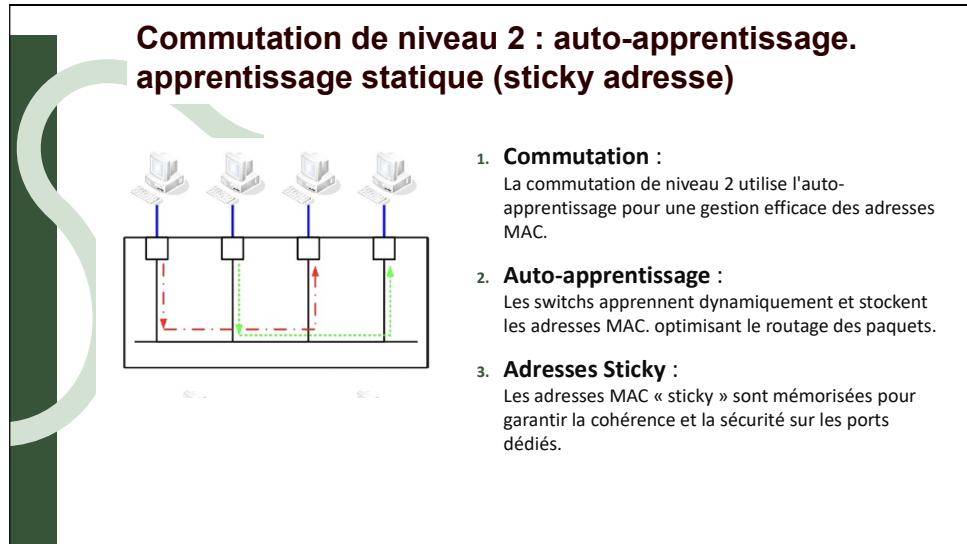
"Dans votre expérience, y a-t-il eu un moment où vous deviez prioriser certains appareils ou services sur votre réseau pour optimiser la performance ? Comment avez-vous décidé quels appareils ou services prioriser ?"

**Sécurité et Accès au Réseau :**

"Avez-vous déjà eu à restreindre ou à contrôler l'accès à votre réseau pour des raisons de sécurité ou de gestion de la bande passante ? Quelles mesures avez-vous prises ?"

**Configuration et Extension du Réseau :**

"Si vous avez déjà été impliqué dans l'ajout de nouveaux appareils ou services à un réseau existant, quelles étaient vos principales considérations pour assurer une intégration réussie ?"



### Commutation de Niveau 2 : Auto-Apprentissage et Apprentissage Statique

La commutation de niveau 2 est une pierre angulaire des réseaux locaux (Local Area Networks, LANs). À ce niveau, les switchs jouent un rôle crucial dans la direction du trafic entre les dispositifs en apprenant et en utilisant les adresses MAC (Media Access Control).

#### Principe d'Auto-Apprentissage

Les switchs de niveau 2 disposent d'une capacité d'auto-apprentissage qui leur permet de construire et de maintenir dynamiquement une table d'adresses MAC. Lorsqu'un paquet arrive sur un port, le switch enregistre l'adresse MAC source de ce paquet dans sa table, associant cette adresse au port correspondant. Lorsque le switch a besoin de transférer un paquet vers une destination spécifique, il consulte sa table pour déterminer le port de sortie adéquat. Si l'adresse n'est pas connue, le switch effectue un flood du paquet sur tous les ports, à l'exception de celui sur lequel le paquet est arrivé.

#### Apprentissage Statique et Adresses "Sticky"

Outre l'auto-apprentissage, les switchs de niveau 2 peuvent être configurés pour utiliser l'apprentissage statique, souvent désigné par le terme "sticky". Dans ce mode, une adresse MAC spécifique est manuellement attribuée à un port, et le switch ne permettra qu'aux dispositifs avec cette adresse MAC d'accéder au réseau via ce port. Les adresses "sticky" sont utiles pour sécuriser l'accès au réseau et pour s'assurer que seuls les dispositifs autorisés peuvent se connecter à des segments spécifiques du réseau.

#### Sécurité et Gestion du Trafic

La combinaison d'auto-apprentissage et d'apprentissage statique offre une gestion efficace du trafic tout en renforçant la sécurité. L'utilisation judicieuse de ces fonctionnalités peut prévenir les accès non autorisés et garantir que le réseau fonctionne de manière optimale.

#### Conclusion

La compréhension de la commutation de niveau 2 est essentielle pour tout professionnel réseau. En maîtrisant l'auto-apprentissage et l'apprentissage statique, vous pouvez non seulement assurer que votre réseau est performant mais aussi sécurisé contre les accès indésirables. Cela crée une base solide pour la mise en œuvre de politiques réseau plus complexes et pour la maintenance d'une infrastructure réseau robuste et sécurisée.

**Commutation de niveau 2 : auto-apprentissage.  
apprentissage statique (sticky adresse)**

— auto-apprentissage:

Int	Mac Adresse
0/1	
0/2	
0/3	
0/4	

The diagram shows a switch with four ports (0/1 to 0/4). Two hosts, both labeled "PC-PT", are connected to the switch. The host at port 0/2 is labeled "@Mac B" and the host at port 0/1 is labeled "@Mac A". Arrows point from the port numbers to the corresponding MAC addresses. To the right of the switch, the MAC addresses are listed: Mac C is associated with port 0/2 and Mac D is associated with port 0/1.

## Commutation de niveau 2 : auto-apprentissage. apprentissage statique (sticky adresse)

### — Sticky adresse:

Résultats au démarrage du switch:

Int	Mac Adresse
0/1	@Mac A
0/2	@Mac B
0/3	@Mac C
0/4	@Mac D

Etapes :

- Configuration des interfaces
- Démarrage des stations (PC)
- Sauvegarde de la configuration du switch

Syntaxe (pour chaque interface station) :

- switchport port-security
- switchport port-security mac-address sticky

- Atelier



– Objectifs :

- Naviguer dans les modes de l'IOS pour nommer un switch.
- Constater la différence entre la running-config et la startup-config.

– Enoncé : voir livret d'ateliers



**Découvrir la commande  
show mac adresse-table**

## **Démonstration**

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---



## Démonstration

Réalisation d'un ping entre  
deux machines.  
puis d'une boucle dans  
"packet tracer" (sans stp)  
observations

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

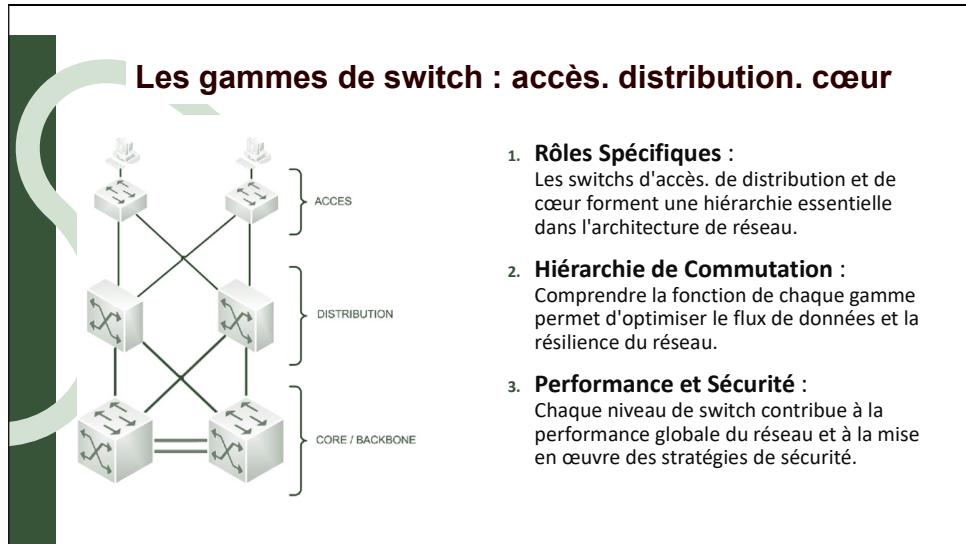
---

---

---

---

---



## Les Gammes de Switchs : Accès. Distribution. Cœur

Dans l'architecture des réseaux d'entreprise modernes, les switchs sont souvent classés en fonction de leur position dans la hiérarchie du réseau : accès, distribution et cœur. Chaque niveau de switch joue un rôle spécifique qui contribue à la performance et à la sécurité du réseau global.

### Switchs d'Accès

- **Fonction :** Connectent les dispositifs utilisateurs finaux au réseau.
- **Caractéristiques :** Souvent offrent des fonctionnalités de contrôle d'accès avancées, telles que le support des VLANs et des fonctions de sécurité.
- **Placement :** Se trouvent généralement à la périphérie du réseau, là où les utilisateurs et les dispositifs se connectent physiquement au réseau.

### Switchs de Distribution

- **Fonction :** Agrègent les connexions des switchs d'accès et les acheminent vers la couche de cœur.
- **Caractéristiques :** Incluent des capacités de routage ou de commutation multicouche pour le filtrage du trafic, la QoS et le routage inter-VLAN.
- **Placement :** Opèrent comme un lien intermédiaire entre les switchs d'accès et les switchs de cœur.

### Switchs de Cœur

- **Fonction :** Constituent le backbone du réseau, offrant un chemin de transport à haute vitesse pour le trafic allant d'un point à un autre du réseau.
- **Caractéristiques :** Conçus pour la fiabilité et la haute performance, avec une capacité à gérer de grands volumes de trafic.
- **Placement :** Sont le cœur du réseau, garantissant la connectivité et la résilience à l'échelle de l'entreprise.

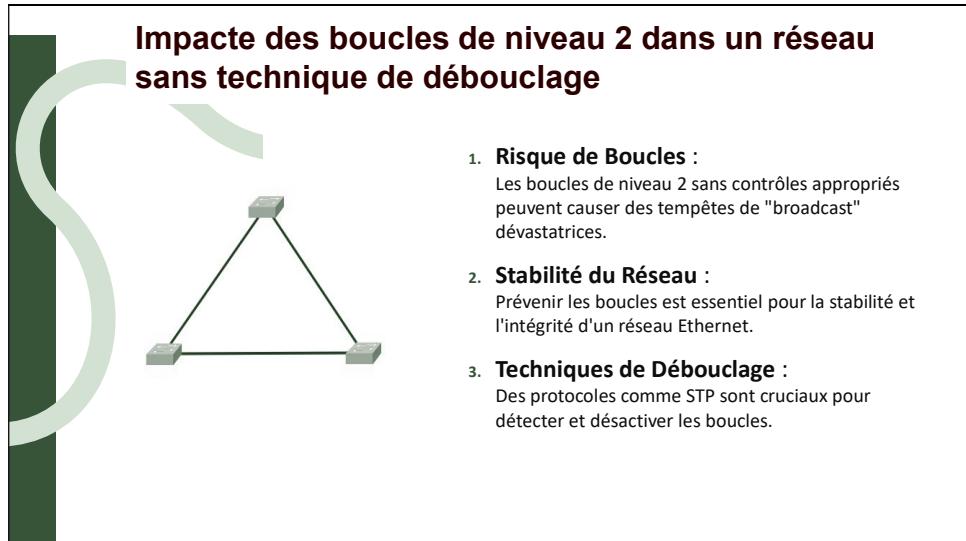
**Importance des Gammes de Switchs**

La sélection du switch approprié pour chaque niveau est cruciale pour assurer l'évolutivité et la gestion efficace du réseau. Les switchs d'accès doivent être choisis en fonction de leur capacité à gérer le nombre d'utilisateurs finaux et leurs besoins spécifiques en termes de connectivité. Les switchs de distribution doivent être capables de gérer le routage efficace du trafic et l'application des politiques de réseau. Les switchs de cœur doivent être choisis pour leur robustesse et leur capacité à supporter les plus hauts débits de données avec une latence minimale.

**Conclusion**

Comprendre les fonctions et les applications des différentes gammes de switchs est essentiel pour la conception d'un réseau fiable et efficace. Les switchs d'accès, de distribution et de cœur travaillent ensemble pour fournir une connectivité transparente, tout en gérant la sécurité, la performance et la redondance nécessaires pour les opérations du réseau.

### Impacte des boucles de niveau 2 dans un réseau sans technique de débouclage



1. **Risque de Boucles :**  
Les boucles de niveau 2 sans contrôles appropriés peuvent causer des tempêtes de "broadcast" dévastatrices.
2. **Stabilité du Réseau :**  
Prévenir les boucles est essentiel pour la stabilité et l'intégrité d'un réseau Ethernet.
3. **Techniques de Débouclage :**  
Des protocoles comme STP sont cruciaux pour détecter et désactiver les boucles.

### Impact des Boucles de Niveau 2 et Importance des Techniques de Débouclage

Les boucles de niveau 2 dans un réseau Ethernet peuvent avoir des conséquences sérieuses sur les performances et la stabilité du réseau. Sans mécanismes de débouclage, les boucles créent des conditions où les trames de données circulent indéfiniment, provoquant une utilisation excessive de la bande passante, des collisions répétées et des tempêtes de diffusion qui peuvent saturer et paralyser le réseau.

### Pourquoi les Boucles sont un Problème

- **Tempêtes de Broadcast :** Les trames de diffusion (broadcast) envoyées en boucle se multiplient et inondent le réseau, consommant la capacité des switchs et la bande passante disponible.
- **Table d'Adresse MAC Instable :** Les switchs apprennent et stockent les adresses MAC associées à leurs ports. Les boucles font fluctuer ces associations de manière imprévisible, ce qui empêche la commutation efficace.
- **Perte de Service :** Une surcharge du réseau due à une boucle peut mener à un service dégradé ou à un arrêt complet, affectant tous les utilisateurs et services du réseau.

### Techniques de Débouclage

Pour contrer les effets néfastes des boucles de niveau 2, les réseaux implémentent des protocoles de débouclage, le plus commun étant le Spanning Tree Protocol (STP) et ses variantes (RSTP, MSTP). Ces protocoles ont pour fonction de :

- **Identifier la Présence de Boucles :** STP échange des informations entre les switchs pour détecter la présence de boucles potentielles.
- **Désactiver les Chemins Redondants :** Lorsqu'une boucle est détectée, STP désactive certains chemins pour empêcher la formation de boucles, tout en assurant qu'un chemin alternatif reste disponible en cas de défaillance d'un lien.
- **Réagir Dynamiquement aux Changements :** STP ajuste dynamiquement l'architecture active du réseau pour s'adapter aux changements, comme l'ajout ou la suppression de switchs, ou les défaillances de liaison.

### **Conclusion**

Comprendre l'impact des boucles de niveau 2 et comment les techniques de débouclage protègent le réseau est fondamental pour tout professionnel en réseau. Une bonne conception de réseau ainsi qu'une mise en œuvre et une gestion appropriées des protocoles de débouclage sont cruciales pour assurer un réseau Ethernet robuste et fiable.



**Architecture redondante :**  
Spanning Tree 802.1D. 802w. 802.1s (usage. algorithme. les types de ports. le paramétrage ). Agrégation de liens (LAG).

1. **Sécurité par Redondance :**  
L'architecture redondante avec STP et LAG prévient les défaillances et assure la continuité des services réseau.
2. **Optimisation STP :**  
Protocoles 802.1D. 802.1w (RSTP). et 802.1s (MSTP) adaptent le réseau pour une topologie sans boucle et efficiente.
3. **Agilité du Réseau :**  
La configuration LAG améliore la bande passante et la tolérance aux pannes par des liens multiples et parallèles.

## Architecture Redondante et Techniques de Gestion

Dans un réseau, l'architecture redondante est un élément crucial pour augmenter la fiabilité et la résilience. Elle emploie des systèmes et des chemins alternatifs pour assurer un service ininterrompu en cas de défaillance d'une composante du réseau. Deux des principales méthodes pour créer une telle architecture sont les protocoles Spanning Tree (STP) et l'Agrégation de Liens (LAG).

### Spanning Tree Protocol (STP) et ses Variations

Les protocoles Spanning Tree, y compris 802.1D (STP traditionnel), 802.1w (Rapid Spanning Tree Protocol, RSTP), et 802.1s (Multiple Spanning Tree Protocol, MSTP), sont conçus pour construire une topologie réseau sans boucle. Voici comment ils fonctionnent :

- **802.1D (STP)** : Identifie et désactive les chemins redondants pour éviter les boucles de réseau potentielles.
- **802.1w (RSTP)** : Une évolution de STP, RSTP accélère le processus de reconfiguration du réseau pour une réponse plus rapide aux changements topologiques.
- **802.1s (MSTP)** : Permet plusieurs instances de STP pour coexister sur le même réseau physique, offrant une plus grande flexibilité et une utilisation plus efficace des ressources de réseau.

Chacun de ces protocoles utilise un algorithme spécifique pour sélectionner des chemins sans boucle, en se basant sur une structure d'arborescence couvrante. Ils utilisent divers états de ports (bloquant, écoute, apprentissage, transfert) pour déterminer le rôle de chaque port dans le réseau. Le paramétrage de ces protocoles est essentiel pour assurer une hiérarchisation efficace et une prise de décision correcte dans le réseau.

### Agrégation de Liens (LAG)

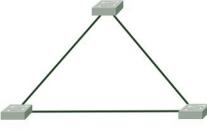
LAG, parfois appelée port channel ou EtherChannel, combine plusieurs connexions réseau physiques en un seul canal logique. Ce processus améliore la bande passante et la tolérance aux pannes, puisque le trafic peut être réparti sur plusieurs liens physiques et le réseau peut continuer à fonctionner même si un lien spécifique échoue.

- **Amélioration de la Bande Passante** : Avec LAG, la capacité de transfert des données est augmentée par l'addition des débits de tous les liens physiques du groupe.
- **Tolérance aux Pannes** : En cas de défaillance d'un lien individuel dans un LAG, les autres liens prennent le relais sans interruption de service notable.

## Conclusion

L'architecture redondante est essentielle pour maintenir la continuité et la qualité des services de réseau. La connaissance et l'application correctes des protocoles STP et des configurations LAG sont des compétences vitales pour les ingénieurs réseau qui souhaitent assurer une infrastructure réseau robuste, flexible et haute disponibilité.

**Architecture redondante :**  
**Spanning Tree 82.1D. 802w. 802.1s (usage. algorithme. les types de ports. le paramétrage ). Agrégation de liens (LAG).**



1. **Prévention des boucles réseau :** "Spanning Tree Protocol est essentiel pour maintenir un réseau sain en prévenant activement les boucles de commutation qui peuvent paralyser le trafic réseau."

2. **Stabilité et fiabilité :** "STP assure une architecture réseau stable et fiable en désactivant automatiquement les liens redondants, tout en les gardant en réserve pour une bascule rapide en cas de défaillance du lien principal."

3. **Optimisation et efficacité :** "Avec les avancées de RSTP et MSTP, le protocole Spanning Tree permet une convergence plus rapide et une gestion plus efficace de plusieurs VLANs, optimisant ainsi la performance globale du réseau."

Le protocole Spanning Tree (STP) est un protocole de réseau essentiel conçu pour empêcher les boucles de commutation dans les réseaux à maillage partiel ou complet. Une boucle de commutation peut se produire dans un réseau lorsque deux commutateurs sont interconnectés par plusieurs chemins. Si un paquet est envoyé dans cette boucle, il peut continuer à circuler indéfiniment, causant des tempêtes de diffusion, des dégradations de performances, voire des pannes du réseau.

STP a été introduit par le standard IEEE 802.1D. Il utilise un algorithme qui sélectionne un commutateur principal appelé Root Bridge. À partir de ce Root Bridge, un arbre recouvrant (spanning tree) est calculé, définissant un seul chemin actif entre tous les points du réseau. Tous les chemins alternatifs qui pourraient causer une boucle sont mis en état de blocage. Voici les éléments clés du protocole Spanning Tree :

• **Root Bridge:** Le commutateur central dans le réseau à partir duquel l'architecture de l'arbre recouvrant est établie.

• **Port Roles:**

- **Root Port:** Le port sur un commutateur non-root qui est le plus proche du Root Bridge, en termes de coût de chemin.
- **Designated Port:** Sur chaque segment de réseau, un seul port est élu pour être le port désigné, par lequel tous les paquets sont transmis.
- **Blocked Port:** Les ports qui sont mis en état de blocage pour éviter les boucles de commutation.

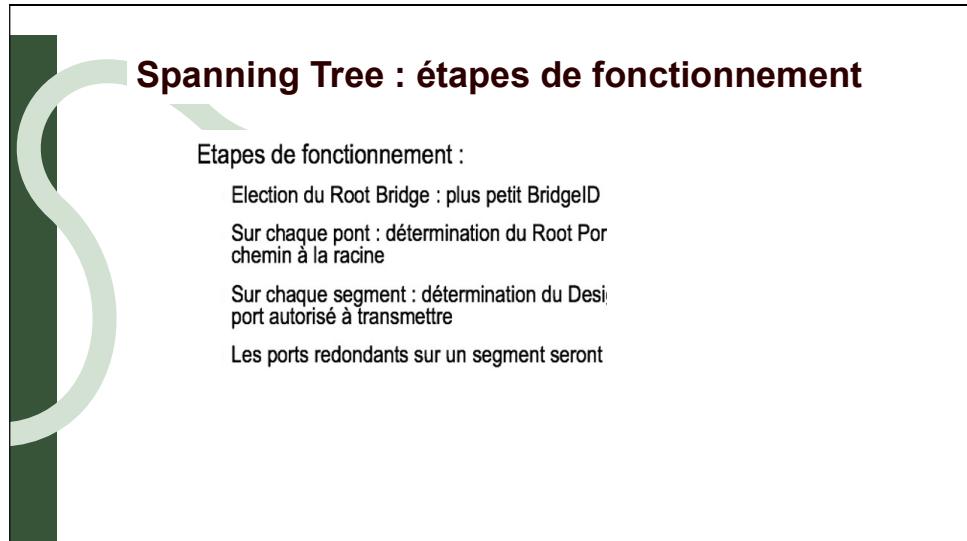
• **Path Cost:** Chaque chemin dans le réseau est évalué avec un coût basé sur la bande passante du lien. Les chemins avec le coût le plus bas deviennent les chemins préférés.

• **BPDU (Bridge Protocol Data Units):** Ce sont des messages d'information utilisés par le protocole STP pour détecter les boucles et calculer les chemins optimaux.

Avec l'évolution des réseaux, de nouvelles versions de Spanning Tree ont été développées :

• **Rapid Spanning Tree Protocol (RSTP)**, ou 802.1w, qui offre des temps de convergence plus rapides que le STP traditionnel.

• **Multiple Spanning Tree Protocol (MSTP)**, ou 802.1s, qui permet de configurer plusieurs instances de STP sur différents VLANs, optimisant ainsi l'utilisation de la bande passante. En pratique, l'utilisation du Spanning Tree Protocol est essentielle pour garantir la stabilité et la performance d'un réseau d'entreprise. Il est important de configurer soigneusement STP pour éviter les temps de convergence longs et les éventuelles pertes de connectivité lors des recalculs de l'arbre. L'agrégation de liens, connue aussi sous le terme LAG (Link Aggregation Group), peut également être utilisée conjointement avec STP pour augmenter la bande passante et la redondance des chemins sans créer de boucles.



### Spanning Tree Protocol : Étapes de Fonctionnement

#### 1. Élection du Root Bridge :

- Le cœur du réseau Spanning Tree est le Root Bridge. Ce commutateur sert de point de référence pour l'ensemble du spanning tree.
- L'élection du Root Bridge est basée sur l'identifiant de pont (Bridge ID), qui se compose d'une priorité (valeur par défaut 32768) et de l'adresse MAC du commutateur.
- Le commutateur avec le plus petit Bridge ID devient le Root Bridge. Si les priorités sont égales, le commutateur avec l'adresse MAC la plus basse est élu.

#### 2. Détermination du Root Port sur chaque commutateur (non Root Bridge) :

- Chaque commutateur non Root doit déterminer son port qui mène au chemin le plus court vers le Root Bridge. Ce port est appelé Root Port (RP).
- Le chemin le plus court est déterminé par le coût du chemin, qui est calculé en fonction de la vitesse des liens de réseau. Plus la vitesse du lien est élevée, plus le coût est faible.
- En cas d'égalité des coûts de chemin, des critères supplémentaires comme l'identifiant de pont envoyeur et l'identifiant de port envoyeur sont utilisés pour déterminer le Root Port.

#### 3. Élection du Designated Port pour chaque segment de réseau :

- Un seul port par segment de réseau (souvent une connexion physique entre commutateurs) est autorisé à transmettre le trafic vers et depuis le Root Bridge. Ce port est appelé le Designated Port (DP).
- L'élection du Designated Port est déterminée par le plus bas coût de chemin vers le Root Bridge, suivi de l'identifiant de pont le plus bas, puis de l'identifiant de port le plus bas en cas d'égalité.

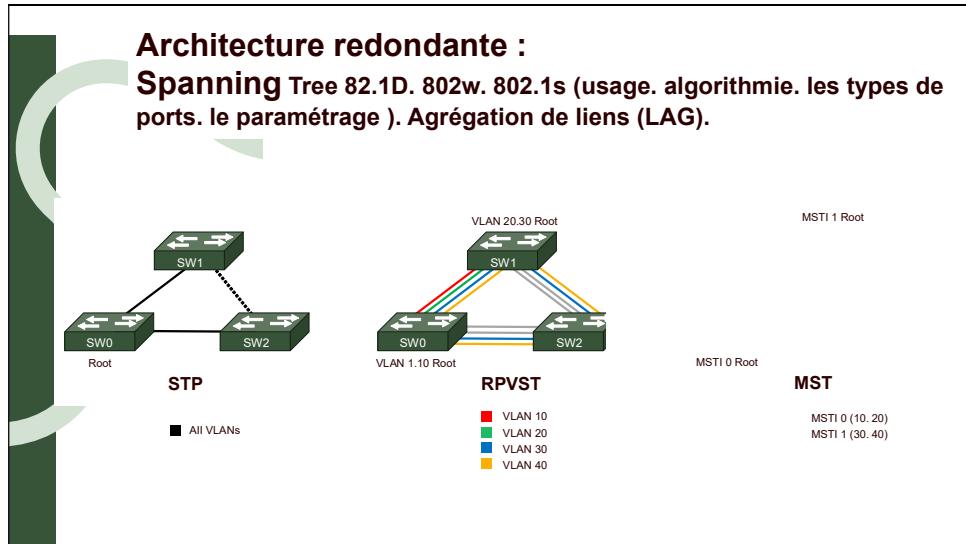
#### 4. Mise en état de blocage des ports redondants :

- Pour éviter les boucles dans le réseau, tous les ports qui ne sont ni le Root Port ni le Designated Port sont mis en état de blocage (Blocking State).
- Ces ports ne transmettent ni ne reçoivent de trames, mais ils écoutent toujours les BPDUs pour pouvoir entrer en action si le Designated Port ou le Root Port actuel devient indisponible.

**Importance de ces étapes :**

- Les étapes énumérées ci-dessus sont critiques pour maintenir un réseau sans boucle et performant. En suivant ces étapes. STP crée une topologie de réseau logique et hiérarchique qui optimise les chemins de transmission de données tout en offrant une redondance en cas de défaillance du lien.
- La compréhension de ces étapes est cruciale pour tout professionnel des réseaux. car elle aide à dépanner et à configurer les réseaux avec une architecture redondante. Cette séquence d'étapes doit être assimilée pour garantir que les stagiaires puissent comprendre et appliquer les principes de STP dans des scénarios de réseau réels.

Ce contenu est destiné à fournir aux stagiaires un aperçu technique et pratique du fonctionnement de STP. qu'ils pourront utiliser comme référence lors de la configuration et de la gestion des réseaux d'entreprise.



### Spanning Tree Protocol (STP)

- **Standard IEEE:** 802.1D
- **Fonctionnement:** STP crée un arbre recouvrant sans boucle pour le réseau entier. avec un seul Root Bridge. Il met en état de blocage tous les chemins redondants pour éviter les boucles.
- **Temps de convergence:** Peut être lent. typiquement 30 à 50 secondes. car il doit passer par les états d'écoute et d'apprentissage avant de transmettre des données.
- **VLANs:** STP ne distingue pas les VLANs et exécute une seule instance pour tous les VLANs présents sur le réseau.

### Rapid Per-VLAN Spanning Tree (RPVST)

- **Standard IEEE:** 802.1w pour Rapid STP (RSTP) et extension Cisco pour le per-VLAN.
- **Fonctionnement:** Amélioration de STP. RPVST permet une convergence plus rapide après un changement de topologie en utilisant RSTP. Il exécute une instance de Spanning Tree pour chaque VLAN. permettant d'optimiser la topologie pour chaque VLAN individuellement.
- **Temps de convergence:** Généralement moins de 10 secondes.
- **VLANs:** Chaque VLAN peut avoir un Root Bridge différent. ce qui peut optimiser le chemin du trafic pour différents services ou applications.

### Multiple Spanning Tree (MST)

- **Standard IEEE:** 802.1s
- **Fonctionnement:** MST permet de regrouper plusieurs VLANs dans une seule instance de Spanning Tree. réduisant ainsi la charge CPU des commutateurs et la complexité de la gestion de réseau. MSTP est conçu pour fonctionner dans des environnements où de multiples VLANs sont en usage.
- **Temps de convergence:** Similaire à RPVST. MST fournit une convergence rapide et un équilibrage de charge efficace.
- **VLANs:** Permet de créer plusieurs instances de spanning tree. chacune pouvant inclure un ou plusieurs VLANs. Chaque instance a sa propre topologie. optimisant les chemins de transit pour les groupes de VLANs concernés.

**Comparatif**

- **STP** est le plus basique et ne gère pas les VLANs de manière individuelle. ce qui le rend moins flexible et plus lent à converger.
- **RPVST** est une amélioration par rapport à STP. avec une convergence plus rapide et une gestion individuelle des VLANs. offrant ainsi une meilleure performance et optimisation.
- **MST** combine les avantages de RSTP et PVST. permettant une convergence rapide tout en réduisant le nombre d'instances nécessaires pour gérer les VLANs. ce qui améliore l'efficacité dans les grands réseaux.  
La diapositive illustre ces concepts avec un schéma de réseau montrant comment chaque protocole pourrait gérer un changement dans le réseau. comme la défaillance d'un lien.

- Atelier



**ATELIER 4**

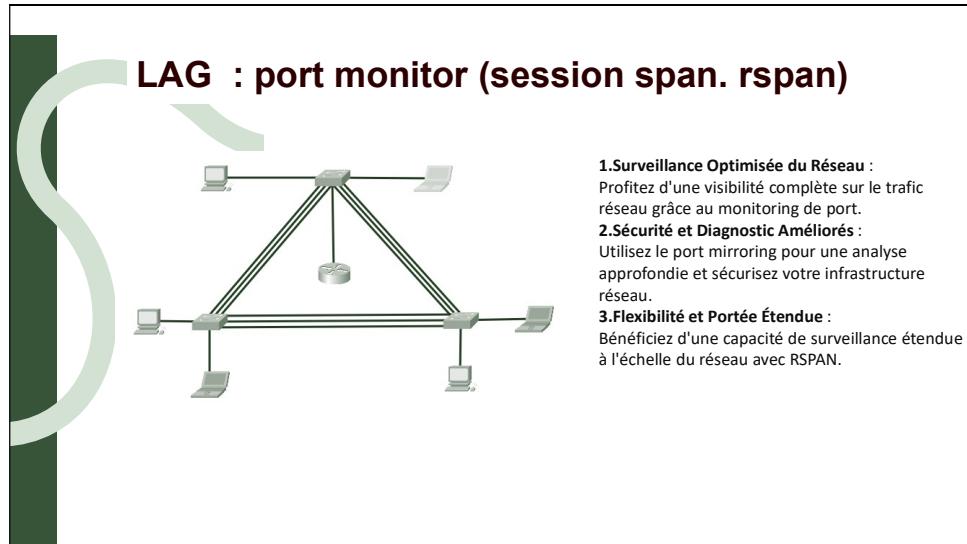
**Activité**

8

**Objectifs :**

- ▶ Visualiser l'état du Spanning-Tree du laboratoire.
- ▶ Configurer les root-bridge.

**Enoncé – Voir livret d'ateliers**



## LAG : Port Monitor (SPAN, RSPAN)

### Le Port Monitoring (Mirroring) :

- Le port monitoring, aussi appelé mirroring, est une fonctionnalité de réseau qui permet de copier le trafic passant par un ou plusieurs ports (ou VLAN) d'un commutateur à un autre port où le trafic peut être analysé.
- Ceci est couramment utilisé pour le dépannage réseau, la surveillance de la sécurité, et pour les analyses de conformité et de performance.

### SPAN (Switched Port Analyzer) :

- SPAN, ou session span, est la fonctionnalité de Cisco pour le port mirroring au sein d'un seul commutateur.
- Il permet de sélectionner les ports sources (ports monitorés) et un port de destination (port d'analyse) sur le même commutateur.
- Cela permet aux administrateurs de capturer et d'analyser le trafic pour le dépannage ou le monitoring.

### RSPAN (Remote SPAN) :

- RSPAN étend la fonctionnalité SPAN en permettant le mirroring de trafic entre commutateurs sur un réseau local (LAN).
- Un VLAN RSPAN est créé spécifiquement pour transporter le trafic miroir d'un commutateur à un autre.
- Cela permet l'analyse de trafic depuis un emplacement central même si les ports sources sont répartis sur plusieurs commutateurs dans le réseau.

### Importance de la LAG avec Port Monitoring :

- Dans un contexte LAG (Link Aggregation Group), le monitoring de port peut s'avérer complexe, car le trafic peut être réparti sur plusieurs liaisons physiques.
- La configuration correcte du port monitoring dans un environnement LAG est cruciale pour garantir que tout le trafic, réparti entre les liens agrégés, est capturé pour l'analyse.
- Cela assure que les données capturées pour la surveillance ou le dépannage sont complètes et représentatives du trafic réseau réel.

La diapositive illustre visuellement comment la surveillance de port peut être configurée dans un environnement réseau qui utilise la LAG. Cela inclut le monitoring du trafic à la fois sur le plan local (SPAN) et à travers le réseau (RSPAN), offrant aux administrateurs réseau la flexibilité nécessaire pour surveiller efficacement et diagnostiquer les problèmes sur un réseau étendu.

- Atelier



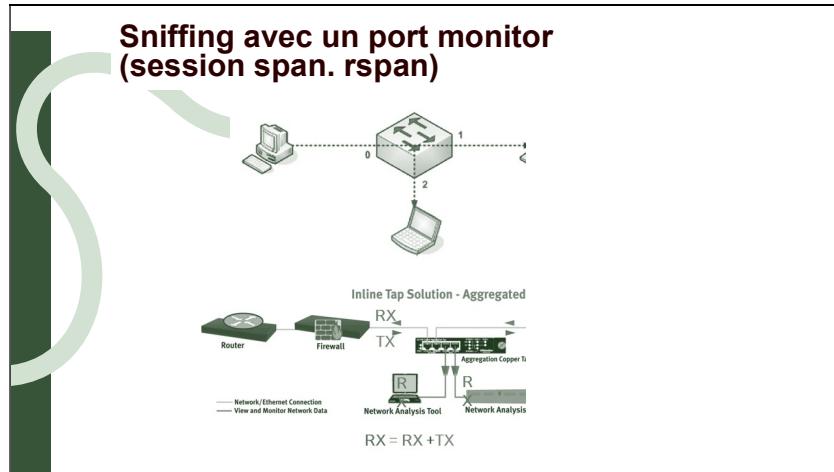
**ATELIER 5**

**Activité**

— **Objectif :**

- ▶ Paramétriser des liens LAG 802.3ad entre des switch

— **Enoncé : voir livret d'ateliers**



### SPAN alias Session Monitor

#### Qu'est-ce que SPAN ?

- SPAN, ou Switched Port Analyzer, est une fonction de surveillance du réseau qui permet de copier le trafic traversant un ou plusieurs ports sélectionnés (ou VLANs) et de l'envoyer vers un port spécifique pour analyse.

#### Configuration Typique :

- Dans la configuration présentée, il y a un commutateur central avec trois ports. Les ports 0 et 1 sont utilisés par les ordinateurs pour le trafic réseau normal.
- Le port 2 est configuré comme un port de destination SPAN. Un appareil d'analyse de réseau, comme un ordinateur portable avec un logiciel de capture de paquets, est connecté à ce port.

#### Fonctionnement de la Session SPAN :

- Le trafic entrant et/ou sortant des ports 0 et 1 est répliqué au port 2. Le réglage de la session SPAN peut être ajusté pour sélectionner le trafic d'intérêt - par exemple, uniquement le trafic entrant, sortant, ou les deux.
- L'appareil connecté au port de destination SPAN reçoit une copie exacte du trafic passant par les ports surveillés, permettant aux administrateurs de réseau d'observer le trafic en temps réel sans interrompre le flux de données.
- Cette technique est souvent utilisée pour le dépannage du réseau, la surveillance de la sécurité, et l'évaluation des performances du réseau.

#### Avantages de SPAN :

- **Non-intrusif** : SPAN ne perturbe pas le trafic réseau car il ne fait que copier les données vers le port de surveillance.
- **Flexibilité** : Les administrateurs peuvent choisir spécifiquement quels ports surveiller, permettant une analyse ciblée.
- **Analyse en Temps Réel** : Les données sont transmises en temps réel au port de surveillance, permettant une réaction immédiate aux problèmes détectés.

#### Considérations :

- Il est crucial de s'assurer que l'appareil d'analyse a la capacité de traiter le volume de trafic répliqué.
- La configuration de SPAN doit être gérée soigneusement pour éviter toute saturation du port de destination avec trop de trafic, ce qui pourrait entraîner la perte de paquets.
- La diapositive illustre de manière concise le concept de SPAN, un outil indispensable pour la gestion et la surveillance des réseaux modernes.



## **Sniffing avec un port monitor (session span. rspan)**

- Syntaxe de création d'une session monitor :

```
monitor session <numéro_session> source interface <interface_source> [both | rx | tx]
monitor session <numéro_session> destination interface <interface_destination>
```
- Syntaxe de visualisation de session monitor :

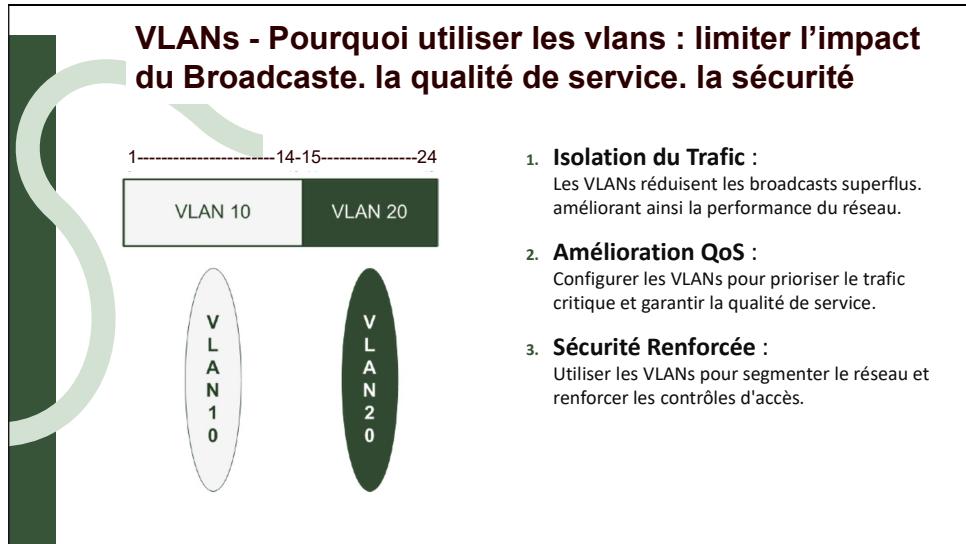
```
show monitor session [<numéro_session>]
```

### **CREATION D'UNE SESSION MONITOR:**

- <numéro\_session> : Le numéro de la session de monitoring que vous souhaitez créer.
- source interface <interface\_source> : L'interface source à partir de laquelle vous souhaitez copier le trafic. Vous pouvez spécifier plusieurs interfaces sources en séparant les interfaces par une virgule.
- [both | rx | tx] : Optionnel. Spécifie le sens du trafic à copier. "both" copie à la fois le trafic entrant et sortant. "rx" copie seulement le trafic entrant. "tx" copie seulement le trafic sortant.
- destination interface <interface\_destination> : L'interface de destination où vous souhaitez envoyer le trafic copié.

### **VISUALISATION DES SESSION MONITORS :**

<numéro\_session> : Optionnel. Si vous spécifiez un numéro de session. seules les informations concernant cette session seront affichées.



### L'Utilité des VLANs dans la Gestion du Réseau

Les réseaux locaux virtuels (VLANs) sont des subdivisions d'un réseau physique qui segmentent les réseaux en groupes plus petits basés sur des fonctions, des services, ou même des exigences de sécurité, plutôt que sur la localisation physique des dispositifs. Les VLANs sont des outils puissants pour la gestion de réseau, offrant des avantages significatifs en termes de performance, de qualité de service (QoS) et de sécurité.

#### Limitation de l'Impact des Broadcasts

• **Gestion des Broadcasts** : Dans un réseau non segmenté, les broadcasts atteignent tous les dispositifs, potentiellement saturant le réseau. Les VLANs limitent la portée de ces broadcasts au sein de leur domaine virtuel, réduisant le trafic inutile et améliorant la performance globale.

• **Optimisation des Ressources** : Moins de trafic broadcast signifie moins de charge sur les dispositifs réseau et les hôtes, optimisant l'utilisation des ressources.

#### Amélioration de la Qualité de Service

• **Priorisation du Trafic** : Les VLANs peuvent être configurés pour reconnaître et prioriser le trafic réseau essentiel, comme la voix sur IP (VoIP) ou les services de vidéoconférence.

• **Assurance de la Bande Passante** : En segmentant le réseau, les VLANs assurent que la bande passante critique est allouée de manière appropriée, améliorant l'expérience utilisateur pour des applications sensibles à la latence.

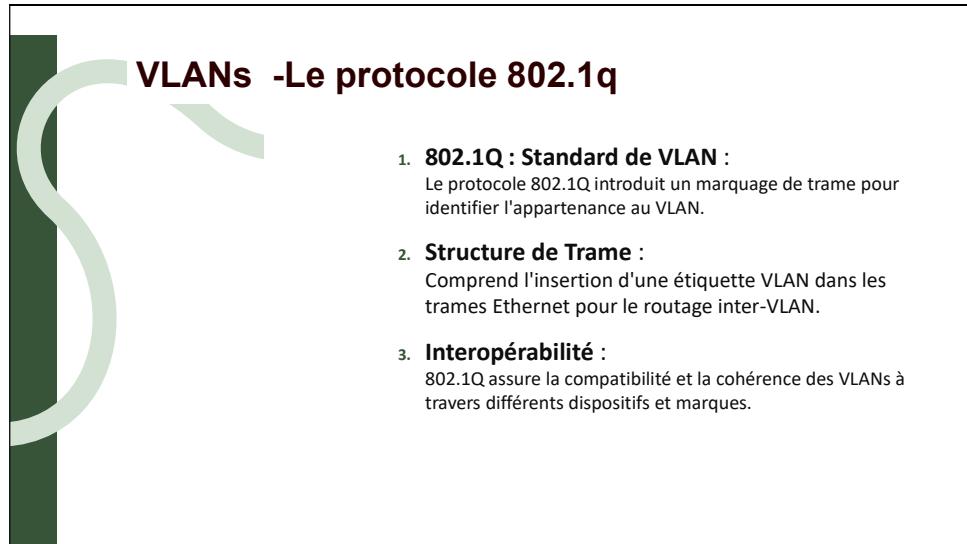
#### Renforcement de la Sécurité Réseau

• **Segmentation pour la Sécurité** : Les VLANs séparent les groupes d'utilisateurs ou les services qui n'ont pas besoin de communiquer directement, réduisant ainsi les vecteurs d'attaque et augmentant la sécurité.

• **Contrôles d'Accès** : Ils permettent la mise en place de politiques de sécurité plus strictes, où les règles d'accès au réseau peuvent être appliquées différemment en fonction du VLAN, empêchant les accès non autorisés.

#### Conclusion

L'utilisation des VLANs est une stratégie efficace pour les administrateurs réseau pour mieux gérer et contrôler le trafic au sein de leur infrastructure. Non seulement les VLANs peuvent améliorer la performance en limitant le trafic broadcast, mais ils jouent également un rôle crucial dans la mise en œuvre de la QoS et le renforcement de la sécurité. La mise en place de VLANs doit être réfléchie et alignée sur les objectifs et les politiques de l'organisation pour maximiser les avantages tout en maintenant un réseau robuste et sécurisé.



### Comprendre le Protocole 802.1q et le Marquage des Trames VLAN

Le protocole IEEE 802.1Q joue un rôle fondamental dans les réseaux modernes en permettant le marquage des trames Ethernet pour l'appartenance aux VLANs. Ce standard est crucial pour la gestion des VLANs dans des environnements de réseau étendus, facilitant le routage et la séparation du trafic entre différents segments de réseau.

#### La Structure Protocolaire de 802.1Q

• **Étiquette VLAN (VLAN Tag) :** L'élément clé introduit par 802.1Q est l'étiquette VLAN insérée dans les trames Ethernet. Cette étiquette se situe entre les champs d'adresse MACsource et le champ de type/longueur dans la trame originale. Elle contient plusieurs informations importantes :

- **VID (VLAN ID) :** Identifiant du VLAN qui permet de distinguer les trames appartenant à différents VLANs. Le VID peut varier de 1 à 4094, offrant une large gamme pour segmenter le réseau.
- **Priorité :** Un champ de priorité (PCP) qui peut être utilisé pour implémenter des mécanismes de Qualité de Service (QoS) en donnant la priorité à certaines trames sur d'autres.

• **Fonctionnement :** Lorsqu'une trame quitte un port marqué sur un switch, 802.1Q insère l'étiquette VLAN dans la trame. À l'arrivée sur un switch, l'étiquette est lue pour déterminer le VLAN auquel la trame appartient, et la trame est dirigée en conséquence. À la sortie du réseau VLAN, l'étiquette est retirée, et la trame est remise à son format original.

#### Rôle et Avantages du Protocole 802.1Q

Le protocole 802.1Q facilite le fonctionnement des VLANs en permettant :

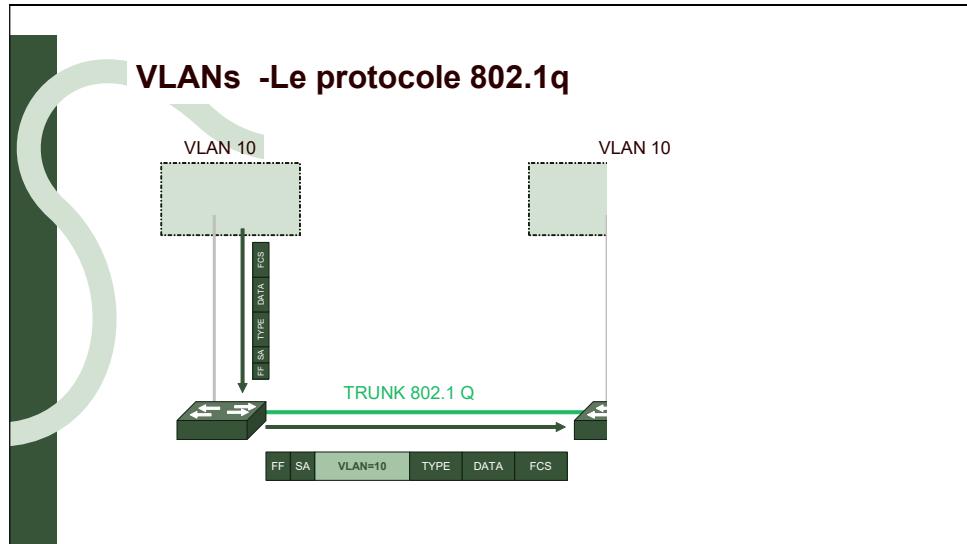
• **Routage Inter-VLAN :** La capacité à router le trafic entre différents VLANs sans nécessiter plusieurs interfaces physiques.

• **Économie de Bande Passante :** En limitant le Broadcast (ou diffusion) des trames aux ports appartenant au même VLAN.

• **Amélioration de la Sécurité :** En segmentant le trafic réseau, 802.1Q aide à isoler les segments sensibles et à réduire les risques de sécurité.

#### Conclusion

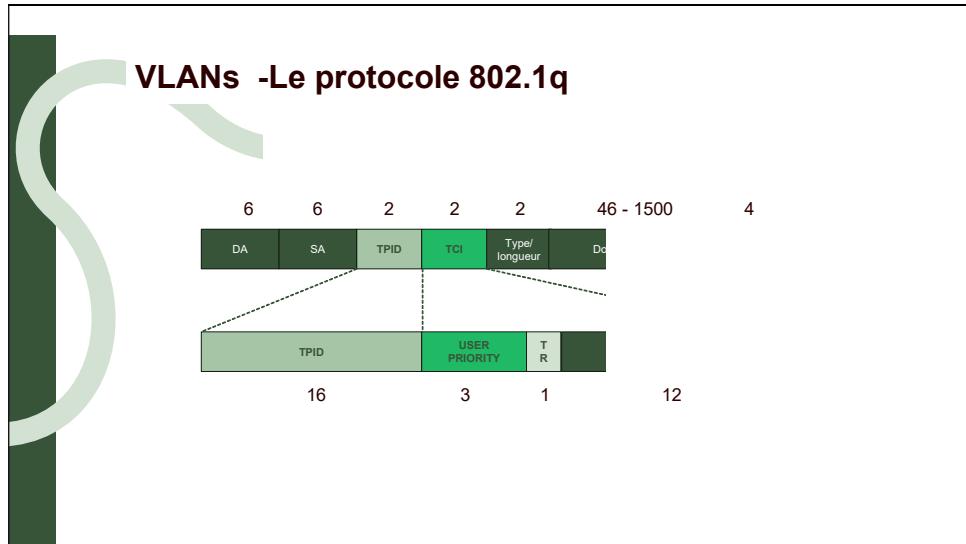
Le protocole 802.1Q est essentiel pour l'implémentation et la gestion efficace des VLANs dans les réseaux d'entreprise. En fournissant un mécanisme standardisé pour le marquage des trames VLAN, il permet une flexibilité, une sécurité et une efficacité accrues dans la gestion du trafic réseau.



Le protocole 802.1Q est un standard essentiel pour la mise en place et la gestion des réseaux VLANs (Virtual Local Area Networks). Son adoption permet une segmentation avancée du réseau, offrant ainsi plusieurs avantages significatifs en termes de performance, de sécurité et de gestion.

En utilisant le protocole 802.1Q, les administrateurs réseau peuvent diviser un réseau physique en plusieurs segments logiques, créant ainsi des VLANs distincts. Cette segmentation permet d'améliorer la sécurité en isolant différents groupes d'utilisateurs ou de ressources, tout en optimisant la bande passante et en facilitant la gestion du trafic. Une des principales caractéristiques du protocole 802.1Q est sa capacité à encapsuler les trames Ethernet avec des étiquettes VLAN, permettant ainsi le transport transparent des données VLAN à travers les réseaux physiques existants. Cette fonctionnalité, appelée "tagging", assure une interopérabilité garantie entre les équipements de différents fabricants, facilitant ainsi le déploiement et la maintenance des réseaux VLANs dans des environnements hétérogènes.

En résumé, le protocole 802.1Q est un élément clé dans la création de réseaux VLANs robustes et évolutifs. En adoptant ce standard, les administrateurs réseau peuvent bénéficier d'une segmentation efficace du réseau, d'une meilleure utilisation des ressources et d'une gestion simplifiée du trafic, contribuant ainsi à l'optimisation des performances et à la sécurité globale du réseau.



### Trame Ethernet et Tag VLAN :

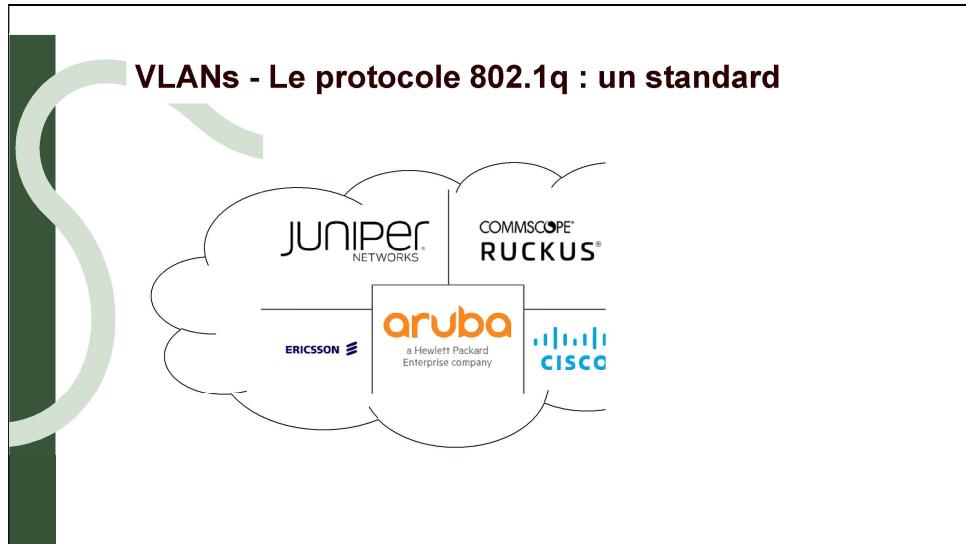
- Le protocole 802.1Q définit un mécanisme de tagging pour les trames Ethernet. permettant ainsi de multiplexer plusieurs VLANs sur un même lien physique.
- Cette technologie est cruciale pour la gestion de réseaux virtuels distincts au sein d'un réseau physique. permettant l'isolation. la sécurité et l'efficacité des ressources réseau.

### Composition d'une Trame Ethernet avec 802.1Q :

- **DA (Destination Address)** : Adresse MAC de destination. indiquant le destinataire de la trame.
- **SA (Source Address)** : Adresse MAC source. indiquant l'expéditeur de la trame.
- **TPID (Tag Protocol Identifier)** : Un champ de 2 octets qui indique la présence d'un tag VLAN. avec une valeur constante de 0x8100 pour 802.1Q.
- **TCI (Tag Control Information)** : Un champ de 2 octets qui contient des informations de contrôle pour le tag VLAN.
  - **USER PRIORITY** : 3 bits utilisés pour la classification du trafic (Quality of Service - QoS).
  - **CFI (Canonical Format Indicator)** : 1 bit utilisé pour la compatibilité entre les formats d'adresse MAC Ethernet et Token Ring.
  - **VLAN ID** : 12 bits qui identifient le VLAN auquel la trame appartient.
- **Type/Longueur** : Indique le type de protocole de niveau supérieur encapsulé dans la trame ou la longueur de la charge utile.
- **Données / 802.2** : La charge utile de la trame. qui peut contenir des données pour différents protocoles de niveau supérieur.
- **FCS (Frame Check Sequence)** : Un champ de 4 octets utilisé pour la détection d'erreurs dans la trame.

**Importance du Tagging VLAN :**

- Le tagging VLAN permet à plusieurs réseaux virtuels de coexister sur un même commutateur ou sur le même lien physique sans risque d'interférence.
  - Il fournit une méthode pour contrôler la circulation du trafic entre les VLANs (isolation), tout en permettant la communication entre eux si nécessaire (inter-VLAN routing).
  - Les champs de priorité utilisateur offrent la possibilité de gérer la qualité de service (QoS) en priorisant certains types de trafic, ce qui est essentiel pour les applications critiques telles que la voix sur IP (VoIP) et la vidéoconférence.
- Cette trame est un élément fondamental des réseaux modernes, en particulier dans les environnements qui nécessitent une segmentation et une gestion de trafic avancées.



### Le Protocole 802.1Q et l'Industrie des Réseaux :

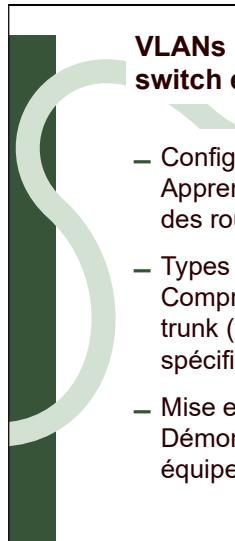
- Le protocole IEEE 802.1Q est le standard de l'industrie pour le tagging VLAN dans les environnements Ethernet. C'est une norme universellement acceptée qui facilite l'interopérabilité entre les équipements de différents fabricants.
- Comme l'indique la diapositive, des marques telles que Juniper Networks, CommScope Ruckus, Aruba Networks et Cisco Systems utilisent toutes ce protocole, ce qui garantit que les équipements de ces fabricants peuvent fonctionner ensemble dans un réseau VLAN mixte.

### Importance de l'Adoption d'un Standard :

- **Interopérabilité** : Grâce à un standard commun, les réseaux construits avec des équipements de différents fournisseurs peuvent fonctionner sans problème, permettant aux entreprises de choisir le meilleur matériel pour leurs besoins spécifiques sans se soucier de la compatibilité.
- **Simplification de la Gestion** : L'utilisation d'un standard unique pour le VLAN tagging simplifie la formation et la gestion des réseaux car les professionnels des réseaux n'ont besoin que de comprendre un seul système de tagging, quel que soit l'équipement utilisé.
- **Investissement Sécurisé** : L'adoption d'un standard par l'industrie signifie que les investissements dans l'infrastructure réseau seront protégés sur le long terme, car les standards ne changent pas aussi fréquemment que les technologies propriétaires.

### Conséquences pour les Architectures de Réseau :

- Les réseaux modernes tirent parti du protocole 802.1Q pour créer des architectures de réseau avancées, qui peuvent supporter plusieurs VLANs avec divers niveaux de service, politiques de sécurité et stratégies d'isolation.
- La cohérence entre les équipements permet une conception réseau plus flexible et plus robuste, où les décisions d'architecture peuvent être prises en fonction des besoins opérationnels plutôt que des contraintes techniques.



**VLANs - Paramétrage des VLANs sur les interfaces des switch et des routeurs (access, trunk ou tagged, untagged)**

- Configuration des Interfaces VLAN :  
Apprendre à configurer les VLANs sur les interfaces des switchs et des routeurs pour assurer la connectivité au sein du réseau.
- Types d'Interfaces :  
Comprendre les différences entre les interfaces access (untagged), trunk (tagged) . et comment les utiliser pour répondre aux besoins spécifiques du réseau.
- Mise en Pratique :  
Démonstration de la configuration des interfaces VLAN sur les équipements réseau pour illustrer les concepts présentés.

### **Paramétrage des VLANs sur les Interfaces des Switchs et des Routeurs**

La configuration des VLANs sur les interfaces des switchs et des routeurs est une étape essentielle pour assurer la connectivité et le routage du trafic entre les différents segments du réseau. Voici un aperçu des différents types d'interfaces VLAN et de leur configuration :

#### **Interfaces Access (Untagged)**

- Les interfaces access sont configurées pour appartenir à un seul VLAN spécifique. Elles sont utilisées pour connecter des périphériques individuels ou des ports de commutation à un VLAN spécifique.

#### **Interfaces Trunk (Tagged)**

- Les interfaces trunk sont utilisées pour transporter le trafic de plusieurs VLANs sur un seul lien physique. Les trames VLAN sont marquées (taggées) avec des identifiants VLAN pour indiquer à quel VLAN elles appartiennent.

#### **Configuration Pratique**

Lors de la configuration des interfaces VLAN, il est important de prendre en compte la topologie du réseau, les besoins en connectivité et les politiques de sécurité. Les administrateurs réseau doivent s'assurer que chaque interface est correctement configurée pour son rôle spécifique dans le réseau.

#### **Conclusion**

La configuration des VLANs sur les interfaces des switchs et des routeurs est une compétence fondamentale pour les administrateurs réseau. En comprenant les différents types d'interfaces VLAN et leur configuration appropriée, les professionnels réseau peuvent créer des environnements réseau flexibles, sécurisés et efficaces qui répondent aux besoins de leur organisation.



**VLANs - Paramétrage des VLANs sur les interfaces des switchs et des routeurs (access, trunk ou tagged, untagged)**

- Access :
  - ▶ Généralement, port d'extrémité relié à des stations, des serveurs ou des téléphones IP
  - ▶ Les trames ne sont pas « taguées »
  - ▶ Un seul VLAN associé à ce type de port
- Trunk :
  - ▶ Accepte des trames taguées et des trames non taguées grâce au VLAN natif
  - ▶ Plusieurs VLANs peuvent être associés à ce type de port du fait du protocole DTP
- Hybrid :
  - ▶ Supporte les deux modes
  - ▶ C'est la connexion et la configuration qui détermineront le mode de fonctionnement

### 1. Access (Accès) :

- **Définition** : Un port configuré en mode accès est destiné à la connexion d'un seul appareil, tel qu'un ordinateur, un serveur, ou un téléphone IP.
- **Fonctionnement** : Les trames qui passent par un port d'accès ne portent pas d'information de tag VLAN (elles ne sont pas « taguées »).
- **Utilisation** : Un seul VLAN est configuré sur le port d'accès. L'appareil connecté au port fait partie de ce VLAN spécifique et n'a pas conscience des tags VLAN.

### 2. Trunk (Tronc) :

- **Définition** : Un port trunk est utilisé pour passer plusieurs VLANs sur un seul lien physique entre deux commutateurs ou entre un commutateur et un routeur.
- **Fonctionnement** : Il peut transporter à la fois des trames taguées et non taguées. Les trames pour le VLAN natif passent non taguées, tandis que les trames pour les autres VLANs sont taguées avec leur VLAN ID respectif.
- **DTP (Dynamic Trunking Protocol)** : Un protocole qui négocie automatiquement entre les ports pour établir s'ils doivent être en mode accès ou trunk.

### 3. Hybrid (Hybride) :

- **Définition** : Les ports hybrides sont capables de fonctionner à la fois en mode accès et trunk, selon la configuration et les besoins.
- **Fonctionnement** : Ils peuvent être configurés pour supporter des trames taguées pour certains VLANs et non taguées pour d'autres.
- **Configuration** : Le mode de fonctionnement d'un port hybride dépend de la manière dont il est configuré et de la nature du trafic qu'il reçoit.



**VLANs - Paramétrage des vlans sur les interfaces des switch et des routeurs (access, trunk ou tagged, untagged)**

– Syntaxe de paramétrage d'un port access :

```
interface <nom_interface>
switchport mode access
switchport nonegotiate
switchport access vlan
<número_VLAN>
```

– Syntaxe de paramétrage d'un port trunk :

```
interface <nom_interface>
switchport mode trunk
switchport nonegotiate
```

**PORT ACCESS :**

- **interface <nom\_interface>** : Cette commande vous place dans le mode de configuration de l'interface spécifiée. Par exemple, pour configurer l'interface GigabitEthernet0/1, vous utiliserez interface GigabitEthernet0/1.
- **switchport mode access** : Cette commande configure le port en mode access, ce qui signifie qu'il ne transporte que le trafic d'un seul VLAN et ne peut pas être utilisé pour les trames VLAN (trunking).
- **switchport nonegotiate** : Cette commande désactive la négociation automatique des paramètres de vitesse et de duplex sur le port. Cela signifie que vous devrez spécifier manuellement ces paramètres pour le port.
- **switchport access vlan <número\_VLAN>** : Cette commande attribue le port au VLAN spécifié par <número\_VLAN>. Tout le trafic sur ce port sera associé à ce VLAN.

**PORT TRUNK :**

- **interface <nom\_interface>** : Cette commande vous place dans le mode de configuration de l'interface spécifiée. Par exemple, pour configurer l'interface GigabitEthernet0/1, vous utiliserez interface GigabitEthernet0/1.
- **switchport mode trunk** : Cette commande configure le port en mode trunk, ce qui signifie qu'il peut transporter plusieurs VLAN.
- **switchport nonegotiate** : Cette commande désactive la négociation automatique des paramètres de vitesse et de duplex sur le port. Cela signifie que vous devrez spécifier manuellement ces paramètres pour le port.

## • Atelier



**ATELIER 6**

**Activité**

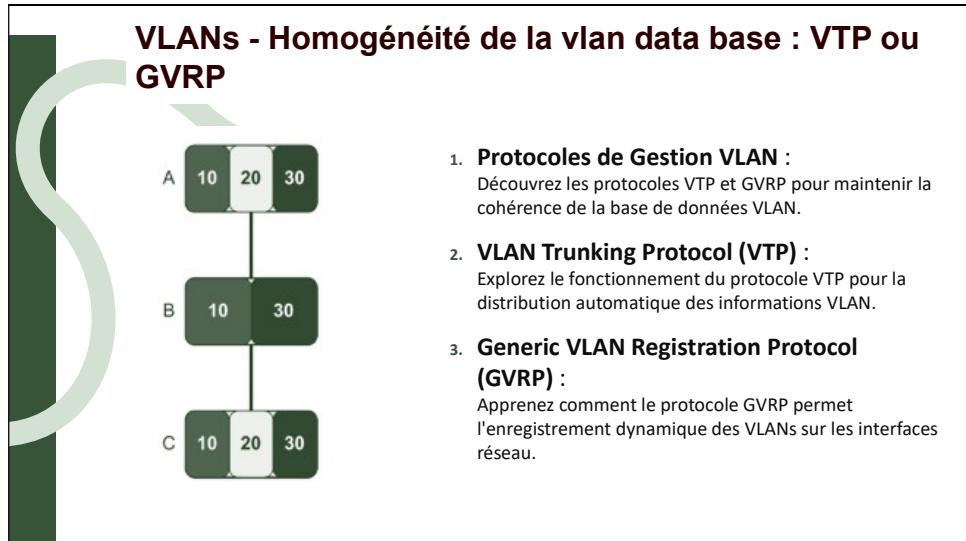
– Objectifs :

- Affectation des vlan aux interfaces Fa
- Paramétrage interface Gi en trunck

– Enoncé : voir livret d'ateliers

**Visualizations :**

```
show vlan  
show interface status  
show int gi 0/1
```



### Homogénéité de la Base de Données VLAN avec VTP et GVRP

La gestion des VLANs à l'échelle d'un réseau étendu peut être simplifiée grâce à l'utilisation de protocoles spécifiques. Voici un aperçu des protocoles VTP et GVRP :

#### VLAN Trunking Protocol (VTP)

• Le protocole VTP permet la distribution automatique des informations VLAN à travers un réseau. Les modifications apportées à la base de données VLAN sur un commutateur activant la fonction VTP serveur, sont propagées aux autres commutateurs du domaine VTP.

#### Generic VLAN Registration Protocol (GVRP)

• Le protocole GVRP permet l'enregistrement dynamique des VLANs sur les interfaces réseau. Lorsqu'un commutateur reçoit des trames VLAN inconnues, il peut demander dynamiquement des informations sur ces VLANs aux autres commutateurs du réseau.

#### Application Pratique

L'utilisation de protocoles de gestion VLAN tels que VTP ou GVRP peut simplifier la configuration et la maintenance des VLANs sur de grands réseaux. Les administrateurs réseau doivent comprendre les avantages et les limitations de chaque protocole pour choisir celui qui convient le mieux à leur environnement.

#### Conclusion

En compréhension des principes de fonctionnement des protocoles VTP et GVRP, les administrateurs réseau peuvent maintenir une base de données VLAN cohérente et éviter les erreurs de configuration. Ces protocoles offrent une gestion centralisée et automatisée des VLANs, ce qui permet de simplifier les opérations de réseau à grande échelle.



## VLANs - Homogénéité de la vlan data base : VTP ou GVRP

- Syntaxe de création d'un serveur VTP :

```
vtp mode server
vtp domain
<nom_du_domaine>
vtp password
<mot_de_passe>
```
- Syntaxe de création d'un serveur VTP :

```
vtp mode client
vtp domain
<nom_du_domaine>
vtp password
<mot_de_passe>
```

### VTP (VLAN Trunking Protocol) :

- VTP est un protocole Cisco qui permet de simplifier la gestion des mises à jour de VLAN dans un réseau étendu de commutateurs. Il assure l'homogénéité des VLANs en partageant les informations de configuration entre les commutateurs.
- Il existe trois modes de fonctionnement pour VTP : server, client, et transparent.

#### Configuration d'un Serveur VTP :

- **Mode Serveur** : Le commutateur en mode serveur peut créer, modifier et supprimer des VLANs pour le domaine VTP. Ces modifications sont ensuite propagées à tous les autres commutateurs dans le domaine VTP.

- vtp mode server : Cette commande configure le commutateur en mode serveur.
- vtp domain <nom\_du\_domaine> : Définit le nom du domaine VTP. Les commutateurs doivent partager le même nom de domaine VTP pour échanger des informations de VLAN.
- vtp password <mot\_de\_passe> : Configure un mot de passe pour le domaine VTP, ajoutant une couche de sécurité pour les mises à jour VTP.

#### Configuration d'un Client VTP :

- **Mode Client** : Un commutateur en mode client reçoit les informations du VLAN de serveurs VTP et les applique mais ne peut pas créer, modifier ou supprimer les VLANs dans le domaine VTP.

- vtp mode client : Configure le commutateur en mode client VTP.
- Les commandes vtp domain et vtp password sont utilisées de la même manière que pour le mode serveur pour assurer que le client et le serveur sont dans le même domaine VTP et sécurisés par le même mot de passe.

#### GVRP (Generic VLAN Registration Protocol) :

- GVRP est un standard de l'industrie, semblable à VTP, mais il est conçu pour l'interopérabilité entre les équipements de différents fabricants. Il permet la gestion dynamique de l'adhésion aux VLANs dans un environnement multi-fournisseurs.

## ● Atelier



## — Objectifs :

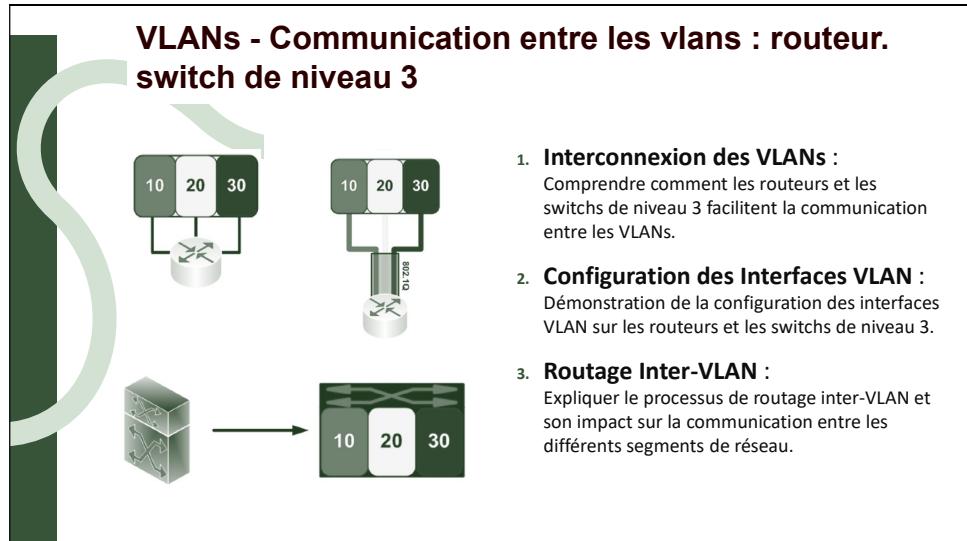
- Comprendre l'usage du VTP (VLAN Trunking Protocol).
- Configurer un switch en tant que serveur VTP.
- Configurer des switches en tant que clients VTP.
- Visualiser la configuration de VTP sur les switches.

► Enoncé : voir livret d'ateliers



## Démonstration

Sortis d'un switch server de production puis remis en production  
(écrasement de la base des vlans)



**Communication entre les VLANs : Configuration avec Routeurs et Switchs de Niveau 3**  
L'interconnexion des VLANs est essentielle pour permettre la communication entre différents groupes d'utilisateurs ou de périphériques sur un réseau. Cette fonctionnalité est réalisée en utilisant des routeurs ou des switchs de niveau 3 pour acheminer le trafic entre les différents VLANs.

### Configuration des Interfaces VLAN

• **Routeurs** : Les routeurs sont configurés avec des interfaces virtuelles (SVI - Switched Virtual Interfaces) pour chaque VLAN. Ces interfaces servent de passerelle par défaut pour les périphériques dans chaque VLAN, permettant le routage du trafic entre eux.

• **Switchs de Niveau 3** : Les switchs de niveau 3 sont des dispositifs qui combinent les fonctionnalités de commutation de couche 2 avec des fonctionnalités de routage de couche 3. Ils peuvent être configurés avec des interfaces VLAN pour le routage inter-VLAN.

### Routage Inter-VLAN

Le routage inter-VLAN est le processus de transfert du trafic entre différents VLANs via un routeur ou un switch de niveau 3. Lorsqu'un périphérique dans un VLAN souhaite communiquer avec un périphérique dans un autre VLAN, le trafic est dirigé vers le routeur ou le switch de niveau 3, qui achemine ensuite le trafic vers le VLAN de destination.

### Avantages de l'Interconnexion des VLANs

• **Sécurité Améliorée** : En limitant le trafic entre les VLANs, on peut renforcer la sécurité du réseau en isolant les segments sensibles.

• **Flexibilité et Gestion du Trafic** : Permet une segmentation efficace du trafic et une gestion flexible des ressources réseau.

• **Scalabilité** : Facilite l'extension du réseau en permettant l'ajout de nouveaux VLANs et en facilitant la communication entre eux.

### Conclusion

La configuration des routeurs et des switchs de niveau 3 pour permettre la communication entre les VLANs est un aspect crucial de la conception et de la gestion d'un réseau. En comprenant comment configurer et utiliser ces dispositifs, les administrateurs réseau peuvent créer des environnements réseau robustes et sécurisés qui répondent aux besoins de leur organisation.



## VLANs - Communication entre les VLANs : routeur. switch de niveau 3

- Syntaxe pour la configuration d'une sub-interface :

```
interface <interface_principale>.<numéro_subinterface>
encapsulation <type_encapsulation>
ip address <adresse_IP> <masque_de_sous-réseau>
```
- Syntaxe pour la création d'une interface svi :

```
interface Vlan<numéro_VLAN>
ip address <adresse_IP> <masque_de_sous-réseau>
```

### VLANs - Communication entre les VLANs : Routeur. Switch de niveau 3

Pour permettre la communication entre différents VLANs. il est nécessaire de mettre en place un routage inter-VLAN. Cela peut être réalisé en configurant des sous-interfaces sur un routeur ou en utilisant des interfaces SVI (Switched Virtual Interfaces) sur un commutateur de niveau 3.

#### 1. Configuration d'une Sub-interface :

• **But** : Sur un routeur. chaque sub-interface représente un VLAN différent. La sub-interface traite le trafic pour un seul VLAN.

##### • **Syntaxe :**

- `interface <interface_principale>.<numéro_subinterface>` : Crée une sub-interface sur l'interface physique du routeur. Le `<numéro_subinterface>` est généralement associé à l'ID VLAN.
- `encapsulation <type_encapsulation>` : Définit le type d'encapsulation VLAN. souvent dot1Q. suivi de l'ID VLAN.
- `ip address <adresse_IP> <masque_de_sous-réseau>` : Attribue une adresse IP et un masque de sous-réseau à la sub-interface. qui servira de passerelle par défaut pour le VLAN correspondant.

#### 2. Création d'une Interface SVI :

• **But** : Sur un commutateur de niveau 3. une SVI est créée pour chaque VLAN afin de permettre le routage entre eux.

##### • **Syntaxe :**

- `interface Vlan<numéro_VLAN>` : Initialise l'interface SVI pour le VLAN spécifié par `<numéro_VLAN>`.
- `ip address <adresse_IP> <masque_de_sous-réseau>` : Configure l'adresse IP et le masque pour l'interface SVI. qui agit comme la passerelle par défaut pour tous les appareils du VLAN.

## ● Ateliers



**ATELIER 8**

Activité

- Objectif : Mise en place d'un routeur pour le routage inter Vlans
- Enoncé : voir livret d'ateliers



**ATELIER 9**

Activité

- Objectif : Dépannage à partir d'un maquette réseau sur un émulateur
- Enoncé : voir livret d'ateliers

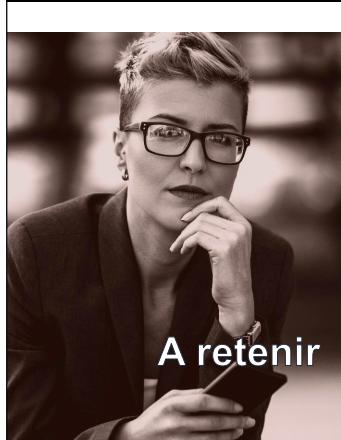


**ATELIER 10**

Activité

- Objectif : Comprendre et à résoudre des problèmes de routage dans un réseau interconnecté.  
L'exercice se concentre sur l'identification des problèmes liés au routage inter-VLAN et la compréhension de l'importance des configurations de routage sur les périphériques réseau.
- Enoncé : voir livret d'ateliers

- Ce qu'il faut retenir



- **Cœur de la Performance Réseau : La Commutation Ethernet**
- **Auto-apprentissage et Dynamisme des Switchs Ethernet**
- **Prévention des Boucles de Réseau avec STP**
- **Séparation et Gestion du Trafic avec les VLANs**
- **Augmentation de la Capacité Réseau avec l'Agrégation de Liens**

**Cœur de la Performance Réseau : La Commutation Ethernet :**

"La commutation Ethernet optimise la distribution des données au sein d'un réseau en dirigeant le trafic de manière intelligente pour éviter les congestions et maximiser la bande passante."

**Auto-apprentissage et Dynamisme des Switchs Ethernet :**

"Les switchs Ethernet utilisent l'auto-apprentissage pour mémoriser les adresses MAC des appareils connectés. permettant une commutation efficace et dynamique du trafic réseau."

**Prévention des Boucles de Réseau avec STP :**

"Les protocoles comme le Spanning Tree Protocol (STP) sont essentiels pour prévenir les boucles de réseau. garantissant ainsi la fiabilité et la stabilité des réseaux Ethernet étendus."

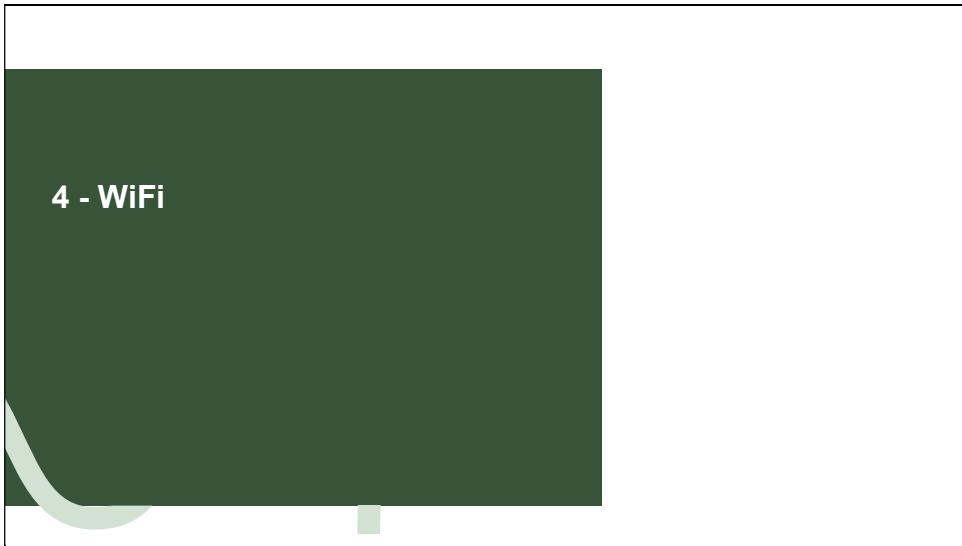
**Séparation et Gestion du Trafic avec les VLANs :**

"Les VLANs (Virtual Local Area Networks) permettent de segmenter les réseaux Ethernet en sous-groupes logiques pour une meilleure gestion du trafic. de la sécurité et de la performance réseau."

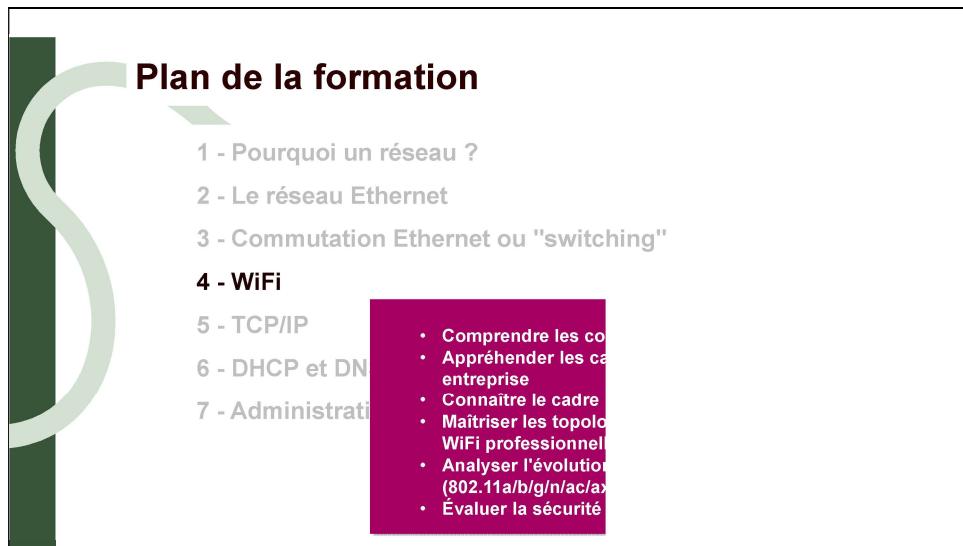
**Augmentation de la Capacité Réseau avec l'Agrégation de Liens :**

"L'agrégation de liens. ou Link Aggregation. augmente la capacité et la fiabilité du réseau en combinant plusieurs liaisons physiques en une seule connexion logique de plus grande capacité."

## Chapitre 4 - Wifi



- Objectifs du chapitre



The slide features a large stylized letter 'S' on the left side. The title 'Plan de la formation' is at the top. A vertical list of topics follows, with the last five items highlighted in a pink box:

- 1 - Pourquoi un réseau ?
- 2 - Le réseau Ethernet
- 3 - Commutation Ethernet ou "switching"
- 4 - WiFi
- 5 - TCP/IP
- 6 - DHCP et DNS
- 7 - Administration

- Comprendre les concepts fondamentaux du WiFi
- Appréhender les cas d'utilisation du WiFi en entreprise
- Connaître le cadre réglementaire du WiFi en France
- Maîtriser les topologies et architectures de bornes WiFi professionnelles
- Analyser l'évolution des normes WiFi (802.11a/b/g/n/ac/ax)
- Évaluer la sécurité des réseaux WiFi

Voici les principaux objectifs du chapitre sur le WiFi :

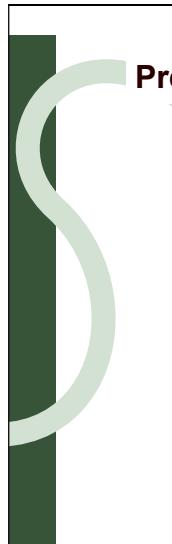
- Comprendre les concepts fondamentaux du WiFi :
  - Comprendre la différence entre les réseaux sans-fil et les réseaux filaires.
  - Définir les termes essentiels tels que WLAN. SSID. BSSID. canaux (OFDM. OFDMA. DSSS). puissance en dB. PIRE et CSMA/CA.
- Appréhender les cas d'utilisation du WiFi en entreprise :
  - Explorer les différents scénarios d'utilisation du WiFi dans un environnement professionnel.
- Connaître le cadre réglementaire du WiFi en France :
  - Comprendre les règles et les limitations de puissance pour les équipements WiFi en intérieur et en extérieur.
- Maîtriser les topologies et architectures de bornes WiFi professionnelles :
  - Apprendre les différentes configurations et architectures utilisées pour déployer des réseaux WiFi professionnels.
- Analyser l'évolution des normes WiFi (802.11a/b/g/n/ac/ax) :
  - Comparer les différentes normes en termes de débit. de couverture. de pénétration des matériaux et de sensibilité aux perturbations.
- Évaluer la sécurité des réseaux WiFi :
  - Comparer les protocoles de sécurité WiFi tels que WEP. WPA. WPA2 et WPA3. ainsi que les modes de sécurité Home (PSK) et Enterprise (802.1X).

En couvrant ces objectifs. les stagiaires seront en mesure de comprendre les principes fondamentaux du WiFi. son fonctionnement. ses applications en entreprise. ainsi que les normes et protocoles associés à la sécurité et à la performance des réseaux WiFi.



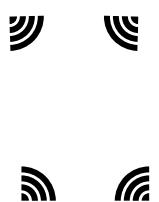
- Pouvez-vous partager une expérience où vous avez utilisé un réseau WiFi dans un environnement professionnel ou personnel ? Quels ont été les avantages et les inconvénients de cette expérience ?
- Comment pensez-vous que le WiFi pourrait améliorer la productivité dans un bureau moderne ? Avez-vous déjà rencontré des situations où un réseau sans-fil aurait été particulièrement utile ?
- Connaissez-vous les différentes normes WiFi telles que 802.11a/b/g/n/ac/ax ? Comment pensez-vous qu'elles se comparent en termes de performances et de couverture ?
- Pouvez-vous expliquer ce que vous savez sur la sécurité des réseaux WiFi ? Avez-vous déjà pris des mesures spécifiques pour sécuriser un réseau sans-fil ?
- À votre avis, quelles pourraient être les limitations ou les défis associés à la mise en place d'un réseau WiFi dans un environnement professionnel complexe, comme un grand bureau ou un entrepôt ?

- Pouvez-vous partager une expérience où vous avez utilisé un réseau WiFi dans un environnement professionnel ou personnel ? Quels ont été les avantages et les inconvénients de cette expérience ?
- Comment pensez-vous que le WiFi pourrait améliorer la productivité dans un bureau moderne ? Avez-vous déjà rencontré des situations où un réseau sans-fil aurait été particulièrement utile ?
- Connaissez-vous les différentes normes WiFi telles que 802.11a/b/g/n/ac/ax ? Comment pensez-vous qu'elles se comparent en termes de performances et de couverture ?
- Pouvez-vous expliquer ce que vous savez sur la sécurité des réseaux WiFi ? Avez-vous déjà pris des mesures spécifiques pour sécuriser un réseau sans-fil ?
- À votre avis, quelles pourraient être les limitations ou les défis associés à la mise en place d'un réseau WiFi dans un environnement professionnel complexe, comme un grand bureau ou un entrepôt ?



## Présentation du wlan

- 1. **WLAN** : Fondation des Communications Modernes
- 2. **Évolution des Réseaux** : Du Fil au Sans-fil
- 3. **Importance Actuelle** : WLAN dans le Tissu Numérique

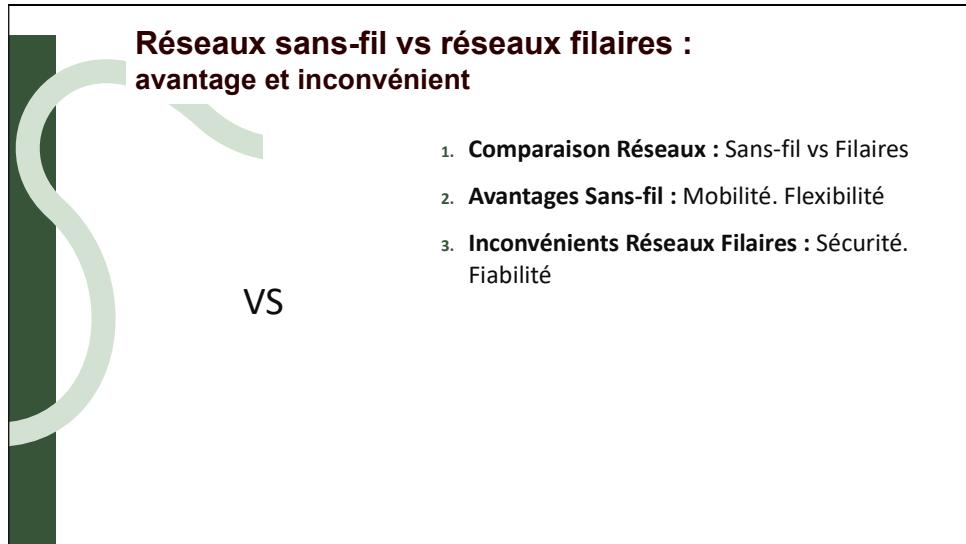


### Principes de base et évolution des réseaux : Découverte du WLAN

Le Wireless Local Area Network (WLAN), ou réseau local sans fil, constitue un pilier essentiel des technologies de communication contemporaines. À mesure que les réseaux évoluent, le WLAN devient de plus en plus omniprésent, offrant une connectivité sans fil fiable et flexible dans divers contextes.

Cette évolution des réseaux, passant des connexions filaires traditionnelles aux réseaux sans fil, reflète les besoins croissants en mobilité, en flexibilité et en connectivité omniprésente. Ainsi, le WLAN joue un rôle central dans la transformation numérique en cours, permettant aux utilisateurs de rester connectés et productifs où qu'ils soient.

Comprendre les principes de base du WLAN est donc essentiel pour naviguer efficacement dans le paysage des communications modernes. Ce chapitre nous plongera dans les fondements du WLAN, explorant son fonctionnement, son évolution et son importance dans les technologies de réseau actuelles.



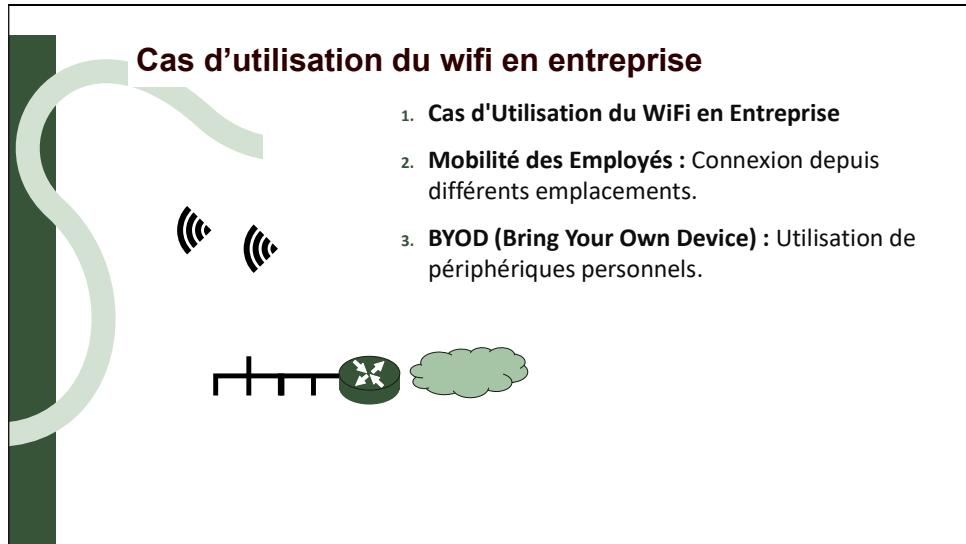
### Réseaux sans-fil vs réseaux filaires : Comparaison et Applications

Les réseaux sans-fil offrent une grande liberté de mouvement et une flexibilité inégalée. Grâce à cette technologie, les utilisateurs peuvent se connecter à Internet ou à un réseau local sans être physiquement liés à un point d'accès. Cette mobilité est particulièrement bénéfique dans les environnements où les utilisateurs doivent se déplacer fréquemment, comme dans les bureaux modernes ou les campus universitaires. De plus, les réseaux sans-fil permettent une installation plus rapide et moins coûteuse que les réseaux filaires, car ils éliminent le besoin de câbles physiques.

Cependant, les réseaux sans-fil présentent également des inconvénients. L'un des principaux défis est la sécurité. Étant donné que les données sont transmises par des ondes radio, il existe un risque accru d'interception par des personnes non autorisées. De plus, les réseaux sans-fil peuvent être sujets à des interférences et des perturbations extérieures, ce qui peut entraîner des problèmes de connectivité et de performance.

En revanche, les réseaux filaires offrent une connexion stable et sécurisée. Les données sont transmises à travers des câbles physiques, ce qui réduit considérablement les risques d'interception ou d'interférence. De plus, les réseaux filaires sont généralement plus fiables et offrent des performances constantes, ce qui en fait un choix idéal pour les applications sensibles comme les systèmes de surveillance ou les transactions financières.

En résumé, le choix entre un réseau sans-fil et un réseau filaire dépend des besoins spécifiques de chaque organisation ou projet. Ce chapitre explorera en détail les avantages et les inconvénients de chaque technologie, ainsi que les meilleures pratiques pour leur déploiement dans différents contextes.



### Cas d'utilisation du wifi en entreprise

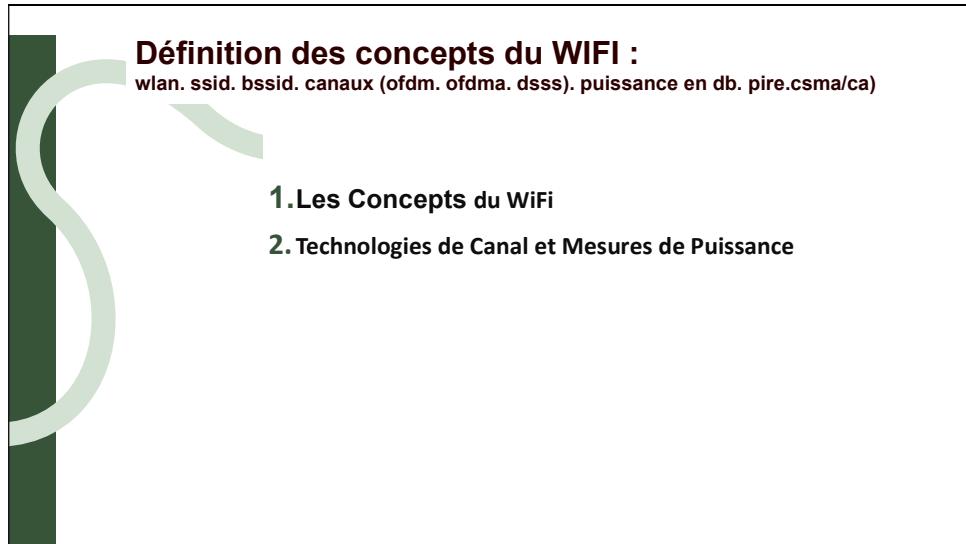
1. Cas d'Utilisation du WiFi en Entreprise
2. Mobilité des Employés : Connexion depuis différents emplacements.
3. BYOD (Bring Your Own Device) : Utilisation de périphériques personnels.

#### Cas d'Utilisation du WiFi en Entreprise : Pratiques et Déploiement

Dans un environnement professionnel, le WiFi joue un rôle crucial en offrant une connectivité flexible et mobile pour les employés. L'un des principaux cas d'utilisation est la mobilité des employés. En permettant aux employés de se connecter à Internet ou au réseau de l'entreprise depuis différents emplacements, le WiFi favorise la productivité en leur offrant un accès rapide et pratique aux ressources nécessaires à leur travail. Cela peut être particulièrement bénéfique dans les environnements de bureau modernes où les employés travaillent à partir de postes de travail flexibles ou de salles de réunion.

Un autre cas d'utilisation important du WiFi en entreprise est le BYOD (Bring Your Own Device). De nombreux employés préfèrent utiliser leurs propres appareils mobiles, tels que des smartphones ou des tablettes, pour effectuer leur travail. Le WiFi permet à ces appareils personnels de se connecter au réseau de l'entreprise de manière sécurisée, facilitant ainsi la collaboration et la communication entre les membres de l'équipe.

Il est essentiel pour les entreprises de mettre en œuvre les meilleures pratiques de déploiement du WiFi pour garantir une connectivité fiable et sécurisée. Cela comprend la conception d'un réseau WiFi robuste, la gestion efficace des canaux pour éviter les interférences, ainsi que la mise en place de mesures de sécurité telles que l'authentification et le cryptage des données. Ce chapitre explorera ces aspects en détail pour aider les entreprises à tirer le meilleur parti de leur infrastructure WiFi.



## Définition des concepts du WiFi :

wlan. ssid. bssid. canaux (ofdm. ofdma. dsss). puissance en db. pire.csma/ca)

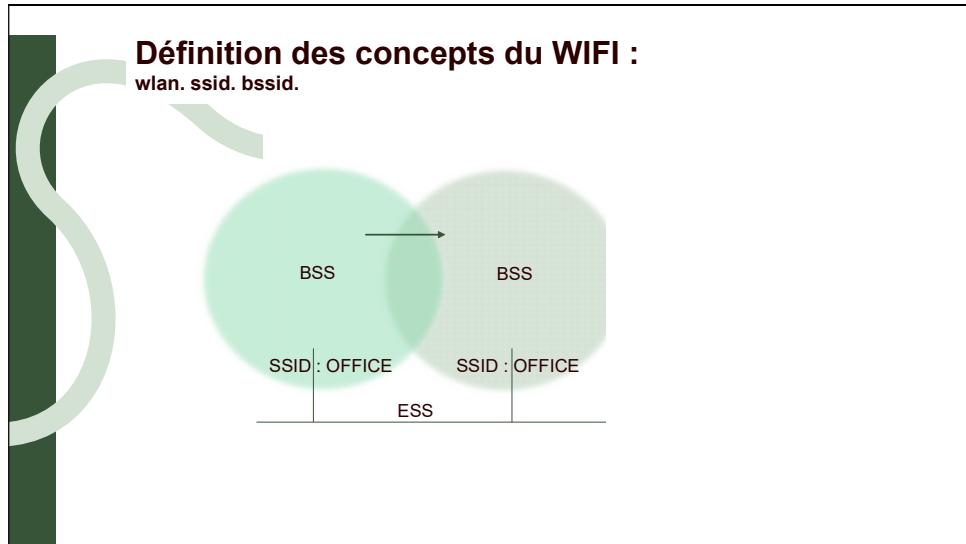
1. Les Concepts du WiFi
2. Technologies de Canal et Mesures de Puissance

### Définition des Concepts du WiFi :

Dans ce chapitre, nous explorerons les concepts fondamentaux du WiFi pour comprendre son fonctionnement et ses applications. Tout d'abord, le WLAN (Wireless Local Area Network) représente un réseau local sans fil qui permet aux dispositifs de communiquer entre eux et avec un réseau câblé.

Le SSID (Service Set Identifier) est un identifiant unique attribué à chaque réseau WiFi, permettant aux dispositifs de le reconnaître et de s'y connecter. Le BSSID (Basic Service Set Identifier) identifie de manière unique chaque point d'accès dans un réseau sans fil. Les technologies de canal, telles que OFDM (Orthogonal Frequency-Division Multiplexing), OFDMA (Orthogonal Frequency-Division Multiple Access) et DSSS (Direct Sequence Spread Spectrum), sont utilisées pour moduler et démoduler les signaux WiFi, permettant une transmission efficace des données sur des canaux sans fil.

En ce qui concerne les mesures de puissance, nous utiliserons les unités dB (décibels) et PIRE (Puissance Isotrope Rayonnée Équivalente) pour évaluer la force du signal WiFi. Plus la puissance est élevée, plus le signal est fort et peut atteindre de plus grandes distances. Enfin, le protocole CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) est utilisé dans les réseaux sans fil pour gérer l'accès au canal et éviter les collisions de données entre les dispositifs.

**•WLAN (Wireless Local Area Network) :**

- Il s'agit d'un réseau local qui permet aux appareils de se connecter et de communiquer sans fil. Un WLAN peut être composé de plusieurs composants, notamment des points d'accès et des contrôleurs WLAN.

**•SSID (Service Set Identifier) :**

- Le SSID est le nom d'un réseau sans fil. Lorsque vous scannez les réseaux Wi-Fi disponibles, les noms que vous voyez sont les SSIDs des différents réseaux. Il sert d'identifiant unique pour les utilisateurs qui souhaitent se connecter à un réseau WLAN particulier.

**•BSSID (Basic Service Set Identifier) :**

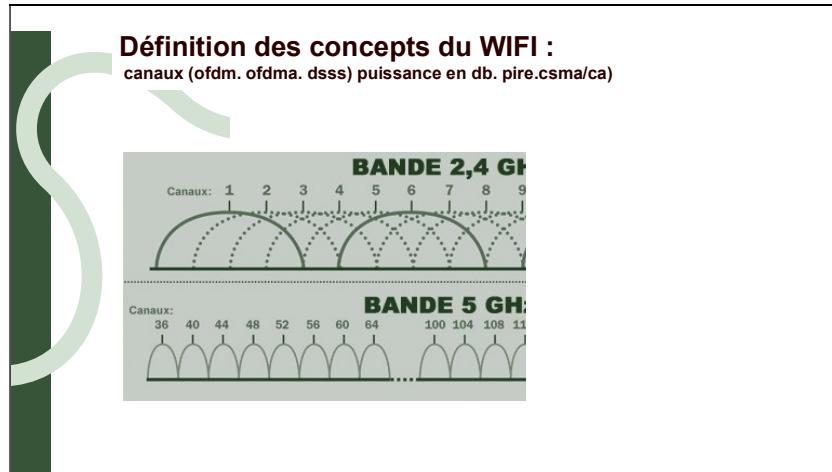
- Le BSSID est l'adresse MAC (Media Access Control) d'un point d'accès sans fil. Il sert à identifier de façon unique le point d'accès au sein d'un réseau WLAN. Un BSSID est à un réseau Wi-Fi ce qu'une adresse physique est à un réseau Ethernet.

**Structure du Réseau Wi-Fi :****•BSS (Basic Service Set) :**

- Un BSS est la zone de couverture de base fournie par un seul point d'accès Wi-Fi. Dans une configuration domestique ou de petite entreprise, un BSS peut suffire pour couvrir l'ensemble du réseau.

**•ESS (Extended Service Set) :**

- Un ESS est formé par plusieurs BSS qui partagent le même SSID. Dans un ESS, un utilisateur peut se déplacer d'un BSS à un autre de manière transparente (roaming), sans perdre la connectivité Wi-Fi.



#### Types de Canaux :

##### •OFDM (Orthogonal Frequency-Division Multiplexing) :

- OFDM est une technique de codage numérique utilisée dans les standards Wi-Fi comme 802.11a/g/n/ac. qui permet de transmettre plusieurs signaux sur une même bande de fréquence en les séparant en plusieurs sous-porteuses orthogonales. Cela réduit l'interférence et améliore l'efficacité du spectre.

##### •OFDMA (Orthogonal Frequency-Division Multiple Access) :

- Une évolution de l'OFDM. OFDMA. utilisée dans le Wi-Fi 6 (802.11ax). permet une utilisation encore plus efficace de la bande passante en divisant chaque sous-porteuse en slots pour permettre à plusieurs utilisateurs de les utiliser simultanément.

##### •DSSS (Direct-Sequence Spread Spectrum) :

- DSSS est une technique de modulation plus ancienne utilisée par les standards 802.11b pour répandre les signaux sur une large bande de fréquence. Cela augmente la résistance du signal aux interférences et au bruit.

#### Concepts de Puissance :

##### •Puissance en dB (Decibels) :

- La puissance du signal Wi-Fi est souvent mesurée en décibels (dB). une unité logarithmique qui décrit le rapport entre deux valeurs de puissance. En Wi-Fi. cela peut être exprimé en dBm. qui fait référence à la puissance par rapport à 1 milliwatt.

##### •PIRE (Puissance Isotrope Rayonnée Équivalente) :

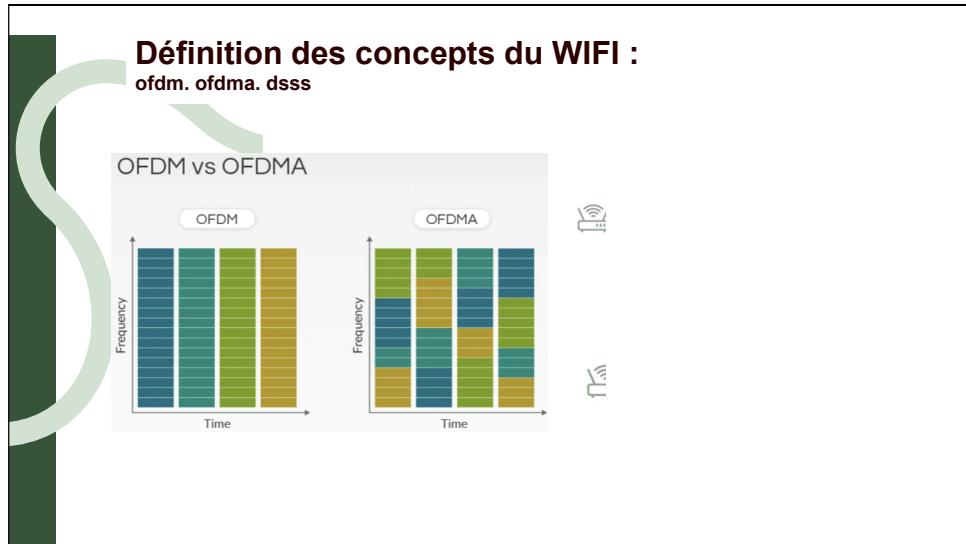
- La PIRE est une mesure de la puissance de l'émetteur en prenant en compte le gain de l'antenne. C'est la puissance qui serait rayonnée si l'antenne était parfaitement isotrope (rayonnant uniformément dans toutes les directions).

##### •CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) :

- CSMA/CA est un protocole de contrôle d'accès au média utilisé dans les réseaux Wi-Fi pour minimiser les collisions de données. Les appareils écoutent d'abord le canal pour s'assurer qu'il est libre avant de transmettre des données et utilisent des accusés de réception pour assurer la livraison des paquets.

#### Fréquences et Bandes :

- La diapositive montre également les bandes de fréquence de 2.4 GHz et 5 GHz. qui sont les plus utilisées dans les réseaux Wi-Fi domestiques et professionnels. Chaque bande a des canaux numérotés qui indiquent des segments spécifiques du spectre de fréquence.



- **OFDM (Orthogonal Frequency Division Multiplexing)** :
- **Principe** : OFDM est une technique de modulation qui divise le signal large bande en plusieurs sous-porteuses plus étroites qui sont orthogonales entre elles. Chaque sous-porteuse est modulée avec des données indépendantes. Cette technique permet de réduire les interférences entre les sous-porteuses et d'optimiser l'utilisation du spectre.
- **Avantages** : Résistance accrue aux interférences. efficacité spectrale élevée. meilleure tolérance aux distorsions du canal.
- **OFDMA (Orthogonal Frequency Division Multiple Access)** :
- **Principe** : Similaire à l'OFDM. mais avec la capacité d'accès multiple (multiple access). OFDMA permet à plusieurs utilisateurs d'accéder simultanément au spectre en attribuant différentes sous-porteuses à différents utilisateurs. Cela améliore l'efficacité et la capacité du réseau.
- **Avantages** : Partage efficace du spectre entre plusieurs utilisateurs. amélioration des performances dans les environnements à forte densité d'utilisateurs.
- **DSSS (Direct Sequence Spread Spectrum)** :
- **Principe** : DSSS étend le signal sur une largeur de bande plus large que nécessaire en utilisant une séquence pseudo-aléatoire (code spreading). Cette séquence est ensuite combinée avec les données à transmettre. Le signal résultant semble être du bruit pour tout autre récepteur qui ne possède pas la même séquence pseudo-aléatoire. mais peut être récupéré par le récepteur approprié.
- **Avantages** : Résistance aux interférences et aux attaques de brouillage. sécurité accrue grâce à la difficulté d'interception du signal.

Ces technologies sont toutes utilisées dans les réseaux Wi-Fi modernes pour optimiser les performances. la fiabilité et la sécurité des communications sans fil. donne moi des exemple dans le wifi

ChatGPT

Bien sûr ! Voici comment ces technologies sont utilisées dans les réseaux Wi-Fi :

- **OFDM (Orthogonal Frequency Division Multiplexing) :**
- Dans les réseaux Wi-Fi. l'OFDM est utilisé pour diviser la bande passante disponible en plusieurs canaux étroits. Par exemple. dans le Wi-Fi 5 (802.11ac). la bande passante est divisée en plusieurs canaux de 20. 40. 80 ou 160 MHz. selon les spécifications du réseau.
- Chaque canal est ensuite modulé avec des données indépendantes. ce qui permet d'optimiser l'utilisation du spectre et d'améliorer les performances du réseau. notamment en termes de débit de données et de robustesse face aux interférences.
- **OFDMA (Orthogonal Frequency Division Multiple Access) :**
- Le Wi-Fi 6 (802.11ax) utilise OFDMA pour permettre à plusieurs utilisateurs de partager efficacement la même bande passante. Dans ce cas. la bande passante est divisée en sous-porteuses qui sont attribuées à différents utilisateurs ou groupes d'utilisateurs.
- Par exemple. dans un environnement densément peuplé où plusieurs appareils Wi-Fi sont actifs simultanément. OFDMA permet à chaque appareil de transmettre et de recevoir des données de manière efficace. ce qui améliore les performances globales du réseau.
- **DSSS (Direct Sequence Spread Spectrum) :**
- Bien que moins couramment utilisé dans les réseaux Wi-Fi modernes. le DSSS était utilisé dans les normes plus anciennes telles que 802.11b. Dans DSSS. chaque bit de données est étendu en une séquence plus longue à l'aide d'un code de répartition pseudo-aléatoire.
- Cela rend le signal plus résistant aux interférences et aux attaques de brouillage. De plus. la largeur de bande étendue augmente également la résilience du signal aux problèmes de propagation dans les environnements sans fil



## Cadre réglementaire en France : puissance indoor et outdoor. pire

1. Cadre Réglementaire en France
2. Puissance des Signaux WiFi
3. Normes Indoor et Outdoor

### 1. Cadre Réglementaire en France :

- En France, l'Agence Nationale des Fréquences (ANFR) réglemente l'utilisation des bandes de fréquences et la puissance des émissions des équipements radio, y compris les réseaux Wi-Fi.
- La réglementation vise à minimiser les interférences entre les différents services radio et à protéger la santé publique contre les risques liés à l'exposition aux champs électromagnétiques.

### 2. Puissance des Signaux Wi-Fi :

- La puissance des émissions Wi-Fi est souvent limitée à des niveaux qui garantissent un équilibre entre une bonne couverture réseau et la minimisation des interférences avec d'autres appareils ou réseaux.
- La PIRE est la valeur de référence pour la limite de puissance des émissions radio en France, prenant en compte à la fois la puissance transmise par l'appareil et le gain de l'antenne.

### 3. Normes Indoor et Outdoor :

#### • Indoor :

- Pour les opérations en intérieur, les équipements Wi-Fi sont généralement limités à une PIRE plus faible, car les signaux ne doivent pas voyager de grandes distances et il y a moins de risque d'interférence avec d'autres réseaux.

#### • Outdoor :

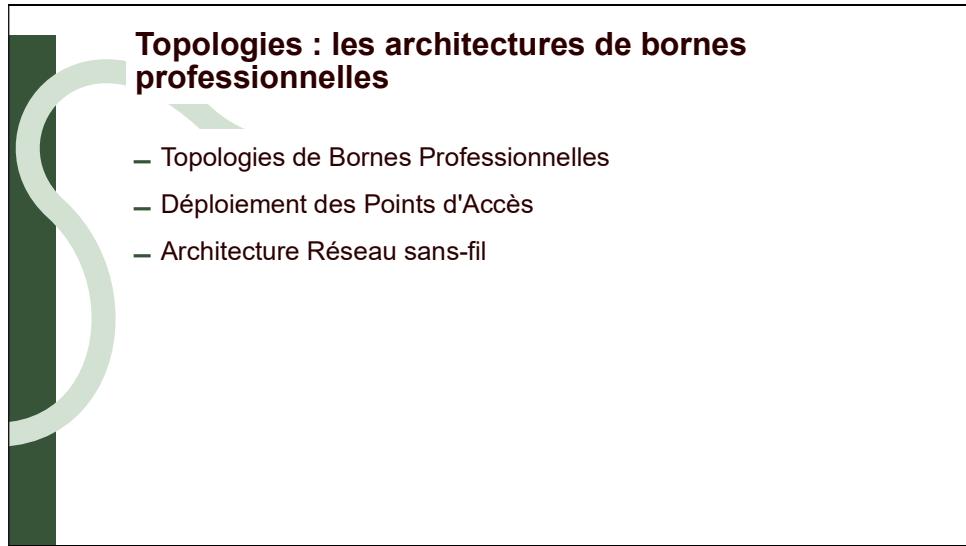
- En extérieur, la PIRE autorisée peut être plus élevée, car les signaux doivent souvent couvrir des distances plus grandes. Cependant, cela peut varier en fonction de la densité de population et de la proximité d'autres réseaux ou de services utilisant le spectre radio.

**Application Pratique :**

- Les installateurs de réseaux Wi-Fi et les ingénieurs doivent connaître le cadre réglementaire et les limites de PIRE pour la conception et le déploiement de réseaux Wi-Fi afin d'assurer la conformité avec la législation locale.
- La compréhension de ces limites est également essentielle pour éviter les sanctions réglementaires et pour garantir une cohabitation harmonieuse avec d'autres systèmes et services sans fil.

**Messages Clés**

- Respect des Normes Réglementaires** : Connaissance et respect du cadre réglementaire pour la mise en place de réseaux Wi-Fi en France.
- Gestion Optimisée de la Puissance** : Ajustement correct de la puissance des émissions pour une utilisation efficace et sûre du Wi-Fi.
- Conception Responsable de Réseau** : Création de réseaux Wi-Fi qui maximisent la couverture et les performances tout en minimisant l'impact sur les autres systèmes et la santé publique.



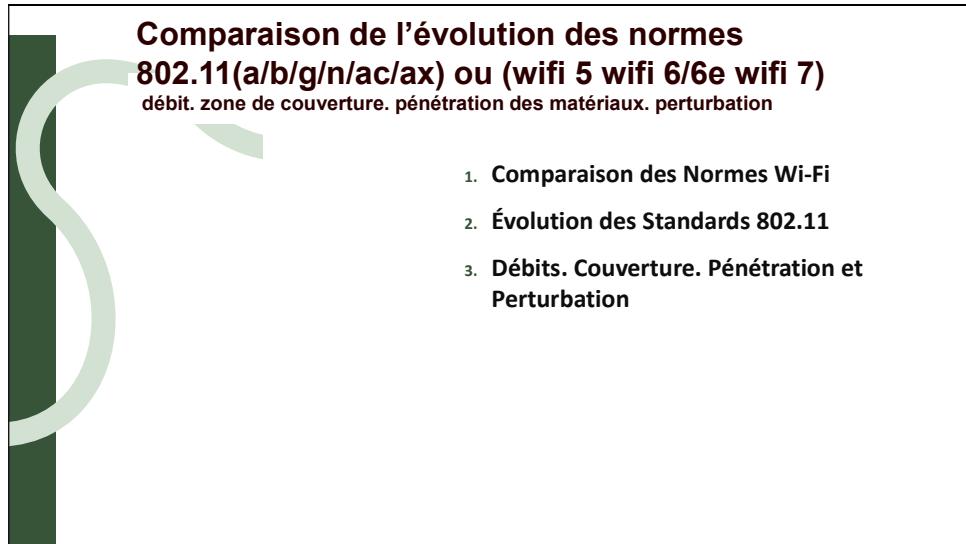
### Topologies des Bornes Professionnelles : Concepts et Applications

Les topologies de bornes professionnelles désignent les différentes configurations et agencements utilisés pour déployer des points d'accès sans-fil (AP) dans un environnement professionnel. Ces configurations sont conçues pour offrir une couverture Wi-Fi optimale et répondre aux besoins spécifiques des entreprises en termes de connectivité et de performance.

Les architectures de bornes professionnelles peuvent varier en fonction de divers facteurs, tels que la taille de l'entreprise, la densité des utilisateurs, les exigences en matière de sécurité et la complexité du réseau. Voici quelques-unes des topologies les plus couramment utilisées :

- **Topologie en Étoile** : Dans cette configuration, chaque point d'accès est connecté à un commutateur central ou à un contrôleur sans-fil. Cette topologie offre une gestion centralisée et simplifiée des AP, ce qui facilite la configuration, la surveillance et la maintenance du réseau sans-fil.
- **Topologie en Maille (Mesh)** : Dans cette configuration, les points d'accès sont interconnectés pour former un maillage de couverture sans-fil. Cette architecture est idéale pour les environnements étendus où il est difficile ou coûteux de tirer des câbles Ethernet. Elle offre également une redondance et une tolérance aux pannes accrues.
- **Topologie Hybride** : Cette configuration combine les avantages des topologies en étoile et en maille pour offrir une solution flexible et robuste. Elle peut inclure des points d'accès connectés à la fois en mode autonome et en mode contrôlé par un contrôleur sans-fil centralisé.

En comprenant les différentes topologies de bornes professionnelles, les entreprises peuvent choisir la configuration qui convient le mieux à leurs besoins spécifiques en matière de connectivité sans-fil, de performance et de gestion du réseau.



## Comparaison de l'évolution des normes 802.11(a/b/g/n/ac/ax) ou (wifi 5 wifi 6/6e wifi 7)

débit. zone de couverture. pénétration des matériaux. perturbation

1. Comparaison des Normes Wi-Fi
2. Évolution des Standards 802.11
3. Débits. Couverture. Pénétration et Perturbation

### Comparaison des Normes Wi-Fi : De l'802.11a au Wi-Fi 7

Les normes Wi-Fi, définies par les spécifications IEEE 802.11, ont connu une évolution significative au fil du temps pour répondre aux besoins croissants de connectivité sans-fil. Voici une comparaison des principales normes et de leur évolution :

#### •802.11a (Wi-Fi 1) :

- Débit : Jusqu'à 54 Mbps
- Zone de Couverture : Limitée, utilisant la bande de fréquence 5 GHz
- Pénétration des Matériaux : Faible, en raison de la haute fréquence
- Perturbations : Faibles, en raison de la disponibilité limitée de périphériques compatibles

#### •802.11b (Wi-Fi 2) :

- Débit : Jusqu'à 11 Mbps
- Zone de Couverture : Plus étendue que l'802.11a, utilisant la bande de fréquence 2.4 GHz
- Pénétration des Matériaux : Meilleure que l'802.11a, mais toujours limitée par la fréquence
- Perturbations : Plus élevées en raison de la bande de fréquence plus encombrée

#### •802.11g (Wi-Fi 3) :

- Débit : Jusqu'à 54 Mbps, compatible avec la bande de fréquence 2.4 GHz
- Zone de Couverture : Similaire à l'802.11b, mais avec des améliorations de débit
- Pénétration des Matériaux : Comparable à l'802.11b
- Perturbations : Similaires à l'802.11b en raison de la bande de fréquence partagée

#### •802.11n (Wi-Fi 4) :

- Débit : Jusqu'à plusieurs centaines de Mbps, utilisant la technologie MIMO
- Zone de Couverture : Étendue, grâce à des antennes multiples et à la compatibilité avec les bandes de fréquence 2.4 GHz et 5 GHz
- Pénétration des Matériaux : Améliorée grâce à la compatibilité avec la bande de fréquence 5 GHz
- Perturbations : Réduites grâce à la technologie MIMO et à la bande de fréquence 5 GHz

**802.11ac (Wi-Fi 5) :**

- Débit : Plusieurs gigabits par seconde. grâce à la technologie MIMO multi-utilisateur (MU-MIMO)
- Zone de Couverture : Étendue. avec une meilleure performance dans les environnements denses
- Pénétration des Matériaux : Améliorée par rapport à l'802.11n. en particulier dans la bande de fréquence 5 GHz
- Perturbations : Réduites grâce à MU-MIMO et à la bande de fréquence 5 GHz

**•802.11ax (Wi-Fi 6) :**

- Débit : Jusqu'à plusieurs gigabits par seconde. avec une efficacité accrue dans les environnements denses
- Zone de Couverture : Améliorée par rapport à l'802.11ac. avec une meilleure gestion du spectre
- Pénétration des Matériaux : Comparable à l'802.11ac
- Perturbations : Réduites grâce à une meilleure utilisation du spectre et à des techniques avancées de modulation

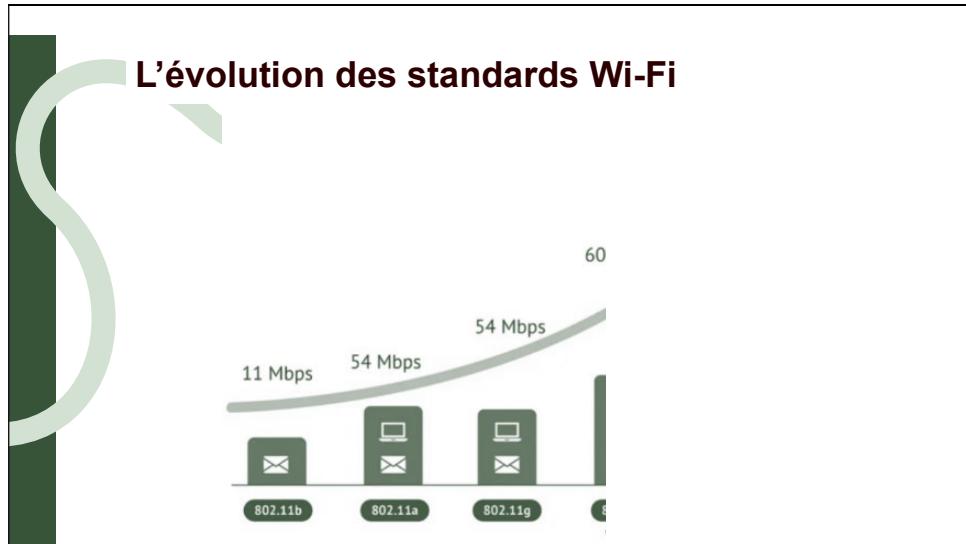
**•Wi-Fi 6E (Wi-Fi 6 Extended) :**

- Débit : Similaire à Wi-Fi 6. mais avec des canaux supplémentaires dans la bande de fréquence 6 GHz
- Zone de Couverture : Améliorée grâce à l'extension du spectre dans la bande de fréquence 6 GHz
- Pénétration des Matériaux : Comparable à Wi-Fi 6
- Perturbations : Réduites grâce à une bande de fréquence moins encombrée

**•Wi-Fi 7 (à venir) :**

- Débit : Attendu pour offrir des débits encore plus élevés. avec une efficacité accrue dans les environnements denses
- Zone de Couverture : Prévu pour étendre davantage la couverture et améliorer les performances dans les zones à forte densité d'appareils
- Pénétration des Matériaux : Les détails seront précisés avec le développement de la norme
- Perturbations : Les améliorations prévues incluent une meilleure gestion du spectre pour réduire les perturbations

En comprenant l'évolution des normes Wi-Fi. les entreprises peuvent prendre des décisions éclairées lors du déploiement de leur infrastructure sans-fil. en tenant compte des débits. de la couverture. de la pénétration des matériaux et de la résistance aux perturbations nécessaires à leurs besoins spécifiques.



### Évolution des Standards Wi-Fi

La technologie Wi-Fi a connu une série d'améliorations au fil des années, chaque nouvelle norme apportant des avancées en termes de vitesse, de fiabilité et d'efficacité.

#### •802.11b :

- Lancé en 1999, il offrait une vitesse maximale de 11 Mbps.
- Utilisait la bande de fréquence de 2.4 GHz.

#### •802.11a :

- Introduit également en 1999 avec des vitesses allant jusqu'à 54 Mbps.
- Opérait sur la bande de fréquence de 5 GHz.

#### •802.11g :

- Arrivé en 2003, combinant les meilleures caractéristiques des normes 802.11a et 802.11b.
- Vitesse maximale similaire à 802.11a, mais sur la bande de 2.4 GHz.

#### •802.11n (Wi-Fi 4) :

- Lancé en 2009, il a introduit la technologie MIMO (Multiple Input Multiple Output) et a augmenté les vitesses jusqu'à 600 Mbps.
- Fonctionnait sur les bandes de 2.4 GHz et 5 GHz.

#### •802.11ac (Wi-Fi 5) :

- Standardisé en 2014, cette norme a augmenté la performance maximale théorique jusqu'à environ 6.8 Gbps avec l'usage accru de la bande de 5 GHz et la modulation 256-QAM.

#### •802.11ax (Wi-Fi 6) :

- La dernière norme en date, aussi connue sous le nom de Wi-Fi 6 depuis 2019.
- Offre des vitesses pouvant atteindre 10 Gbps et améliore l'efficacité du réseau grâce à des technologies comme OFDMA et BSS Coloring.



Protocole IEEE 802.11	Date de sortie	Bandes de fréquence
802.11-1997	1997	2.4
11b	1999	2.4
11a	1999	5
11g	2003	2.4
11n (Wi-Fi 4)	2009	2.4/5
11ac (Wi-Fi 5)	2013	5
11ax (Wi-Fi 6)	2019	2.5/5
11ax (Wi-Fi 6E)	2020	2.5/5/6
11be (Wi-Fi 7)	2024 (prévu)	2.5/5/6

## Évolution des Standards IEEE 802.11

La technologie Wi-Fi s'est considérablement développée depuis son introduction, avec des standards qui ont évolué pour offrir des vitesses plus élevées, une meilleure couverture et une capacité accrue. Le tableau suivant résume l'évolution des standards :

- **802.11-1997** : Le premier standard Wi-Fi avec un débit de 2 Mbit/s sur la bande de 2.4 GHz.
- **802.11b** : Introduit en 1999, ce standard a augmenté le débit à 11 Mbit/s tout en restant sur la bande de 2.4 GHz.
- **802.11a** : Également introduit en 1999, mais avec une bande de fréquence de 5 GHz et un débit de 54 Mbit/s.
- **802.11g** : Ce standard de 2003 combinait les fréquences de 2.4 GHz avec les débits de 802.11a.
- **802.11n (Wi-Fi 4)** : En 2009, avec des débits pouvant atteindre 600 Mbit/s et des bandes de fréquence doubles, il a introduit la technologie MIMO.
- **802.11ac (Wi-Fi 5)** : Lancé en 2013, il a considérablement augmenté les débits jusqu'à 6.8 Gbit/s, utilisant exclusivement la bande de 5 GHz.
- **802.11ax (Wi-Fi 6 et 6E)** : A partir de 2019, il améliore encore les performances avec des débits théoriques allant jusqu'à 9.6 Gbit/s et utilise les bandes de 2.5 GHz, 5 GHz et 6 GHz (Wi-Fi 6E).
- **802.11be (Wi-Fi 7)** : Prévu pour 2024, ce standard promet des débits révolutionnaires allant jusqu'à 46.1 Gbit/s.

## Application Pratique

• **Planification et Mise en Œuvre de Réseaux** : Les professionnels du réseau doivent choisir le bon standard Wi-Fi pour répondre aux besoins de performance et de portée de leur organisation.

• **Prévision de Besoins Futurs** : La connaissance des futurs standards comme le Wi-Fi 7 est essentielle pour anticiper les évolutions des infrastructures réseau.

Ce tableau et ces explications permettent aux stagiaires de visualiser le chemin parcouru en termes d'évolution du Wi-Fi et de comprendre l'importance de la sélection du bon standard pour leurs applications spécifiques.



Utilisation d'un outils  
d'observation wifi comme  
inssider

## Démonstration

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

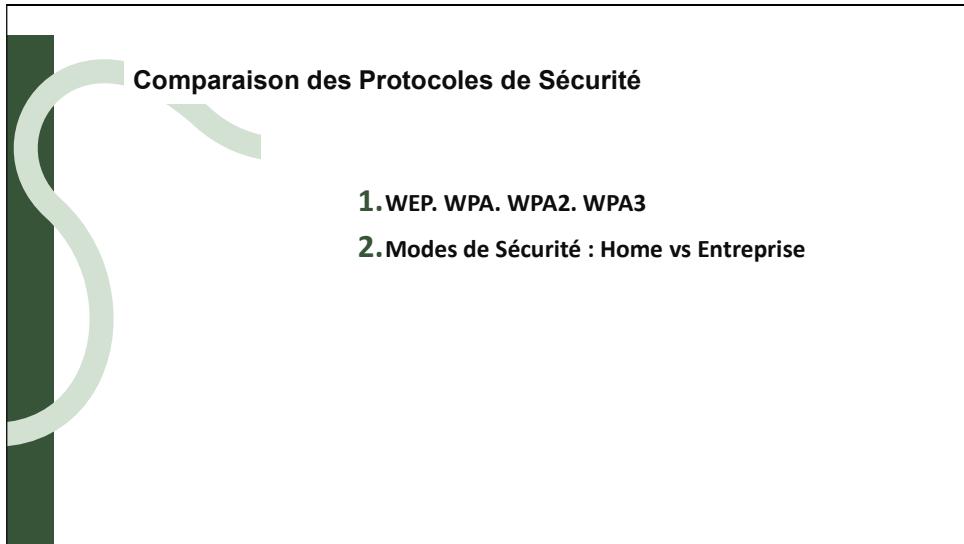
---

---

---

---

---



### Comparaison des Protocoles de Sécurité Wi-Fi

La sécurité est une préoccupation majeure dans les réseaux sans-fil, et plusieurs protocoles ont été développés pour protéger les communications Wi-Fi. Voici une comparaison des protocoles de sécurité les plus courants :

• **WEP (Wired Equivalent Privacy) :**

- Ancien et peu sécurisé
- Utilise une clé partagée statique
- Vulnérable aux attaques par force brute et par cryptanalyse

• **WPA (Wi-Fi Protected Access) :**

- Amélioration de la sécurité par rapport au WEP
- Utilise TKIP (Temporal Key Integrity Protocol) pour le chiffrement
- Moins vulnérable aux attaques que le WEP, mais toujours insuffisant pour les normes actuelles de sécurité

• **WPA2 :**

- Successeur de WPA, considéré comme le standard de sécurité pendant de nombreuses années
- Utilise AES (Advanced Encryption Standard) pour le chiffrement, plus sécurisé que TKIP
- Prise en charge des modes de sécurité personnelle (PSK) et d'entreprise (802.1X)

• **WPA3 :**

- Dernière itération de la sécurité Wi-Fi
- Améliorations de la sécurité, y compris la protection contre les attaques de force brute, le chiffrement individuel et le chiffrement opportun
- Introduit des améliorations de sécurité significatives par rapport à WPA2

### **Modes de Sécurité : Home vs Entreprise**

Outre les protocoles de sécurité eux-mêmes, il est important de comprendre les différents modes de sécurité utilisés dans les réseaux sans-fil :

•**Mode Personnel (PSK) :**

- Utilisé dans les réseaux domestiques et de petite taille
- La clé de sécurité est partagée entre tous les appareils et est souvent facilement accessible

•**Mode Entreprise (802.1X) :**

- Utilisé dans les environnements professionnels et les réseaux d'entreprise
- Requiert une authentification individuelle pour chaque utilisateur ou appareil, généralement via un serveur d'authentification RADIUS
- Offre un contrôle d'accès plus granulaire et une sécurité renforcée, mais nécessite une infrastructure plus complexe

En comprenant les différences entre ces protocoles et modes de sécurité, les entreprises peuvent mettre en place des mesures de sécurité adaptées à leurs besoins spécifiques et protéger efficacement leurs réseaux sans-fil contre les menaces potentielles.



	WEP	WPA	WPA2
Release Year	1999	2003	2004
Encryption Method	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP) with RC4	CCMP and AES
Session Key Size	40-bit	128-bit	128-bit
Cipher Type	Stream	Stream	Block
Data Integrity	CRC-32	Message Integrity Code	CBC-MAC
Key Management	Not provided	4-way handshaking mechanism	4-way handshake mechanism
Authentication	WEP-Open WEP-Shared	Pre-Shared Key (PSK) & 802.1x with EAP variant	Pre-Shared Key (PSK) & 802.1x with EAP variant

## Évolution des Standards de Sécurité Wi-Fi

### WEP (Wired Equivalent Privacy) :

- Lancé en 1999 avec le standard original 802.11.
- Utilise le chiffrement RC4 et offre des clés de session de 40 bits.
- Considéré comme peu sûr en raison de ses faiblesses structurelles. Il est maintenant obsolète.

### WPA (Wi-Fi Protected Access) :

- Introduit en 2003 pour remplacer WEP.
- Emploie le protocole TKIP (Temporal Key Integrity Protocol) avec RC4 pour une meilleure sécurité, avec des clés de session de 128 bits.
- Inclut une authentification améliorée avec un mécanisme de poignée de main à 4 voies.

### WPA2 (Wi-Fi Protected Access 2) :

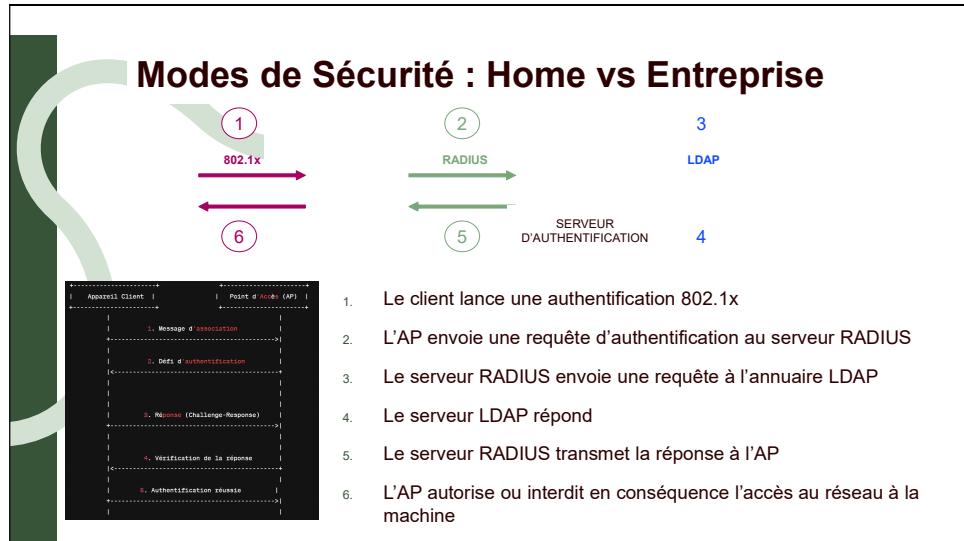
- Adopté en 2004, il représente une amélioration par rapport à WPA.
- Introduit le chiffrement AES (Advanced Encryption Standard) pour une sécurité renforcée.
- Continue d'utiliser un mécanisme de poignée de main à 4 voies pour la gestion des clés.

### WPA3 (Wi-Fi Protected Access 3) :

- Publié en 2018, il est la dernière avancée en termes de sécurité Wi-Fi.
- Offre deux versions : WPA3-Personal et WPA3-Enterprise. La personnelle utilise des clés de session de 128 bits tandis que l'entreprise utilise des clés de 192 bits.
- WPA3 utilise un mécanisme d'authentification plus sécurisé appelé SAE (Simultaneous Authentication of Equals), et AES est utilisé pour le chiffrement.

## Application Pratique

- **Configuration de Réseau** : Les administrateurs réseau doivent appliquer le protocole de sécurité Wi-Fi le plus avancé disponible sur leurs équipements pour garantir une protection maximale.
- **Conformité aux Normes de Sécurité** : Les organisations doivent se conformer aux standards de sécurité pour protéger les informations sensibles et maintenir la confiance des utilisateurs.



### Modes de Sécurité : Home vs Entreprise

Dans un environnement domestique, la sécurité Wi-Fi est généralement gérée par un mot de passe pré-partagé (Pre-Shared Key ou PSK) utilisant WPA2 ou WPA3. C'est un mode de sécurité simple et suffisant pour la plupart des réseaux domestiques.

En entreprise, le niveau de sécurité requis est plus élevé, et le processus d'authentification est plus complexe pour s'assurer que seuls les utilisateurs autorisés accèdent au réseau. La diapositive décrit le processus utilisant 802.1x avec RADIUS et LDAP :

• **Le client lance une authentification 802.1x :**

- Un ordinateur ou un autre appareil tente de se connecter au réseau en initiant une authentification 802.1x, un standard pour le contrôle d'accès réseau.

• **L'AP (Access Point) envoie une requête d'authentification au serveur RADIUS :**

- L'AP agit comme un intermédiaire, transmettant la demande d'authentification de l'utilisateur au serveur RADIUS, un serveur d'authentification, d'autorisation et de comptabilité.

• **Le serveur RADIUS envoie une requête à l'annuaire LDAP :**

- RADIUS communique avec un annuaire LDAP (Lightweight Directory Access Protocol) pour vérifier les informations d'identification de l'utilisateur.

• **Le serveur LDAP répond :**

- L'annuaire LDAP confirme si les informations d'identification de l'utilisateur sont valides et retourne cette information au serveur RADIUS.

• **Le serveur RADIUS transmet la réponse à l'AP :**

- Sur la base de la réponse LDAP, le serveur RADIUS informe l'AP si l'utilisateur doit être autorisé ou non sur le réseau.

• **L'AP autorise ou interdit en conséquence l'accès au réseau à la machine :**

- Si les informations d'identification sont validées, l'AP autorise l'appareil à se connecter au réseau. Dans le cas contraire, l'accès est refusé.

### Application Pratique

• **Déploiement de Réseau :** Les ingénieurs réseau doivent mettre en œuvre des solutions d'authentification qui correspondent au niveau de sécurité requis par l'entreprise.

• **Maintenance de la Sécurité :** Les administrateurs doivent régulièrement réviser et mettre à jour les politiques de sécurité pour s'adapter aux menaces émergentes et aux nouvelles réglementations.



— Objectifs :

- Installer et utiliser l'outil « inssider »  
(visualisation des AP.  
observation des canaux .  
de la puissance. des  
débits)

**Démonstration**

- Ce qu'il faut retenir



- WiFi : Connectivité Sans Fil Essentielle
- Sécurité WiFi : Une Priorité
- Comparaison des Normes 802.11
- Gestion du Spectre et Canaux WiFi
- Architecture WiFi et Solutions d'Entreprise

**WiFi : Connectivité Sans Fil Essentielle :**

"Le WiFi offre une connectivité sans fil essentielle permettant aux appareils de communiquer et d'accéder à Internet sans la contrainte des câbles, facilitant la mobilité et la flexibilité."

**Sécurité WiFi : Une Priorité :**

"La sécurisation des réseaux WiFi est cruciale pour protéger les données. Les protocoles de sécurité tels que WPA2 et WPA3 sont indispensables pour assurer la confidentialité et l'intégrité des informations échangées."

**Comparaison des Normes 802.11 :**

"Les différentes normes WiFi (a/b/g/n/ac/ax) ou (wifi 5 wifi 6/6e wifi 7) offrent des vitesses et des portées variées, adaptées à divers besoins et environnements, soulignant l'importance de choisir la norme appropriée pour optimiser la performance du réseau."

**Gestion du Spectre et Canaux WiFi :**

"La sélection judicieuse des canaux WiFi, en tenant compte des interférences et de la congestion du spectre, est essentielle pour maintenir une connexion stable et performante."

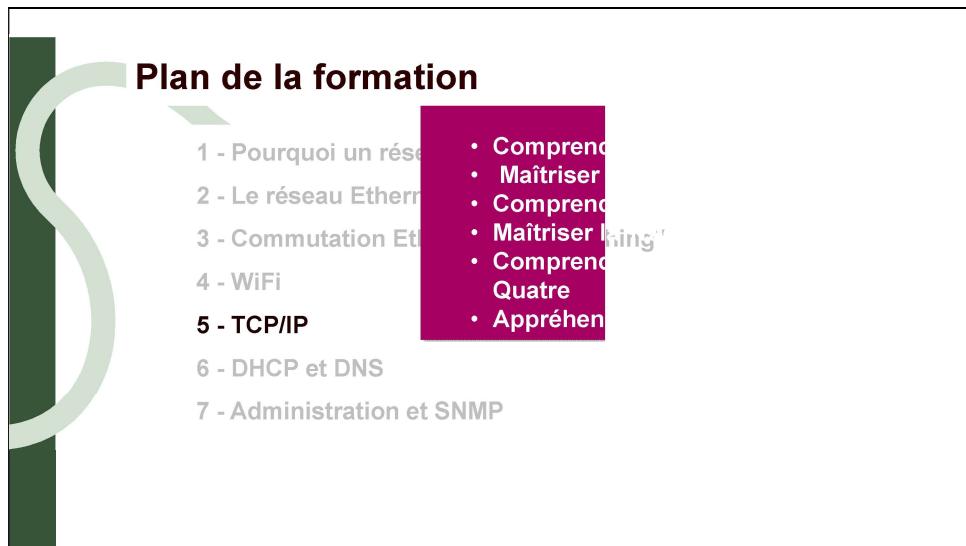
**Architecture WiFi et Solutions d'Entreprise :**

"Les architectures de réseau WiFi, y compris les configurations de points d'accès et les solutions d'entreprise, doivent être soigneusement planifiées pour garantir une couverture étendue, une haute disponibilité et une gestion efficace du trafic."

## Chapitre 5 – TCP/IP

### 5 – TCP/IP

- Objectifs du chapitre

**Objectifs du Chapitre 5 - TCP/IP :****•Comprendre l'Empilement Protocolaire :**

- Expliquer la structure et le fonctionnement de l'empilement protocolaire TCP/IP.
- Identifier les différentes couches de l'empilement et leur rôle dans la communication réseau.

**•Maîtriser les Protocoles Fondamentaux :**

- Définir et comprendre l'utilisation des protocoles ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) et ICMP (Internet Control Message Protocol).
- Expliquer les scénarios d'utilisation de chaque protocole et leur importance dans la résolution d'adresses et la gestion des messages de contrôle.

**•Comprendre l'Adressage IP :**

- Différencier les adresses IP publiques des adresses IP privées, en mettant en évidence les classes d'adresses et les plages réservées définies par le RFC 1918.
- Expliquer les concepts de sous-réseaux et de sur-réseaux, ainsi que leur utilisation dans la segmentation des réseaux IP.

**•Maîtriser la Traduction d'Adresse :**

- Décrire les concepts de SNAT (Source Network Address Translation) et DNAT (Destination Network Address Translation) dans le cadre de la traduction d'adresses IP.
- Illustrer les cas d'utilisation typiques de la traduction d'adresse dans les environnements réseau.

**•Comprendre l'Adressage de Niveau Quatre :**

- Expliquer le concept de socket et son rôle dans les communications réseau.
- Utiliser des outils tels que netstat, tcpview et le gestionnaire de tâches pour visualiser l'état des sockets et comprendre leur fonctionnement.

**•Appréhender les Protocoles TCP et UDP :**

- Comprendre les fonctionnalités du protocole TCP (Transmission Control Protocol) et son utilisation dans le transfert fiable de données.
- Analyser les cinématiques de connexion, d'échange de données et de déconnexion dans le cadre du protocole TCP.
- Examiner les caractéristiques et les cas d'utilisation du protocole UDP (User Datagram Protocol) dans les applications temps réel et transactionnelles.
- Comprendre les cinématiques de communication spécifiques à UDP.



- "Comment décririez-vous le fonctionnement de l'Internet à quelqu'un qui n'est pas familier avec la technologie ? Quels éléments clés mentionneriez-vous ?"
- "Avez-vous déjà eu besoin de connaître votre adresse IP ? Dans quel contexte et pourquoi était-ce important ?"
- "Pouvez-vous partager une expérience où vous avez dû diagnostiquer un problème de connectivité Internet ? Quels outils ou méthodes avez-vous utilisés ?"
- "Quelles mesures prenez-vous pour protéger votre vie privée et votre sécurité en ligne ? Comment ces mesures se rapportent-elles, à votre avis, au protocole TCP/IP ?"
- "Quand vous utilisez des services en ligne, comme le courrier électronique ou le streaming, êtes-vous conscient de la manière dont vos données sont transférées sur Internet ? Avez-vous des hypothèses sur ce processus ?"

**Compréhension de l'Internet :**

"Comment décririez-vous le fonctionnement de l'Internet à quelqu'un qui n'est pas familier avec la technologie ? Quels éléments clés mentionneriez-vous ?"

**Importance de l'Adressage IP :**

"Avez-vous déjà eu besoin de connaître votre adresse IP ? Dans quel contexte et pourquoi était-ce important ?"

**Expériences avec la Connectivité :**

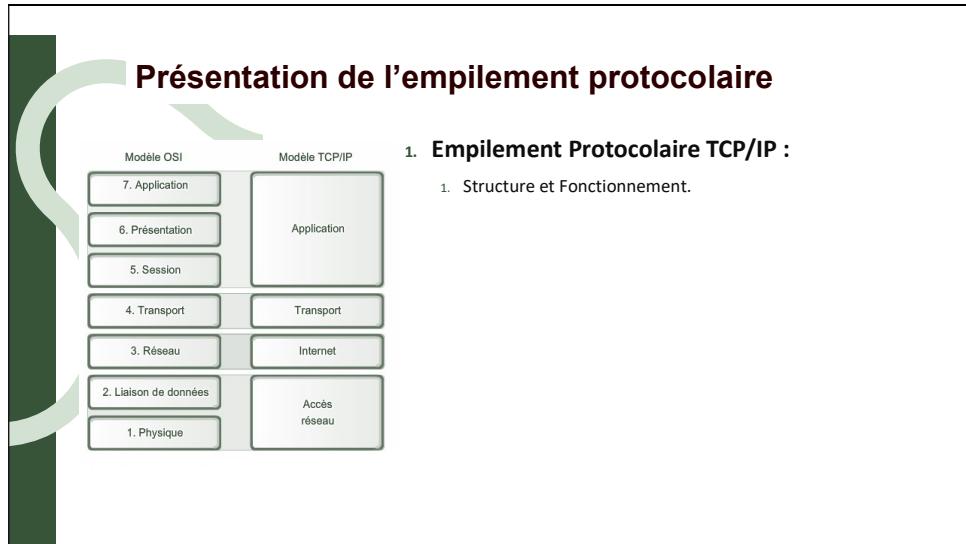
"Pouvez-vous partager une expérience où vous avez dû diagnostiquer un problème de connectivité Internet ? Quels outils ou méthodes avez-vous utilisés ?"

**Sécurité et Communication en Ligne :**

"Quelles mesures prenez-vous pour protéger votre vie privée et votre sécurité en ligne ? Comment ces mesures se rapportent-elles, à votre avis, au protocole TCP/IP ?"

**Utilisation des Services en Ligne :**

"Quand vous utilisez des services en ligne, comme le courrier électronique ou le streaming, êtes-vous conscient de la manière dont vos données sont transférées sur Internet ? Avez-vous des hypothèses sur ce processus ?"



### Présentation de l'Empilement Protocolaire TCP/IP

L'empilement protocolaire TCP/IP constitue le cadre fondamental qui régit la communication sur les réseaux informatiques. Il est composé de plusieurs couches, chacune jouant un rôle spécifique dans le processus de transmission des données. Comprendre cette structure est essentiel pour appréhender le fonctionnement global des communications réseau.

#### 1. Couche Application :

- La couche supérieure de l'empilement protocolaire est la couche Application. Elle est responsable de l'interaction directe avec les applications utilisateur, telles que les navigateurs web, les clients de messagerie, etc. Cette couche utilise des protocoles tels que HTTP, SMTP, FTP pour fournir des services de communication aux applications.

#### 2. Couche Transport :

- Juste en dessous de la couche Application se trouve la couche Transport. Cette couche assure la transmission des données entre les applications sur différents périphériques. Les protocoles couramment utilisés dans cette couche sont TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).

#### 3. Couche Réseau :

- La couche Réseau est chargée du routage des paquets de données à travers le réseau. Elle utilise des adresses IP pour identifier les périphériques sur le réseau et détermine le meilleur chemin pour acheminer les données d'un point à un autre. Les protocoles IP (Internet Protocol) et ICMP (Internet Control Message Protocol) sont utilisés dans cette couche.

#### 4. Couche Liaison de Données :

- En dessous de la couche Réseau se trouve la couche Liaison de Données. Cette couche assure la fiabilité de la transmission des données sur un support physique. Elle est subdivisée en sous-couches : la sous-couche LLC (Logical Link Control) et la sous-couche MAC (Media Access Control). Les protocoles Ethernet, PPP, et WLAN sont utilisés dans cette couche.

**5. Couche Physique :**

•La couche la plus basse de l'empilement est la couche Physique. qui définit les aspects matériels de la transmission des données. Elle spécifie les caractéristiques électriques. mécaniques et fonctionnelles des périphériques de réseau. ainsi que les types de câblage. les connecteurs et les signaux électriques utilisés.

La compréhension de cette structure en couches est cruciale pour comprendre le fonctionnement des réseaux informatiques et des communications sur Internet. Chaque couche contribue à la transmission des données de manière distincte. et une défaillance ou un dysfonctionnement dans l'une de ces couches peut affecter la communication dans son ensemble.



## Définition et usage des protocoles : (ARP.RARP). ICMP

- Protocoles Fondamentaux : ARP. RARP. ICMP
  - ▶ Fonctions et Utilisation.
- ARP : Mapping IP-MAC
  - ▶ Découvrez comment ARP facilite la communication en associant les adresses IP aux adresses MAC sur un réseau local.
- ICMP : Diagnostic et Contrôle
  - ▶ Explorez le rôle crucial de ICMP dans la détection d'erreurs, le diagnostic réseau et la gestion du trafic.

### Définition et Usage des Protocoles : ARP. RARP. ICMP

Dans le fonctionnement d'un réseau informatique, plusieurs protocoles jouent des rôles critiques pour garantir la connectivité et la gestion efficace des périphériques. Parmi ceux-ci, les protocoles ARP, RARP et ICMP occupent une place centrale.

#### 1. ARP (Address Resolution Protocol) :

• Le protocole ARP est utilisé pour mapper une adresse IP à une adresse MAC (Media Access Control) sur un réseau local. Lorsqu'un périphérique souhaite communiquer avec un autre sur le même réseau, il utilise ARP pour découvrir l'adresse MAC correspondant à une adresse IP spécifique. Cela permet d'établir la communication entre les périphériques au niveau de la couche liaison de données.

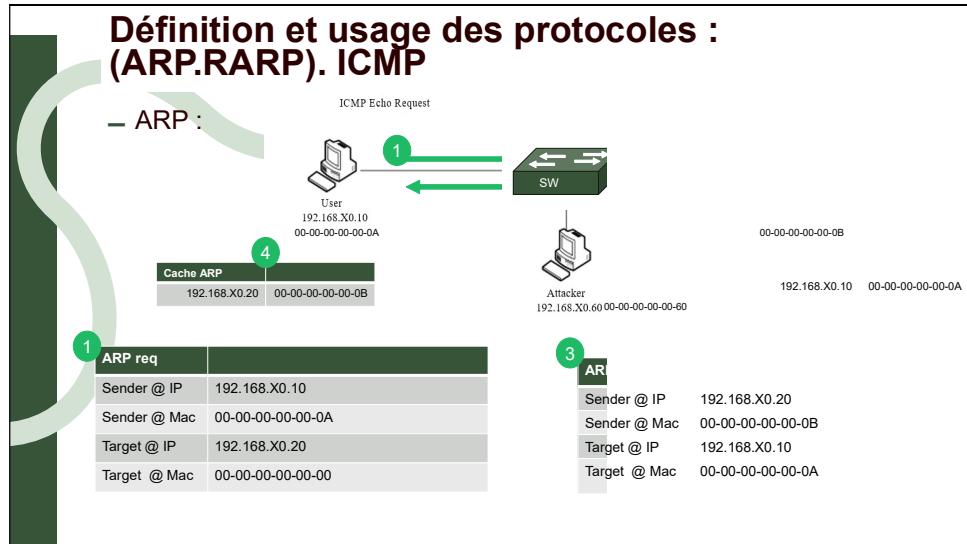
#### 2. RARP (Reverse Address Resolution Protocol) :

• À l'inverse d'ARP, le protocole RARP est utilisé pour obtenir une adresse IP à partir d'une adresse MAC. Il est principalement utilisé dans les environnements où les périphériques ne disposent pas d'une configuration IP statique et doivent obtenir une adresse IP auprès d'un serveur RARP.

#### 3. ICMP (Internet Control Message Protocol) :

• ICMP est un protocole utilisé pour envoyer des messages de contrôle et de diagnostic entre les périphériques réseau. Il fournit des informations sur la disponibilité et l'état des périphériques, ainsi que des mécanismes de détection d'erreurs et de gestion du trafic. Les messages ICMP sont utilisés pour tester la connectivité réseau avec des commandes telles que Ping et Traceroute.

La compréhension de ces protocoles est essentielle pour diagnostiquer et résoudre les problèmes réseau, ainsi que pour assurer un fonctionnement fluide et efficace des communications entre les périphériques. Chaque protocole remplit des fonctions spécifiques dans la gestion et le contrôle du trafic sur le réseau, contribuant ainsi à sa fiabilité et à sa performance globale.



## Fonctionnement du Protocole ARP (Address Resolution Protocol)

### Qu'est-ce que l'ARP ?

- L'ARP est un protocole fondamental utilisé dans les réseaux IP pour découvrir l'adresse MAC (Media Access Control) correspondante à une adresse IP connue.

### Étapes du Processus ARP :

#### • ARP Request (Demande ARP) :

- Un utilisateur (192.168.X0.10) souhaite communiquer avec un serveur (192.168.X0.20) mais ne connaît pas l'adresse MAC du serveur.
- L'utilisateur envoie une demande ARP (ARP Request) sur le réseau, demandant l'adresse MAC correspondant à l'adresse IP 192.168.X0.20.

#### • Diffusion de la Demande ARP :

- La demande ARP est une diffusion (broadcast) sur le réseau local, ce qui signifie que tous les appareils du réseau reçoivent la demande.

#### • Réponse ARP (ARP Reply) :

- Le serveur ayant l'adresse IP 192.168.X0.20 reconnaît sa propre adresse IP dans la demande et envoie une réponse ARP (ARP Reply) à l'utilisateur, fournissant son adresse MAC (00-00-00-00-0B).

#### • Mise à Jour du Cache ARP :

- L'utilisateur reçoit la réponse ARP et met à jour son cache ARP avec l'association de l'adresse IP du serveur à son adresse MAC.
- Le cache ARP est une table stockée dans la mémoire de l'appareil qui conserve les associations IP-MAC récemment résolues pour accélérer les communications futures.

**Sécurité et Vulnérabilités d'ARP :**

- La diapositive montre également un attaquant potentiel sur le réseau (192.168.X0.60). Dans les réseaux non sécurisés, l'ARP peut être exploité pour effectuer des attaques comme l'empoisonnement de cache ARP (ARP Poisoning) ou l'usurpation ARP (ARP Spoofing).
- Ces attaques peuvent conduire à des interceptions de données (man-in-the-middle attacks), où l'attaquant répond à des demandes ARP pour des adresses IP avec sa propre adresse MAC, redirigeant le trafic à travers son appareil.

**Application Pratique**

- **Dépannage Réseau** : La compréhension d'ARP est importante pour le dépannage réseau, permettant aux administrateurs de diagnostiquer des problèmes de connectivité.
- **Conception de Réseau Sécurisé** : Les architectes réseau doivent planifier des mesures pour sécuriser les communications ARP dans la conception des réseaux d'entreprise.



Observation d'ARP avec  
Wireshark

## Démonstration

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

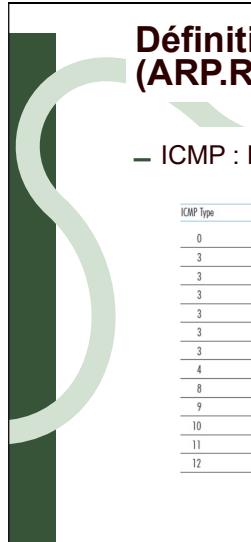
---

---

---

---

---



## Définition et usage des protocoles : (ARP.RARP). ICMP

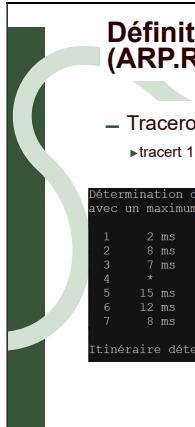
### - ICMP : Diagnostic et Contrôle

ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

ICMP signifie "Internet Control Message Protocol". C'est un protocole de communication utilisé pour envoyer des messages de contrôle et de diagnostic entre les périphériques sur un réseau IP. ICMP est généralement utilisé pour signaler les erreurs ou les conditions anormales dans la communication IP, ainsi que pour tester la connectivité entre les hôtes

### Les messages ICMP les plus courants :

- **Type 0 code 0** : Echo Reply - Ce message ICMP est une réponse à un message Echo Request (Ping). Il indique que le paquet ICMP a été reçu correctement.
- **Type 3 code 0** : Destination Unreachable - Ce message ICMP indique qu'il est impossible d'atteindre la destination spécifiée. Le code 0 signifie "Network Unreachable", ce qui indique qu'aucun itinéraire n'est disponible pour atteindre le réseau de destination.
- **Type 3 code 1** : Destination Unreachable - Le code 1 signifie "Host Unreachable", ce qui indique que la destination spécifiée est inaccessible car l'hôte de destination est hors de portée.
- **Type 3 code 2** : Destination Unreachable - Le code 2 signifie "Protocol Unreachable", ce qui indique qu'aucun protocole approprié n'est disponible pour atteindre la destination spécifiée.
- **Type 3 code 3** : Destination Unreachable - Le code 3 signifie "Port Unreachable", ce qui indique qu'aucun service n'est disponible sur le port spécifié de l'hôte de destination.
- **Type 3 code 6** : Destination Unreachable - Le code 6 signifie "Destination Network Unknown", ce qui indique que l'adresse IP de destination n'est pas connue sur le réseau.
- **Type 3 code 7** : Destination Unreachable - Le code 7 signifie "Destination Host Unknown", ce qui indique que l'hôte de destination spécifié est inconnu.
- **Type 4 code 0** : Source Quench - Ce message ICMP est utilisé pour informer un émetteur qu'il envoie des paquets trop rapidement et qu'il devrait ralentir son débit.
- **Type 8 code 0** : Echo Request - Ce message ICMP est envoyé par un émetteur pour tester la connectivité avec un hôte distant.
- **Type 9 code 0** : Router Advertisement - Ce message ICMP est utilisé par un routeur pour annoncer sa présence sur un réseau.
- **Type 10 code 0** : Router Solicitation - Ce message ICMP est utilisé par un hôte pour demander des annonces de routeur sur un réseau.
- **Type 11 code 0** : Time Exceeded - Ce message ICMP est généré lorsqu'un paquet IP dépasse sa durée de vie maximale (Time To Live) ou lorsqu'il atteint un nombre maximum de sauts (Hop Limit). Le code 0 signifie que le paquet a dépassé le nombre maximum de sauts.



**Définition et usage des protocoles :**  
**(ARP.RARP). ICMP**

— Traceroute :  
►tracert 1.1.1.1

```
Détermination de l'itinéraire vers one.one.one.one [1]
avec un maximum de 30 sauts :

 1   2 ms    1 ms    1 ms  192.168.250.254
 2   8 ms    8 ms    7 ms station11.multimania.
 3   7 ms    7 ms    *     station3.multimania.
 4   7 ms    6 ms    7 ms prs-b3-link.ip.twelve
 5  15 ms   10 ms   10 ms cloudflare-ic-382666.
 6  12 ms   7 ms    6 ms  141.101.67.54
 7   8 ms    8 ms    7 ms one.one.one.one [1.0.0.1]

Itinéraire déterminé.
```

### Traceroute : Un Outil de Diagnostic Réseau Essentiel

La commande traceroute, ici illustrée par son équivalent sous Windows tracert, est un outil de diagnostic qui permet de suivre le chemin (route) que prend un paquet IP pour atteindre sa destination finale. Le processus de traceroute envoie des paquets avec des valeurs TTL (Time To Live) croissantes pour découvrir chaque saut (hop) sur le chemin de la destination.

**Utilisation :** La commande tracert suivi de l'adresse IP ou du nom de domaine, ici 1.1.1.1 (un service DNS public de Cloudflare), initie l'outil de diagnostic.

#### Interprétation de la Sortie :

- La première colonne indique le numéro de saut.
- Les colonnes suivantes montrent le temps que chaque paquet prend pour atteindre le saut en question et revenir, mesuré en millisecondes (ms).
- Chaque ligne représente un routeur ou un commutateur par lequel les paquets transitent sur le chemin de la destination.
- Les adresses IP ou noms de domaine de chaque périphérique intermédiaire sont affichés, s'ils sont disponibles.
- Un astérisque (\*) indique que la réponse n'a pas été reçue dans le délai imparti pour ce saut, ce qui peut indiquer un filtre ICMP en place qui empêche la réponse.

#### Comprendre le Résultat :

- Des temps de réponse cohérents ou décroissants indiquent un réseau stable sans encombrement.
- Une augmentation soudaine du temps de réponse peut indiquer un goulot d'étranglement ou un problème de réseau à ce point spécifique.
- Des temps de réponse fluctuants peuvent indiquer un problème de stabilité de la connexion.

#### Applications Pratiques :

- **Dépannage du Réseau :** Si vous ne pouvez pas atteindre un site web ou un service, traceroute peut vous aider à déterminer où la connexion est bloquée.
- **Performance du Réseau :** Analyser les temps de réponse pour identifier les liens lents dans le réseau.
- **Sécurité Réseau :** Identifier les chemins inattendus qui pourraient indiquer une redirection malveillante du trafic.

En résumé, traceroute est un outil précieux pour les administrateurs réseau et les techniciens de support pour diagnostiquer les problèmes de connectivité et optimiser les performances du réseau.



- Time	Source	Destination	Protocol	Type	(Code)
132 1.5335525	R1	1.1.1.1	ICMP	11,8	
132 1.5335521	Source	1.1.1.1	ICMP	11,8	
132 1.5335521	R1	Source	ICMP	11,8	
133 1.5388934	Source	1.1.1.1	ICMP	11,8	
135 1.5416112	R1	Source	ICMP	11,8	
209 10.586950	Source	1.1.1.1	ICMP	11,8	
209 10.586950	R2	Source	ICMP	11,8	
209 10.586950	Source	1.1.1.1	ICMP	11,8	
209 9.559723	R2	Source	ICMP	11,8	
209 9.559723	Source	1.1.1.1	ICMP	11,8	
211 10.400758	R3	Source	ICMP	11,8	
211 10.400758	Source	1.1.1.1	ICMP	11,8	
211 10.400758	R3	Source	ICMP	11,8	
212 2.409228	Source	1.1.1.1	ICMP	11,8	
212 2.409228	R4	Source	ICMP	11,8	
272 14.409271	Source	1.1.1.1	ICMP	11,8	
322 18.378212	Source	1.1.1.1	ICMP	11,8	
322 18.378212	R5	Source	ICMP	11,8	
324 18.386706	Source	1.1.1.1	ICMP	11,8	
325 18.394086	R4	Source	ICMP	11,8	
329 18.394086	Source	1.1.1.1	ICMP	11,8	
400 19.419898	R5	Source	ICMP	11,8	
401 19.426792	Source	1.1.1.1	ICMP	11,8	
402 19.426792	R6	Source	ICMP	11,8	
404 19.442382	Source	1.1.1.1	ICMP	11,8	
407 19.453397	R5	Source	ICMP	11,8	
421 20.487055	Source	1.1.1.1	ICMP	11,8	
422 20.489691	R6	Source	ICMP	11,8	
424 20.493016	Source	1.1.1.1	ICMP	11,8	
425 20.499657	R6	Source	ICMP	11,8	
578 26.439884	Source	1.1.1.1	ICMP	11,8	
579 26.439884	1.1.1.1.3	Source	ICMP	0	
580 26.485707	Source	1.1.1.1	ICMP	0	
581 26.439880	1.1.1.1	Source	ICMP	0	
582 26.439880	Source	1.1.1.1	ICMP	0	
583 26.506191	1.1.1.1	Source	ICMP	0	



## Adressage IP : Public (classes d'adresses). privé (RFC 1918) sous réseaux et sur réseaux

1. Adressage IP : Public et Privé
  - les différences entre les adresses IP publiques et privées et leur utilisation dans les réseaux.
2. Classes d'Adresses IP
  - les différentes classes d'adresses IP et comprenez comment elles sont attribuées aux réseaux.
3. Sous-Réseaux et Sur-Réseaux
  - Mise en œuvre des sous-réseaux et sur-réseaux pour optimiser l'utilisation des adresses IP dans les réseaux.

```
Entrez une adresse IP      (format xxx.xxx.xxx.x
Entrez un masque de réseau (format xxx.xxx.xxx.x
-----AND-----
Réseau IP en décimal =====
-----
Adresse IP en binaire     : 11000000.10101000.
Masque de réseau en binaire : 11111111.11111111
-----AND-----
Réseau IP en binaire       : 11000000.10101000.
```

### Adressage IP : Public et Privé

L'adressage IP est crucial pour l'identification et la communication entre les périphériques sur un réseau. Il existe deux types d'adresses IP : les adresses publiques et les adresses privées. Les adresses publiques sont routables sur Internet, tandis que les adresses privées sont utilisées au sein des réseaux locaux et ne sont pas routables sur Internet.

Les adresses IP publiques sont généralement attribuées par les organismes de régulation des adresses IP, telles que l'IANA, et sont réparties en différentes classes, telles que les classes A, B et C, en fonction de leur plage d'adresses et de leur taille de réseau. Ces adresses sont utilisées pour identifier des périphériques individuels sur Internet.

D'autre part, les adresses IP privées sont définies dans le standard RFC 1918 et sont réservées pour une utilisation dans les réseaux locaux privés. Les plages d'adresses IP privées sont les suivantes : 10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16. Elles peuvent être utilisées librement au sein des réseaux locaux pour assigner des adresses aux périphériques.

La subdivision des adresses IP en sous-réseaux et sur-réseaux permet d'optimiser l'utilisation des adresses IP en permettant la segmentation du réseau en sous-unités logiques plus petites. Cela permet d'améliorer l'efficacité de la gestion des adresses IP et de mieux organiser la connectivité au sein du réseau.

En compréhension des concepts d'adressage IP public et privé, ainsi que l'utilisation des sous-réseaux et sur-réseaux, les administrateurs réseau peuvent mieux concevoir et gérer leurs infrastructures réseau pour répondre aux besoins spécifiques de leur organisation.



**Adressage IP : Public (classes d'adresses). privé (RFC 1918) sous réseaux et sur réseaux**

– Adressage IP : Public et Privé

**Règles d'adressage**

Un ID hôte ne peut avoir tous ses bits ni à 1 ni à 0  
Tout à 1 signifie : « tout hôte de ce réseau », c'est l'adresse réseau logique IP  
Tout à 0 signifie : « ce réseau »  
Le réseau 127.0.0.0 est réservé pour les adresses de loopback  
Le réseau 0.0.0.0 est réservé :  
En adresse source pour les machines clientes DHCP/BC  
En adresse de destination pour désigner la route par défaut dans les tables de routage  
255.255.255.255 est une adresse de diffusion locale et n'est pas routable, qui signifie « toute machine IP »

## Adressage IP : Public et Privé

### Adressage IP Public :

- Les adresses IP publiques sont uniques dans tout l'internet. Elles sont attribuées par l'IANA (Internet Assigned Numbers Authority) et gérées par des registres régionaux.
- Utilisées pour la communication sur Internet. elles permettent à un appareil d'être identifié et atteint de manière unique de n'importe où dans le monde.

### Adressage IP Privé (RFC 1918) :

- Les adresses IP privées sont destinées à être utilisées uniquement à l'intérieur des réseaux privés et ne sont pas routables sur Internet. Elles permettent à plusieurs réseaux d'utiliser les mêmes adresses sans conflit. tant qu'ils ne se connectent pas directement à l'internet public.
- Les plages d'adresses IP privées selon la RFC 1918 sont :
  - 10.0.0.0 à 10.255.255.255
  - 172.16.0.0 à 172.31.255.255
  - 192.168.0.0 à 192.168.255.255

### Règles d'adressage :

- Un ID de réseau ne peut pas avoir tous ses bits à 1 ni à 0 :
  - Un identifiant de réseau tout à 1 est considéré comme l'adresse de diffusion (broadcast).
  - Un identifiant de réseau tout à 0 spécifie le réseau lui-même.
- Le réseau **127.0.0.0** est réservé pour les adresses de bouclage (loopback). utilisées pour le trafic interne à l'hôte.
- Le réseau **0.0.0.0** est utilisé :
  - En adresse source pour les machines clientes DHCP/BOOTP lorsqu'elles ne connaissent pas encore leur propre adresse.
  - En adresse de destination pour désigner la route par défaut dans les tables de routage.
- **255.255.255.255** est l'adresse de diffusion locale et n'est pas routable. Elle sert à envoyer un paquet à tous les appareils sur le réseau local.

## Application Pratique

- **Conception de Réseau** : Les ingénieurs réseau doivent comprendre ces règles pour attribuer des adresses IP correctement et configurer les routeurs et les pare-feu pour protéger les réseaux.
- **Sécurité et Conformité** : Les administrateurs système doivent veiller à ce que les adresses privées soient utilisées conformément à la RFC 1918 et que des NAT (Network Address Translation) soient mis en place pour la communication avec l'Internet public.



Adressage IP : Public (classes d'adresses)			
Classe	Début	Fin	
Classe A	0.0.0.0	127.255.255.255	IP v4 Unicast
Classe B	128.0.0.0	191.255.255.255	
Classe C	192.0.0.0	223.255.255.255	
Classe D (multicast)	224.0.0.0	239.255.255.255	IP v4 Multicast
Classe E (réservée)	240.0.0.0	255.255.255.255	IP v4 Multicast
		255.255.255.255	Broadcast

### Adressage IP : Public (Classes d'adresses)

Le système traditionnel de classes d'adresses IP était basé sur la répartition des adresses IPv4 en cinq classes principales, A à E, en fonction des premiers bits de l'adresse. Voici les détails des classes :

#### Classe A :

- Plage d'adresses : De 0.0.0.0 à 127.255.255.255.
- Utilisées pour les très grands réseaux, comme les réseaux gouvernementaux. Le premier octet désigne le réseau, tandis que les trois derniers peuvent être utilisés pour les hôtes.

#### Classe B :

- Plage d'adresses : De 128.0.0.0 à 191.255.255.255.
- Destinées aux réseaux de taille moyenne, comme les entreprises ou les universités. Les deux premiers octets représentent le réseau et les deux derniers les hôtes.

#### Classe C :

- Plage d'adresses : De 192.0.0.0 à 223.255.255.255.
- Conçues pour les petits réseaux, comme les réseaux d'entreprise. Les trois premiers octets sont pour le réseau et le dernier pour les hôtes.

#### Classe D (multicast) :

- Plage d'adresses : De 224.0.0.0 à 239.255.255.255.
- Réservée pour le multicast, qui permet à une source unique d'envoyer un paquet à plusieurs hôtes en une seule transmission.

#### Classe E (réservée) :

- Plage d'adresses : De 240.0.0.0 à 255.255.255.255.
- Ces adresses sont réservées pour une utilisation future ou pour la recherche.

#### Adresse Broadcast :

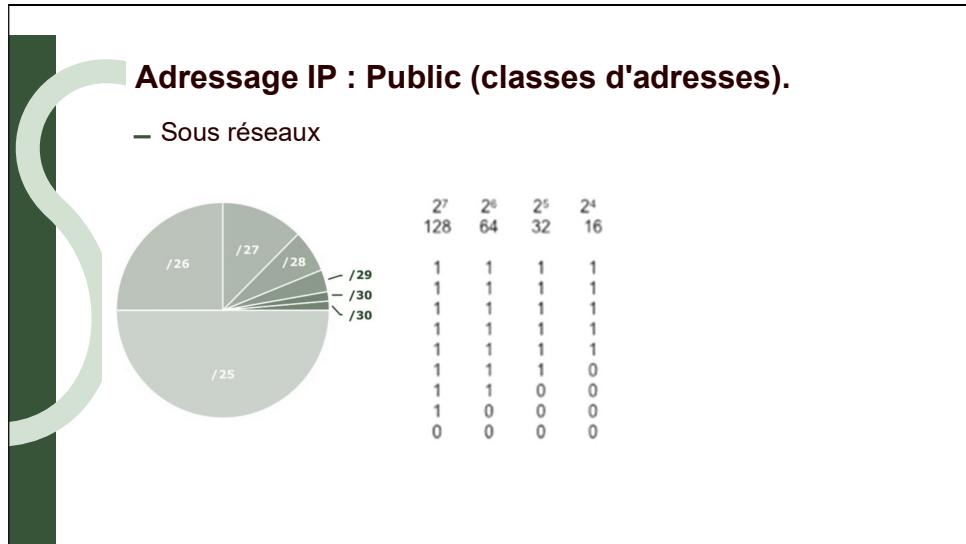
- Adresse : 255.255.255.255.
- Utilisée pour envoyer des messages à tous les hôtes d'un réseau local.

### Application Pratique

• **Connaissance de Base** : Comprendre le système de classes d'adresses IP est essentiel pour toute personne apprenant sur les réseaux, malgré l'utilisation de CIDR dans la pratique moderne.

• **Planification de Réseau** : Une compréhension des plages d'adresses aide les administrateurs réseau à planifier et à configurer les réseaux locaux.

Bien que le système de classes d'adresses IPv4 soit largement remplacé par le CIDR, cette connaissance reste importante pour comprendre les concepts de base du réseau et l'histoire de l'internet.



### CIDR Notation:

- La notation CIDR spécifie le nombre de bits alloués pour le réseau dans l'adresse IP par un suffixe comme /26 ou /27. Par exemple, 192.168.1.0/24 indique que les 24 premiers bits de l'adresse IP sont réservés pour l'identification du réseau et les 8 bits restants pour les hôtes.

### Subnetting:

- Le processus de division d'un réseau en sous-réseaux plus petits est appelé subnetting. Cela permet une utilisation plus efficace de l'adresse IP et peut améliorer la gestion du réseau, la sécurité et les performances.

### Exemple avec un Réseau /24:

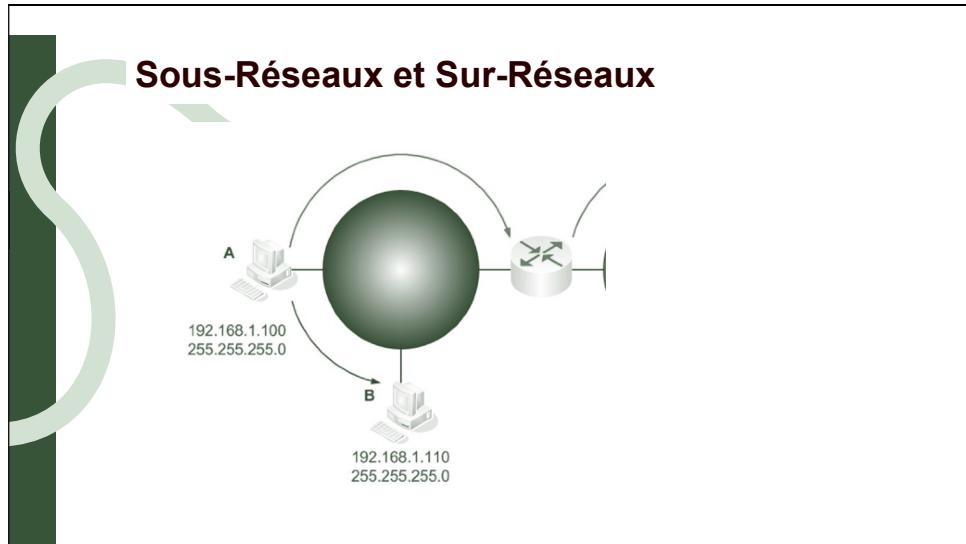
- Un réseau avec un masque de sous-réseau de /24 a 256 adresses IP possibles (de 0 à 255).
- Ce réseau peut être subdivisé en sous-réseaux plus petits, par exemple en /25, /26, ou /27, etc., qui fourniraient respectivement 2, 4, 8 sous-réseaux, chacun avec un nombre réduit d'adresses IP disponibles pour les hôtes.

### Sous-réseaux et Masques:

- Sur la diapositive, le diagramme circulaire illustre la division d'un réseau en sous-réseaux plus petits, et le tableau à droite montre la correspondance entre la notation CIDR et le masque de sous-réseau décimal.
- Par exemple, /26 correspond à un masque de sous-réseau de 255.255.255.192, ce qui signifie que les 26 premiers bits sont utilisés pour l'identification du réseau et les 6 bits restants pour les hôtes.

### Application Pratique

- Conception de Réseau :** Lors de la conception de réseaux IP, le sous-réseau est utilisé pour créer des hiérarchies de réseau et pour définir des segments de réseau clairs.
- Adressage Efficace :** En entreprise, le sous-réseau aide à gérer de manière flexible les adresses IP en fonction de la taille et des exigences des différents départements ou zones opérationnelles.



- Réseau bleu : Les ordinateurs A et B ont des adresses IP de 192.168.1.100 et 192.168.1.110 respectivement, tous deux avec un masque de sous-réseau de 255.255.255.0. Cela indique qu'ils sont sur le même sous-réseau.

Réseau rouge : L'ordinateur C a une adresse IP de 172.16.0.50 avec un masque de sous-réseau de 255.255.0.0, ce qui suggère qu'il est sur un réseau différent.

Cela illustre un concept clé de la mise en réseau : des sous-réseaux différents sont généralement interconnectés via un routeur pour permettre la communication entre eux. Le masque de sous-réseau détermine quelle portion de l'adresse IP représente le réseau et quelle portion peut être utilisée pour les hôtes (ordinateurs, appareils, etc.) au sein de ce réseau.

La communication entre ces réseaux nécessiterait un routage intermédiaire, où le routeur connaît les adresses des deux réseaux et peut transférer les paquets entre eux. Si l'ordinateur A souhaite communiquer avec l'ordinateur C, il enverrait d'abord ses paquets au routeur, qui les acheminerait ensuite vers le bon réseau.

## Adressage IP : Public (classes d'adresses). privé (RFC 1918) sous réseaux et sur réseaux

– Sous réseaux

255.255.255.0  
/24

192.168.1.0      192.168.1.1

192.168.1.254  
192.168.1.255

Entrez une adresse IP (f  
Entrez un masque de réseau (f  
====AND=====  
Réseau IP en décimal ======  
-----  
Adresse IP en binaire :  
Masque de réseau en binaire :  
====AND=====  
Réseau IP en binaire :

## Adressage IP : Public (classes d'adresses). privé (RFC 1918) sous réseaux et sur réseaux

– Sous réseaux

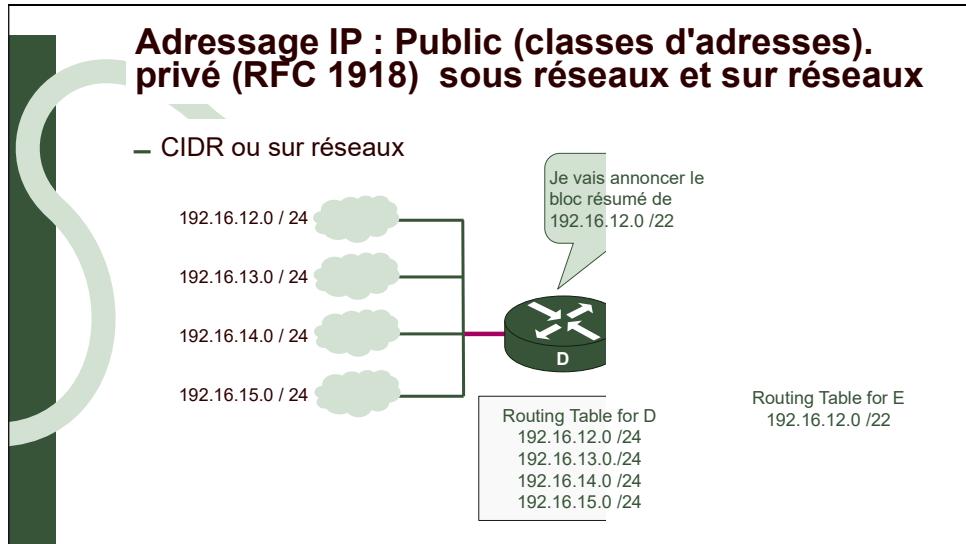
255.255.255.128  
/25

192.168.1.0      192.168.1.1  
192.168.1.127      192.168.1.128

192.168.1.128      192.168.1.129  
192.168.1.255      192.168.1.254

Entrez une adresse IP (format xxx.xxx.xxx.  
Entrez un masque de réseau (format xxx.xxx.xxx.  
====AND=====  
Réseau IP en décimal ======  
-----  
Adresse IP en binaire : 11000000.10101000  
Masque de réseau en binaire : 11111111.11111111  
====AND=====  
Réseau IP en binaire : 11000000.10101000

Entrez une adresse IP (format xxx.xxx.xxx.  
Entrez un masque de réseau (format xxx.xxx.xxx.  
====AND=====  
Réseau IP en décimal ======  
-----  
Adresse IP en binaire : 11000000.10101000  
Masque de réseau en binaire : 11111111.11111111  
====AND=====  
Réseau IP en binaire : 11000000.10101000



### Adressage IP : CIDR et Agrégation d'adresses

La diapositive présente un concept essentiel en réseau appelé agrégation d'adresses ou résumé de route, utilisant le système CIDR. Ce système permet d'optimiser et de simplifier les tables de routage dans les réseaux informatiques.

#### Fonctionnement de l'Agrégation d'Adresses :

- Quatre sous-réseaux distincts :
  - 192.16.12.0/24
  - 192.16.13.0/24
  - 192.16.14.0/24
  - 192.16.15.0/24
- Peuvent être agrégés en un seul bloc : 192.16.12.0/22.
- Le routeur D contient des entrées détaillées pour chaque sous-réseau tandis que le routeur E utilise un résumé de route pour tous.

#### Application Pratique

- **Planification de Réseau** : Les ingénieurs réseau utilisent CIDR pour la conception de réseaux, permettant une utilisation plus flexible et une allocation des adresses IP.
- **Optimisation des Performances** : Les administrateurs système s'appuient sur l'agrégation d'adresses pour optimiser la performance des appareils de routage, en particulier dans les réseaux étendus.

L'agrégation d'adresses est une technique importante pour les professionnels du réseau, car elle facilite la gestion des grandes infrastructures en réduisant la taille des tables de routage et en améliorant la performance des réseaux.



- Visualisation de configuration  
ipconfig/all  
(linux ifconfig ou ip a)

## Démonstration

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

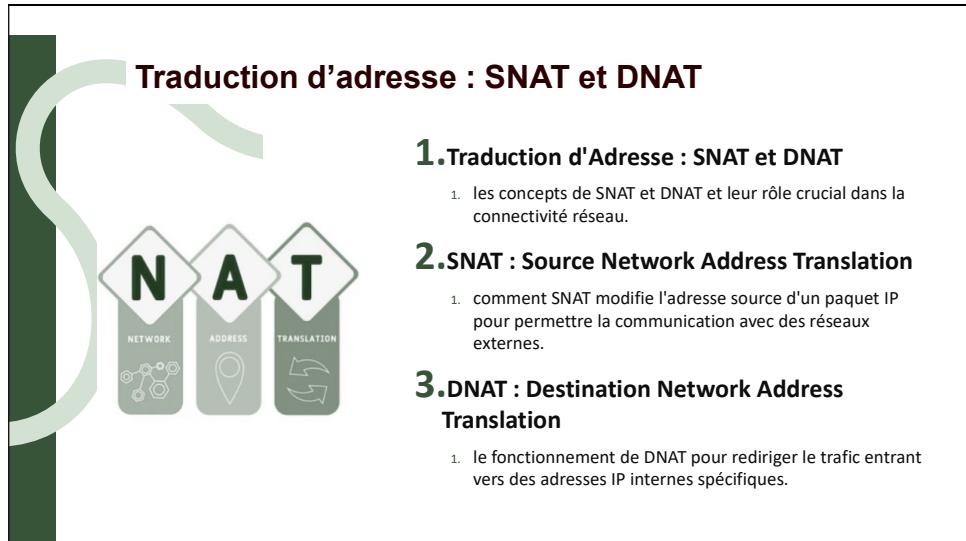
---

---

---

---

---



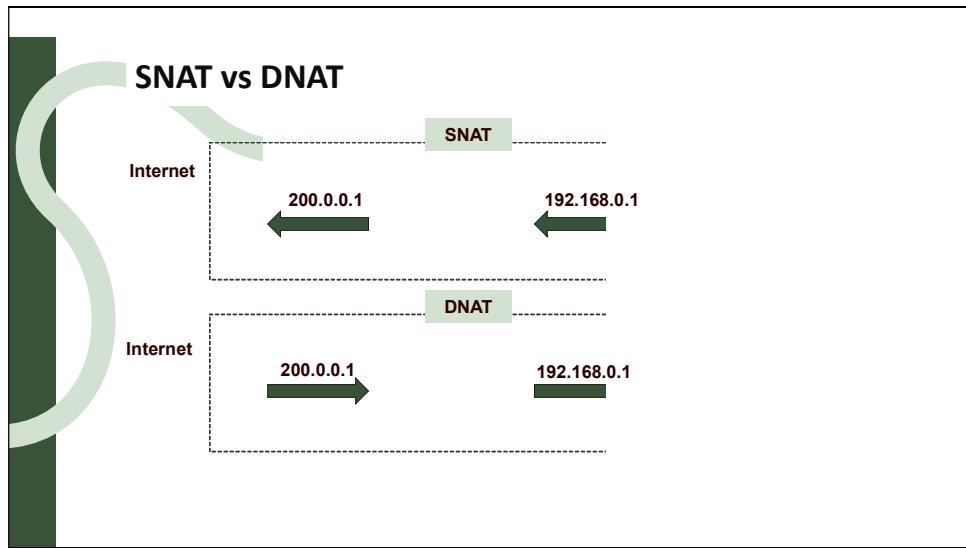
### Traduction d'Adresse : SNAT et DNAT

La traduction d'adresse réseau (NAT) est une technique utilisée pour modifier les adresses IP et les numéros de port des paquets IP lorsqu'ils traversent un périphérique de réseau, tel qu'un routeur ou un pare-feu. Deux types de NAT couramment utilisés sont la traduction d'adresse réseau source (SNAT) et la traduction d'adresse réseau de destination (DNAT).

**SNAT (Source Network Address Translation)** : Lorsqu'un périphérique à l'intérieur d'un réseau privé envoie un paquet à un périphérique à l'extérieur du réseau, SNAT modifie l'adresse source du paquet en remplaçant l'adresse IP source privée par une adresse IP publique attribuée par le routeur ou le pare-feu. Cela permet aux périphériques internes d'accéder à des ressources sur Internet tout en masquant leurs adresses IP privées.

**DNAT (Destination Network Address Translation)** : Lorsqu'un paquet est reçu depuis Internet, DNAT modifie l'adresse de destination du paquet pour rediriger le trafic vers un périphérique spécifique à l'intérieur du réseau privé. Cela permet de publier des services internes, tels que des serveurs Web ou de messagerie, sur Internet, en redirigeant le trafic entrant vers les adresses IP internes correspondantes.

La traduction d'adresse est essentielle pour permettre la connectivité entre les réseaux privés et Internet tout en préservant la sécurité et en simplifiant la gestion des adresses IP. En compréhension des concepts de SNAT et DNAT, les administrateurs réseau peuvent configurer efficacement leurs périphériques réseau pour répondre aux besoins de connectivité de leur organisation.



### **SNAT (Source Network Address Translation)**

#### **Fonctionnement :**

- SNAT modifie l'adresse IP source d'un paquet sortant. C'est souvent utilisé pour masquer les adresses IP internes d'un réseau local lorsqu'elles accèdent à l'internet.

#### **Exemple sur la Diapositive :**

- Un ordinateur dans le réseau local avec l'adresse IP 192.168.0.1 envoie un paquet à l'internet.
- Le routeur ou le pare-feu modifie l'adresse source de 192.168.0.1 en une adresse IP publique 200.0.0.1 avant d'envoyer le paquet sur l'internet.

#### **Applications Pratiques :**

- Permet aux multiples appareils d'un réseau privé d'accéder à l'internet utilisant une seule adresse IP publique.
- Améliore la sécurité en masquant les adresses IP internes du réseau local.

#### **Messages Clés :**

- SNAT est essentiel pour la confidentialité et la conservation des adresses IP.
- Simplifie la gestion du réseau en réduisant le besoin d'adresses IP publiques uniques pour chaque appareil.

### **DNAT (Destination Network Address Translation)**

#### **Fonctionnement :**

- DNAT modifie l'adresse IP de destination d'un paquet entrant, généralement utilisé pour rediriger les paquets entrants vers un appareil spécifique sur un réseau privé.

#### **Exemple sur la Diapositive :**

- Un paquet provenant de l'internet destiné à l'adresse IP publique 200.0.0.1 est modifié par le routeur ou le pare-feu pour être redirigé vers un ordinateur spécifique dans le réseau local avec l'adresse IP 192.168.0.1.

#### **Applications Pratiques :**

- Permet aux serveurs situés dans un réseau privé d'être accessibles depuis l'internet.
- Utilisé pour la redirection de ports pour les services comme les serveurs web, FTP, ou VPN.



— Montrer la connexion au site [www.mon-ip.com](http://www.mon-ip.com)

## Démonstration

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---



## **Adressage de niveau quatre : Les sockets. visualisation de leur état avec netstat. tcpview. gestionnaire de tâche**

- 1. Adressage de Niveau 4 : Les Sockets**
  - le concept des sockets et leur importance dans la communication réseau.
- 2. Visualisation avec Netstat**
  - comment utiliser Netstat pour afficher l'état des sockets et les connexions réseau actives.
- 3. Outils de Visualisation : TCPView et Gestionnaire de Tâches**
  - utiliser des outils comme TCPView et le Gestionnaire de Tâches pour une visualisation détaillée des sockets et des connexions réseau.

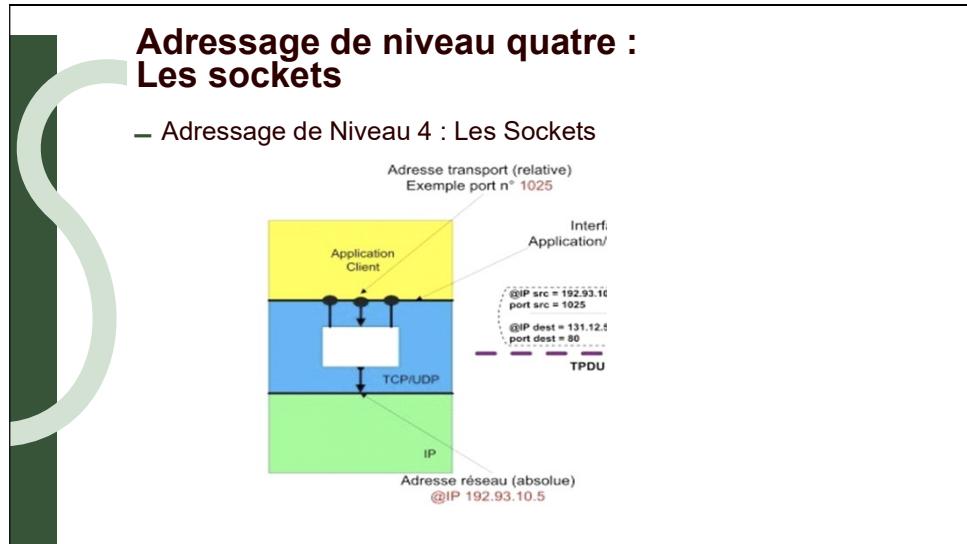
### **Adressage de Niveau 4 : Les Sockets et Visualisation**

Les sockets sont des interfaces de programmation utilisées pour établir des connexions de communication bidirectionnelles entre deux programmes sur un réseau. Ils jouent un rôle crucial dans la communication de niveau 4 (transport) du modèle OSI.

**Visualisation avec Netstat :** Netstat est une commande de ligne de commande permettant d'afficher diverses informations sur les connexions réseau actives, y compris les sockets. En utilisant des options spécifiques, comme -a pour afficher toutes les connexions et les ports en écoute, -n pour afficher les adresses IP et les numéros de port numériquement, et -o pour afficher les identifiants de processus (PID), les stagiaires peuvent obtenir une vue détaillée des connexions réseau en cours.

**Outils de Visualisation : TCPView et Gestionnaire de Tâches :** En plus de Netstat, des outils graphiques comme TCPView (sous Windows) ou le Gestionnaire de Tâches offrent une interface conviviale pour visualiser les sockets et les connexions réseau. Ces outils fournissent des informations supplémentaires telles que les noms des applications associées aux connexions et les processus correspondants.

En comprenant les sockets et en utilisant des outils de visualisation tels que Netstat, TCPView et le Gestionnaire de Tâches, les administrateurs réseau peuvent diagnostiquer les problèmes de connectivité, surveiller les activités réseau et optimiser les performances du réseau de manière efficace.



**Les sockets** sont utilisés pour établir une connexion point-à-point entre le client et le serveur pour la communication réseau. Ils sont essentiels pour le transfert de données en utilisant des protocoles comme TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol).

### Composants d'un Socket :

- **Adresse IP** : Identifie de manière unique l'hôte sur le réseau.
- **Numéro de Port** : Identifie de manière unique l'application au sein de l'hôte.

### Exemples sur la Diapositive :

- Un client utilise le port 1025 pour se connecter à un serveur sur le port 80, qui est le port standard pour le trafic HTTP.
- L'adresse IP source est 192.93.10.5 et le port source est 1025.
- L'adresse IP de destination est 131.12.5.97 et le port de destination est 80.

### Plages de Ports :

- **Ports Bien Connus (Well-known Ports)** : De 0 à 1023, assignés aux services standard comme le HTTP, le FTP, etc.
- **Ports Enregistrés (Registered Ports)** : De 1024 à 49151, généralement utilisés pour les applications utilisateur.
- **Ports Dynamiques ou Privés** : De 49152 à 65535, pour l'usage interne des applications.

### Application Pratique

- **Développement d'Applications** : Les développeurs d'applications utilisent des sockets pour établir des connexions réseau pour des services comme les bases de données, les services web et le chat en ligne.
  - **Sécurité du Réseau** : Les administrateurs réseau peuvent configurer des pare-feu et des systèmes de prévention d'intrusion basés sur des numéros de ports spécifiques pour sécuriser les communications.
- Les sockets sont fondamentaux pour la communication sur les réseaux informatiques, permettant le fonctionnement de diverses applications et services sur internet.

## S Adressage de niveau quatre : netstat

- Syntaxe de netstat (pour visualiser les sockets)
  - netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p <protocole>] [-r] [-s] [intervalle]
  - netstat -an | more

Connexions actives	
Proto	Adresse locale
TCP	0.0.0.0:17
TCP	0.0.0.0:19
TCP	0.0.0.0:13
TCP	0.0.0.0:17
TCP	0.0.0.0:19
TCP	0.0.0.0:139
TCP	0.0.0.0:445
TCP	0.0.0.0:808
TCP	0.0.0.0:902
TCP	0.0.0.0:912
TCP	0.0.0.0:2008
TCP	0.0.0.0:1290
TCP	0.0.0.0:1045
TCP	0.0.0.0:7680
TCP	0.0.0.0:139000
TCP	0.0.0.0:49664
TCP	0.0.0.0:49665
TCP	0.0.0.0:49666
TCP	0.0.0.0:49667
TCP	0.0.0.0:49668
TCP	0.0.0.0:49701
TCP	0.0.0.0:58085
TCP	10.10.10.9:139
TCP	127.0.0.1:5354
TCP	127.0.0.1:2490

### Utilité de netstat :

- netstat est une commande qui permet de diagnostiquer des problèmes de réseau et de déterminer la quantité de trafic sur le réseau.

### Options Communes :

- -a : Affiche tous les ports actifs et les connexions (TCP et UDP).
- -b : Montre le programme associé à chaque connexion (Windows).
- -e : Affiche les statistiques Ethernet, comme les erreurs et les paquets envoyés ou reçus.
- -n : Affiche les adresses et les ports en format numérique, plutôt que d'essayer de déterminer les noms.
- -o : Montre les ID de processus associés aux connexions (Windows).
- -p <protocole> : Affiche les connexions pour un protocole spécifique (TCP, UDP).
- -r : Affiche la table de routage.
- -s : Affiche les statistiques par protocole.
- [intervalle] : Met à jour les informations affichées à intervalles réguliers.

### Exemple d'Utilisation :

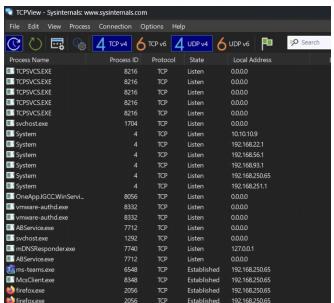
- netstat -an | more : Affiche toutes les connexions et ports d'écoute (-a) et utilise le format numérique pour les adresses et les ports (-n). L'ajout de | more permet de parcourir les résultats page par page si les résultats sont trop nombreux pour tenir sur une seule page.

### Application Pratique

- **Gestion de Réseau** : Les administrateurs système et réseau utilisent netstat pour gérer et surveiller les réseaux en temps réel.
  - **Dépannage** : netstat est un outil de première ligne pour le dépannage des problèmes de connectivité et d'application.
- En apprenant à utiliser netstat, les professionnels et les étudiants en réseau peuvent gagner en visibilité sur l'état et la performance de leurs systèmes de réseau.

## S Adressage de niveau quatre : tcpview

- Sysinternals :
  - Live.sysinternal.com
  - Tcpview.exe



### Sysinternals :

- Un ensemble d'outils de diagnostic et de dépannage pour Windows, créé par Mark Russinovich et Bryce Cogswell, maintenant hébergé et maintenu par Microsoft.

### Fonctionnalités de TCPView :

- TCPView.exe offre une interface graphique dynamique montrant en temps réel toutes les connexions réseau actives.
- Contrairement à netstat, TCPView actualise automatiquement sa liste et peut être plus convivial pour les utilisateurs qui préfèrent une interface graphique.

### Application Pratique

- **Détection de Malware** : TCPView peut aider à identifier les connexions suspectes qui pourraient être dues à des logiciels malveillants ou à des applications non autorisées.
- **Dépannage des Applications** : Les développeurs et les administrateurs peuvent utiliser TCPView pour diagnostiquer les problèmes de connectivité d'une application. TCPView est un outil précieux pour toute personne qui gère des systèmes Windows, offrant une visibilité claire sur les opérations réseau qui pourraient autrement passer inaperçues.



## TCP - Fonctionnalités, cas d'utilisation (fiabilité transfert de données)

- TCP : Fiabilité et Transfert de Données
  - les fonctionnalités de TCP en termes de fiabilité et de transfert de données.
- Différenciation TCP vs UDP
  - les différences fondamentales entre TCP et UDP et leurs implications sur les transferts de données.
- Cas d'Utilisation de TCP
  - les scénarios où TCP est préféré pour assurer la fiabilité et l'intégrité des données.

### TCP : Fiabilité et Transfert de Données

TCP (Transmission Control Protocol) est un protocole de transport fiable qui assure l'acheminement sûr et ordonné des données sur un réseau. Contrairement à UDP (User Datagram Protocol), TCP garantit la livraison des données sans perte ni duplication, ce qui le rend idéal pour les applications nécessitant une transmission fiable.

**Différenciation TCP vs UDP :** La principale différence entre TCP et UDP réside dans leur approche de livraison des données. TCP établit une connexion bidirectionnelle avant de transférer des données, utilise un mécanisme de suivi des paquets pour garantir la réception dans l'ordre et offre un contrôle de flux pour éviter la surcharge du réseau. En revanche, UDP est plus simple et n'assure pas la fiabilité ni l'ordonnancement des données, ce qui le rend approprié pour les applications nécessitant une latence minimale, telles que la diffusion en continu et la voix sur IP.

**Cas d'Utilisation de TCP :** TCP est largement utilisé dans des applications telles que le web, le courrier électronique, le transfert de fichiers et les transactions en ligne où la fiabilité et l'intégrité des données sont primordiales. Par exemple, lors de la navigation sur le Web, TCP garantit que toutes les parties d'une page Web sont reçues et affichées correctement, même en cas de perte ou de réarrangement de paquets sur le réseau.

En compréhension des fonctionnalités de TCP et en identifiant les cas d'utilisation appropriés, les administrateurs réseau peuvent choisir le protocole de transport le mieux adapté à leurs besoins spécifiques en matière de transfert de données et de fiabilité.



**TCP - Cinématiques : connexion. échange de données (correction d'erreur. contrôle de flux). déconnexions**

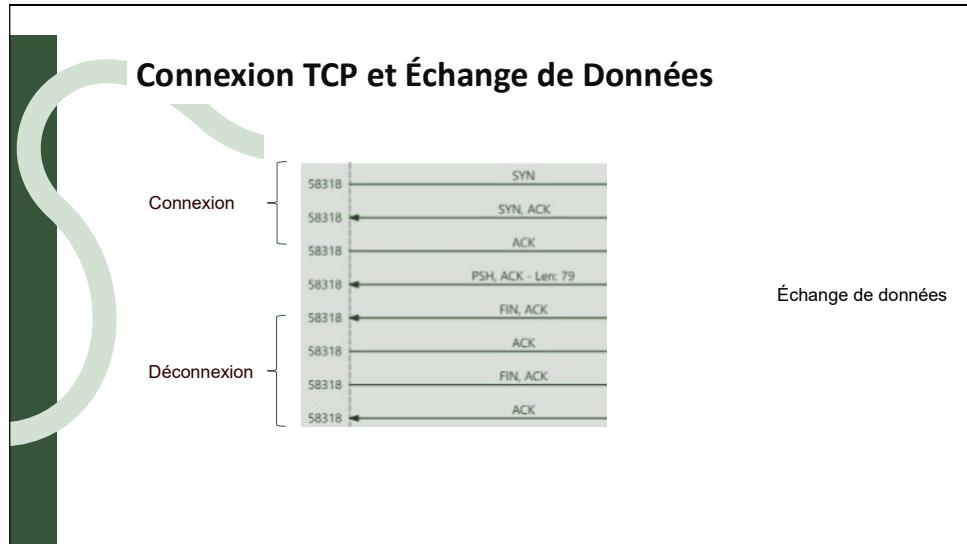
- Cinématiques TCP : Connexion. Échange de Données et Déconnexion
  - ▶ les séquences de connexion, d'échange de données et de déconnexion pour TCP, ainsi que le comportement de UDP.
- Correction d'Erreur et Contrôle de Flux
  - ▶ comment TCP gère la correction d'erreur et le contrôle de flux pour assurer la fiabilité et les performances du transfert de données.
- Analyse Pratique avec Wireshark
  - ▶ comment analyser ces séquences en pratique à l'aide de Wireshark pour mieux comprendre le fonctionnement des protocoles TCP et UDP.

### **Cinématiques TCP : Connexion. Échange de Données et Déconnexion**

TCP suit une séquence bien définie lors de l'établissement d'une connexion, du transfert de données et de la déconnexion. Lors de la phase de connexion, TCP utilise un processus en trois temps (SYN, SYN-ACK, ACK) pour établir une connexion bidirectionnelle entre le client et le serveur. Pendant l'échange de données, TCP garantit l'ordre et l'intégrité des paquets en utilisant des numéros de séquence et d'acquittement, ainsi que des mécanismes de retransmission et de correction d'erreur pour assurer la fiabilité du transfert. Enfin, lors de la déconnexion, TCP utilise un processus en quatre temps (FIN, ACK-FIN, FIN, ACK) pour fermer la connexion de manière ordonnée.

**Correction d'Erreur et Contrôle de Flux :** TCP utilise des mécanismes de correction d'erreur tels que les numéros de séquence et d'acquittement pour garantir la fiabilité du transfert de données. De plus, TCP utilise le contrôle de flux pour éviter la congestion du réseau en ajustant dynamiquement la vitesse de transmission en fonction de la capacité du réseau et de la réception des données par le destinataire. En comprenant ces mécanismes, les administrateurs réseau peuvent optimiser les performances du réseau et garantir une communication fluide et fiable.

**Analyse Pratique avec Wireshark :** Wireshark est un outil puissant pour analyser le trafic réseau en temps réel. En utilisant Wireshark, les administrateurs réseau peuvent capturer et examiner le trafic TCP et UDP pour comprendre les séquences de connexion, d'échange de données et de déconnexion. En analysant ces séquences, les stagiaires peuvent mieux comprendre le comportement des protocoles TCP et UDP et diagnostiquer les problèmes éventuels dans les communications réseau.



## Connexion TCP et Échange de Données

### Établissement de la Connexion (Three-Way Handshake) :

- **SYN** : Le client envoie un paquet SYN au serveur pour demander une connexion.
- **SYN-ACK** : Le serveur répond avec un paquet SYN-ACK pour reconnaître la demande de connexion.
- **ACK** : Le client envoie un paquet ACK pour confirmer la réception du paquet SYN-ACK et établir la connexion.

### Échange de Données :

- **PSH-ACK avec Données** : Une fois la connexion établie, les données peuvent être échangées. Le flag PSH indique que les données doivent être transmises immédiatement.

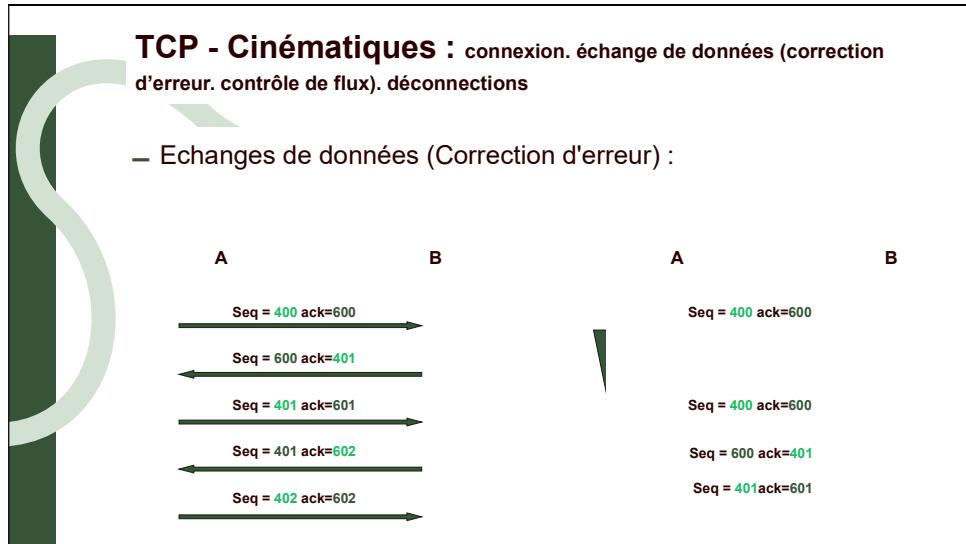
### Terminaison de la Connexion :

- **FIN-ACK** : Un paquet FIN-ACK est envoyé par l'une des parties pour initier la fermeture de la connexion.
- **ACK** : L'autre partie envoie un paquet ACK en réponse au FIN-ACK.
- **FIN-ACK** : L'autre partie envoie ensuite son propre paquet FIN-ACK pour confirmer qu'elle a terminé l'envoi des données.
- **ACK** : Le premier expéditeur répond avec un paquet ACK final, et la connexion est fermée des deux côtés.

### Application Pratique

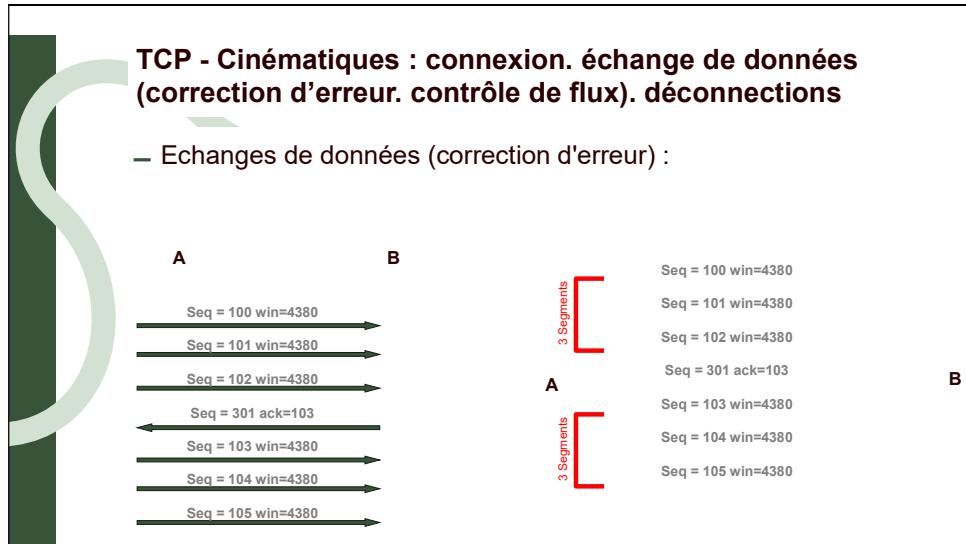
- **Communication Fiable** : TCP est utilisé par des applications nécessitant une communication fiable, comme les navigateurs web, les e-mails et les transferts de fichiers.
- **Analyse du Réseau** : Les administrateurs réseau utilisent la compréhension de ce processus pour dépanner les problèmes de réseau et surveiller la performance des applications.

La compréhension des étapes de connexion et de déconnexion TCP est fondamentale pour ceux qui travaillent avec des réseaux TCP/IP, car elle affecte directement la performance et la stabilité des communications réseau.



TCP inclut un mécanisme de correction d'erreurs pour s'assurer que les données envoyées sont reçues sans altération. Voici comment cela fonctionne :

- **Numérotation des séquences** : TCP numérote chaque octet de données envoyé. Le récepteur utilise ces numéros de séquence pour reconstruire les données dans le bon ordre et détecter les éventuelles pertes ou duplications.
- **Acquittements (ACK)** : Lorsque le récepteur reçoit des données, il envoie un acquittement au transmetteur pour indiquer qu'il a bien reçu ces données. Si le transmetteur ne reçoit pas d'acquittement après un certain temps, il réémet les données.
- **Timeouts** : Si le transmetteur n'a pas reçu d'acquittement dans un délai donné, il suppose que les données ont été perdues et les réémet.
- **Contrôle de flux** : TCP utilise un mécanisme de contrôle de flux pour éviter que le récepteur ne soit submergé par un débit de données trop élevé. Le récepteur peut indiquer au transmetteur le nombre d'octets qu'il est prêt à accepter.
- **Répétition sélective** : Plutôt que de retransmettre tout le segment en cas de perte, TCP peut identifier spécifiquement les segments manquants et les retransmettre, ce qui réduit la surcharge du réseau.
- **Checksums** : TCP utilise des sommes de contrôle (checksums) pour vérifier l'intégrité des données. Le récepteur vérifie le checksum des données reçues pour détecter toute altération. Si le checksum est incorrect, les données sont rejetées et le transmetteur est invité à les renvoyer.



### Correction d'Erreur dans TCP :

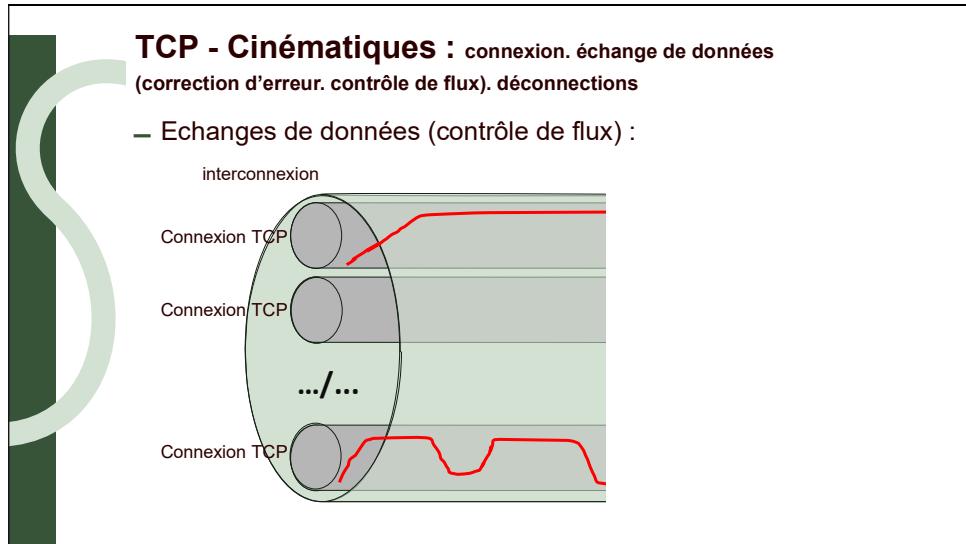
- TCP garantit la livraison des données sans erreur en utilisant un mécanisme de numéro de séquence (Seq) et d'accusé de réception (ack).
- Chaque segment de données envoyé par TCP est numéroté séquentiellement.
- Le destinataire utilise les numéros d'accusé de réception pour confirmer la réception des segments.

### Exemple de la Diapositive :

- L'ordinateur A envoie des segments de données avec des numéros de séquence consécutifs (100, 101, 102...) à l'ordinateur B.
- Si un segment (ici avec Seq=102) est perdu, l'ordinateur B envoie un accusé de réception avec le numéro de séquence attendu suivant (ack=103), signalant à A de renvoyer le segment manquant.
- Le mécanisme de contrôle de flux, indiqué par win=4380, montre la taille de la fenêtre de réception, c'est-à-dire le nombre d'octets que B est prêt à recevoir.

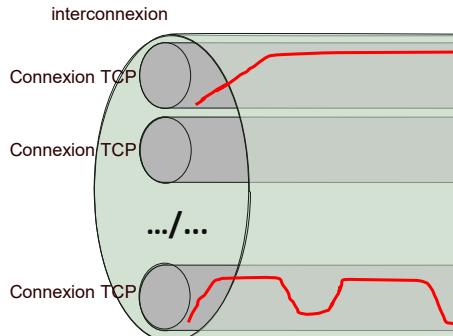
### Application Pratique

- **Transmission de Données Critiques** : Idéal pour les applications nécessitant une garantie de livraison, comme les transferts de fichiers et les bases de données.
- **Optimisation du Réseau** : La correction d'erreur permet d'optimiser l'utilisation de la bande passante et de réduire la congestion du réseau.  
La compréhension de la correction d'erreur est vitale pour ceux qui conçoivent et maintiennent des réseaux fiables et efficaces, ainsi que pour les développeurs qui créent des applications qui utilisent des connexions réseau.



### TCP - Cinématiques : connexion. échange de données (correction d'erreur. contrôle de flux). déconnexions

#### – Echanges de données (contrôle de flux) :



### TCP - Cinématiques : Échanges de Données (Contrôle de Flux)

#### Contrôle de Flux dans TCP :

- Le contrôle de flux est un mécanisme de TCP qui permet à l'expéditeur et au destinataire de gérer efficacement la quantité de données en transit. Cela évite que l'expéditeur n'envoie plus de données que le destinataire ne peut en traiter à un moment donné.

#### Fonctionnement :

- La taille de la "fenêtre" (Window Size) dans les en-têtes TCP indique la quantité de données (en octets) que le destinataire est prêt à accepter.
- L'expéditeur ajuste la vitesse d'envoi des données en fonction de la taille de la fenêtre pour éviter la saturation du buffer du destinataire.

#### Application Pratique

- **Gestion de Réseau** : Les administrateurs réseau doivent comprendre et surveiller le contrôle de flux pour maintenir la performance du réseau, en particulier dans les environnements avec des volumes de données élevés.
  - **Développement d'Applications** : Les développeurs d'applications réseau doivent intégrer des mécanismes de contrôle de flux pour assurer la fiabilité et l'efficacité des communications.
- Le contrôle de flux est crucial dans tous les scénarios où la fiabilité de la transmission des données est une priorité, comme les systèmes de transfert de fichiers, les communications vidéo et audio en streaming, et les applications de messagerie instantanée.



Observation des cinématiques  
TCP avec Wireshark

## Démonstration



## UDP - Fonctionnalités, cas d'utilisation (temps réel, Transactionnel, Transfert de Données)

- UDP : Fonctionnalités et Cas d'Utilisation
  - ▶ les fonctionnalités principales d'UDP et découvrez ses cas d'utilisation typiques dans les environnements temps réel et transactionnels.
- Applications Temps Réel
  - ▶ comment UDP est utilisé dans les applications temps réel telles que la voix sur IP (VoIP), la diffusion en continu et les jeux en ligne pour offrir une communication rapide et réactive.
- Applications Transactionnelles
  - ▶ les cas d'utilisation d'UDP dans les applications transactionnelles telles que les services DNS (Domain Name System) et SNMP (Simple Network Management Protocol) pour des transactions rapides et efficaces.

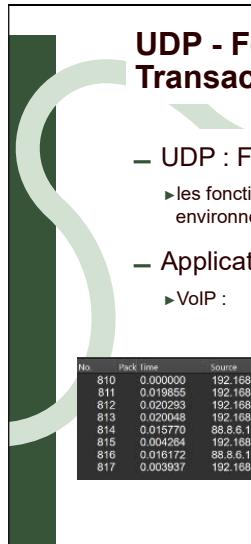
### Fonctionnalités et Cas d'Utilisation

UDP (User Datagram Protocol) est un protocole de communication sans connexion qui offre des fonctionnalités simples mais rapides pour le transfert de données. Contrairement à TCP, UDP ne garantit pas la livraison des paquets ni leur ordre, ce qui le rend idéal pour les applications où la vitesse et la réactivité sont plus importantes que la fiabilité.

**Applications Temps Réel :** UDP est largement utilisé dans les applications temps réel telles que la voix sur IP (VoIP), la diffusion en continu (streaming), les jeux en ligne et les vidéos en direct. Dans ces applications, la latence est critique, et UDP permet une transmission rapide des données sans surcharge de gestion de connexion.

**Applications Transactionnelles :** UDP est également utilisé dans les applications transactionnelles où des transactions rapides sont nécessaires. Par exemple, les services DNS (Domain Name System) utilisent UDP pour les requêtes de résolution de noms de domaine, et SNMP (Simple Network Management Protocol) utilise UDP pour la surveillance et le contrôle des équipements réseau. Dans ces cas, la rapidité de transmission est privilégiée par rapport à la fiabilité, car les pertes occasionnelles de paquets peuvent être tolérées.

En comprenant les fonctionnalités et les cas d'utilisation d'UDP, les administrateurs réseau peuvent choisir le bon protocole pour répondre aux besoins spécifiques de leurs applications et optimiser les performances du réseau.



## UDP - Fonctionnalités, cas d'utilisation (temps réel, Transactionnel, Transfert de Données)

- UDP : Fonctionnalités et Cas d'Utilisation
  - les fonctionnalités principales d'UDP et découvrez ses cas d'utilisation typiques dans les environnements temps réel et transactionnels.
- Applications Temps Réel
  - VoIP :

No	Pack time	source	Destination	Protocol	Protocol-App	Length	Lenq Info
810	0.000000	192.168.146.10	88.8.6.10	UDP	RTP	...	PT=ITU-T G.7
811	0.019855	192.168.146.10	88.8.6.10	UDP	RTP	...	PT=ITU-T G.7
812	0.020293	192.168.146.10	88.8.6.10	UDP	RTP	...	PT=ITU-T G.7
813	0.020048	192.168.146.10	88.8.6.10	UDP	RTP	...	PT=ITU-T G.7
814	0.015770	88.8.6.10	192.168.146.10	UDP	RTP	...	PT=ITU-T G.7
815	0.004264	192.168.146.10	88.8.6.10	UDP	RTP	...	PT=ITU-T G.7
816	0.016172	88.8.6.10	192.168.146.10	UDP	RTP	...	PT=ITU-T G.7
817	0.003937	192.168.146.10	88.8.6.10	UDP	RTP	...	PT=ITU-T G.7

### Fonctionnalités et Cas d'Utilisation

UDP (User Datagram Protocol) est un protocole de communication sans connexion qui offre des fonctionnalités simples mais rapides pour le transfert de données. Contrairement à TCP, UDP ne garantit pas la livraison des paquets ni leur ordre, ce qui le rend idéal pour les applications où la vitesse et la réactivité sont plus importantes que la fiabilité.

**Applications Temps Réel** : UDP est largement utilisé dans les applications temps réel telles que la voix sur IP (VoIP), la diffusion en continu (streaming), les jeux en ligne et les vidéos en direct. Dans ces applications, la latence est critique, et UDP permet une transmission rapide des données sans surcharge de gestion de connexion.

## UDP - Fonctionnalités, cas d'utilisation (temps réel, Transactionnel, Transfert de Données)

– Applications Transactionnelles

- ▶ les cas d'utilisation d'UDP dans les applications transactionnelles telles que les services DNS (Domain Name System) et SNMP (Simple Network Management Protocol) pour des transactions rapides et efficaces.
- ▶ DNS :

No.	Pkt. Time	Source	Destination	Protocol	Protocol App	Length Info	
0	125	0.000000	192.168.146.10	dns.google	UDP	DNS	70 Standard query 0xa052 A www.google.com
1	126	0.020492	dns.google	192.168.146.10	UDP	DNS	161 Standard query response 0xa052 A

### Fonctionnalités et Cas d'Utilisation

UDP (User Datagram Protocol) est un protocole de communication sans connexion qui offre des fonctionnalités simples mais rapides pour le transfert de données. Contrairement à TCP, UDP ne garantit pas la livraison des paquets ni leur ordre, ce qui le rend idéal pour les applications où la vitesse et la réactivité sont plus importantes que la fiabilité.

**Applications Transactionnelles** : UDP est également utilisé dans les applications transactionnelles où des transactions rapides sont nécessaires. Par exemple, les services DNS (Domain Name System) utilisent UDP pour les requêtes de résolution de noms de domaine, et SNMP (Simple Network Management Protocol) utilise UDP pour la surveillance et le contrôle des équipements réseau. Dans ces cas, la rapidité de transmission est privilégiée par rapport à la fiabilité, car les pertes occasionnelles de paquets peuvent être tolérées.

En comprenant les fonctionnalités et les cas d'utilisation d'UDP, les administrateurs réseau peuvent choisir le bon protocole pour répondre aux besoins spécifiques de leurs applications et optimiser les performances du réseau.



## UDP - Fonctionnalités, cas d'utilisation (temps réel, Transactionnel, Transfert de Données)

1. Cinématiques UDP
  1. les étapes de connexion, le transfert de données et les méthodes de gestion des erreurs dans le protocole UDP.
2. Connexion et Transfert de Données
  1. comment UDP gère la communication sans connexion et examinez les défis liés à la transmission de données sans mécanisme de contrôle de flux.
3. Gestion des Erreurs
  1. les approches pour la gestion des erreurs dans UDP, y compris les méthodes de retransmission et de détection des pertes de paquets.

### Cinématiques UDP

UDP (User Datagram Protocol) est un protocole de communication sans connexion, ce qui signifie qu'il ne nécessite pas d'établir une connexion avant de transférer des données. Cela présente à la fois des avantages et des inconvénients par rapport à TCP.

**Connexion et Transfert de Données :** Contrairement à TCP, UDP n'a pas d'étape de connexion formelle. Les données sont simplement envoyées sous forme de datagrammes, ce qui rend le transfert plus rapide mais moins fiable. UDP ne fournit pas de mécanisme de contrôle de flux pour réguler le flux de données, ce qui signifie qu'il peut y avoir des pertes de paquets ou de la congestion dans le réseau.

**Gestion des Erreurs :** UDP ne garantit pas la livraison des paquets ni leur ordre, et il n'y a pas de mécanisme intégré pour la gestion des erreurs. Les applications utilisant UDP doivent mettre en œuvre leurs propres méthodes de détection des pertes de paquets et de retransmission si nécessaire. Cela rend UDP moins adapté aux applications où la fiabilité est primordiale, mais il peut être plus efficace pour les applications où la latence et la vitesse de transfert sont plus importantes que la fiabilité.

En comprenant les cinématiques d'UDP, les administrateurs réseau peuvent choisir le bon protocole pour répondre aux besoins spécifiques de leurs applications et optimiser les performances du réseau.

### UDP - Fonctionnalités, cas d'utilisation (temps réel, Transactionnel, Transfert de Données)

– Cas du protocole TFTP :

Numéro	Port Source	Port Destination	Opération	Protocole	Type	Message
70	0.0.0.0:0	192.168.146.11	192.168.146.10	UDP	TFTP	81 Write Request, File: top.pdf, Transfer type: octet, 0
73	0.3.27306	192.168.146.10	192.168.146.11	UDP	TFTP	65 Option Acknowledgement, bsize=512 [Malformed]
74	0.0.0.0:0	192.168.146.10	192.168.146.11	UDP	TFTP	48 Acknowledgement, Block: 1
75	0.0.0.0:162	192.168.146.10	192.168.146.11	UDP	TFTP	558 Data Packet, Block: 1
76	0.0.0.0:0	192.168.146.10	192.168.146.11	UDP	TFTP	48 Acknowledgement, Block: 2
77	0.0.0.0:0	192.168.146.10	192.168.146.11	UDP	TFTP	558 Data Packet, Block: 3
78	0.0.0.1343	192.168.146.11	192.168.146.10	UDP	TFTP	47 Acknowledgement, Block: 3
79	0.0.0.0:0	192.168.146.11	192.168.146.10	UDP	TFTP	558 Data Packet, Block: 4
80	0.0.0.1306	192.168.146.11	192.168.146.10	UDP	TFTP	48 Data Packet, Block: 18 (last)
108	0.0.0.77950	192.168.146.10	192.168.146.11	UDP	TFTP	48 Acknowledgement, Block: 18
109	0.0.0.0:0	192.168.146.10	192.168.146.11	UDP	TFTP	

TFTP (Trivial File Transfer Protocol) est un protocole de transfert de fichiers simple, souvent utilisé pour le transfert de fichiers entre des périphériques sur un réseau local. Voici comment il fonctionne :

- **Connexion initiale** : Le client TFTP envoie une demande de connexion au serveur TFTP sur le port 69 UDP (User Datagram Protocol).
- **Mode de transfert** : Le client spécifie le mode de transfert souhaité, qui peut être soit le mode binaire (octet par octet) soit le mode ASCII (caractère par caractère).
- **Transfert de fichiers** :
  - Le client envoie une demande de lecture (RRQ - Read Request) au serveur pour obtenir un fichier ou une demande d'écriture (WRQ - Write Request) pour envoyer un fichier.
  - Le serveur répond en envoyant le fichier demandé ou en confirmant que le fichier peut être écrit.
  - Les données du fichier sont transférées en blocs de 512 octets (par défaut) entre le client et le serveur.
  - Chaque bloc de données est accompagné d'un numéro de bloc pour suivre l'ordre des données.
  - Le serveur envoie un accusé de réception (ACK) pour chaque bloc reçu avec succès. S'il ne reçoit pas un ACK pour un bloc dans un certain délai, il le renvoie.
  - Le transfert continue jusqu'à ce que tout le fichier soit transféré.
- **Terminaison de la connexion** :
  - Une fois le transfert de fichier terminé, le client envoie un message de terminaison au serveur.
  - Le serveur répond avec un message de terminaison confirmant la fin du transfert.
  - La connexion TFTP est ensuite fermée.

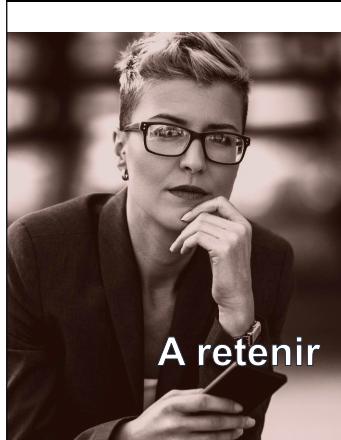
TFTP est souvent utilisé dans des environnements où une installation de serveur de fichiers plus robuste comme FTP n'est pas nécessaire, ou lorsque les ressources système sont limitées. Cependant, TFTP ne prend pas en charge l'authentification ni le chiffrement, ce qui le rend moins sécurisé que d'autres protocoles de transfert de fichiers



Observation des  
cinématiques UDP avec  
Wireshark

## Démonstration

- Ce qu'il faut retenir



- **Fondation de l'Internet**
- **Adressage IP : Identité sur le Réseau**
- **Protocoles de Communication Essentiels**
- **Résolution d'Adresses et Connexions Réseau**
- **Importance de la Configuration et de la Gestion du Réseau**

**Fondation de l'Internet :**

"Le modèle TCP/IP est le fondement sur lequel repose toute la communication sur Internet, permettant l'échange de données entre des ordinateurs sur des réseaux globalement interconnectés."

**Adressage IP : Identité sur le Réseau :**

"L'adressage IP fournit une identité unique à chaque appareil sur le réseau, facilitant le routage précis des informations à travers le vaste écosystème d'Internet."

**Protocoles de Communication Essentiels :**

"TCP assure une livraison fiable et ordonnée des données, tandis que UDP offre une méthode de transmission plus rapide mais sans garantie, chacun servant des cas d'utilisation spécifiques dans la communication en réseau."

**Résolution d'Adresses et Connexions Réseau :**

"Les protocoles comme ARP (Address Resolution Protocol) jouent un rôle crucial en liant les adresses IP aux adresses MAC physiques, permettant ainsi la formation effective de connexions réseau."

**Importance de la Configuration et de la Gestion du Réseau :**

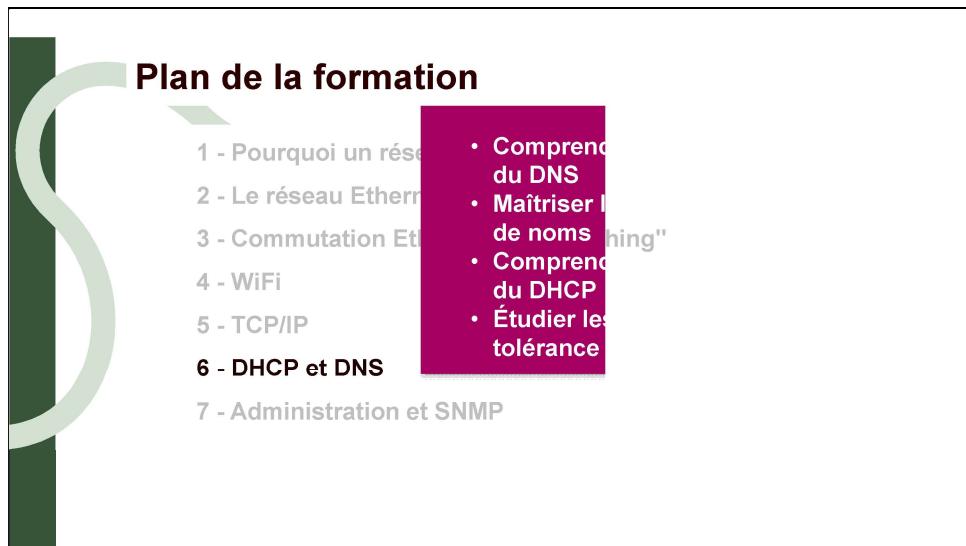
"La compréhension approfondie et la gestion adéquate des paramètres TCP/IP sont essentielles pour le dépannage, la sécurité et l'optimisation des performances du réseau."

## Chapitre 6 – DHCP et DNS

---

### 6 - DHCP et DNS

- Objectifs du chapitre



Les principaux objectifs du chapitre sur DHCP et DNS sont les suivants :

- Comprendre les principes fondamentaux du DNS :

- Expliquer le fonctionnement du DNS (Domain Name System) et son rôle dans la résolution des noms de domaine en adresses IP.
- Analyser l'architecture du système de nommage et la hiérarchie des domaines.
- Définir les concepts clés tels que les zones DNS, les rôles des serveurs DNS et les différents types d'enregistrements DNS.

- Maîtriser la cinématique de la résolution de noms :

- Décrire le processus de résolution de noms DNS, y compris la recherche de nom, la résolution de nom local et la résolution de nom récursive.
- Identifier les différentes étapes impliquées dans la résolution d'un nom de domaine.

- Comprendre les principes fondamentaux du DHCP :

- Expliquer le fonctionnement du DHCP (Dynamic Host Configuration Protocol) et son rôle dans l'attribution dynamique des adresses IP aux périphériques réseau.
- Analyser le processus de fonctionnement du DHCP, y compris le renouvellement des baux, la réservation d'adresses IP par adresse MAC et la gestion des pools d'adresses IP.

- Étudier les aspects de redondance et de tolérance de panne :

- Examiner les stratégies de mise en œuvre de la redondance et de la tolérance de panne dans les environnements DHCP, notamment l'utilisation de serveurs DHCP redondants et de relais DHCP dans les architectures réseau d'entreprise.

En abordant ces objectifs, les apprenants seront en mesure de comprendre en profondeur les principes, les fonctionnalités et les mécanismes de DHCP et DNS, ce qui leur permettra de configurer, gérer et optimiser efficacement ces services au sein de leurs réseaux.



- "Avez-vous déjà enregistré ou configuré un nom de domaine pour un site web ou un service ? Quels défis avez-vous rencontrés lors de ce processus ?"
- "Qu'arrive-t-il, selon vous, lorsque vous ne pouvez pas accéder à un site web par son nom, mais que la connexion via son adresse IP fonctionne ?"
- "Dans quelles situations avez-vous dû attribuer manuellement une adresse IP à un appareil ? Pourquoi était-ce nécessaire ?"
- "Avez-vous déjà eu un problème où vos appareils semblaient être connectés au réseau mais ne pouvaient pas accéder à Internet ? Comment avez-vous tenté de résoudre ce problème ?"
- "Comment assurez-vous que les sites web auxquels vous accédez sont légitimes et sécurisés ? Utilisez-vous des outils ou des méthodes spécifiques pour vérifier l'identité des sites ?"

**Expérience avec des Noms de Domaine :**

"Avez-vous déjà enregistré ou configuré un nom de domaine pour un site web ou un service ? Quels défis avez-vous rencontrés lors de ce processus ?"

**Compréhension de la Connexion Internet :**

"Qu'arrive-t-il, selon vous, lorsque vous ne pouvez pas accéder à un site web par son nom, mais que la connexion via son adresse IP fonctionne ?"

**Gestion des Adresses IP :**

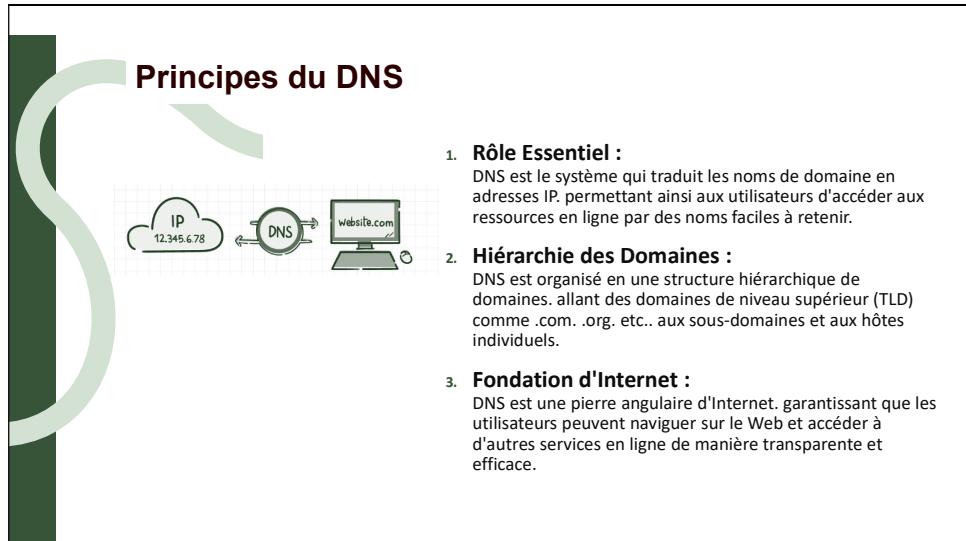
"Dans quelles situations avez-vous dû attribuer manuellement une adresse IP à un appareil ? Pourquoi était-ce nécessaire ?"

**Rencontre avec les Problèmes de Réseau :**

"Avez-vous déjà eu un problème où vos appareils semblaient être connectés au réseau mais ne pouvaient pas accéder à Internet ? Comment avez-vous tenté de résoudre ce problème ?"

**Sécurité et Nommage sur Internet :**

"Comment assurez-vous que les sites web auxquels vous accédez sont légitimes et sécurisés ? Utilisez-vous des outils ou des méthodes spécifiques pour vérifier l'identité des sites ?"



•**Rôle Essentiel** : Le DNS est le système qui traduit les noms de domaine en adresses IP. permettant ainsi aux utilisateurs d'accéder aux ressources en ligne par des noms faciles à retenir.

•**Hiérarchie des Domaines** : Le DNS est organisé en une structure hiérarchique de domaines. allant des domaines de niveau supérieur (TLD) comme .com. .org. etc.. aux sous-domaines et aux hôtes individuels.

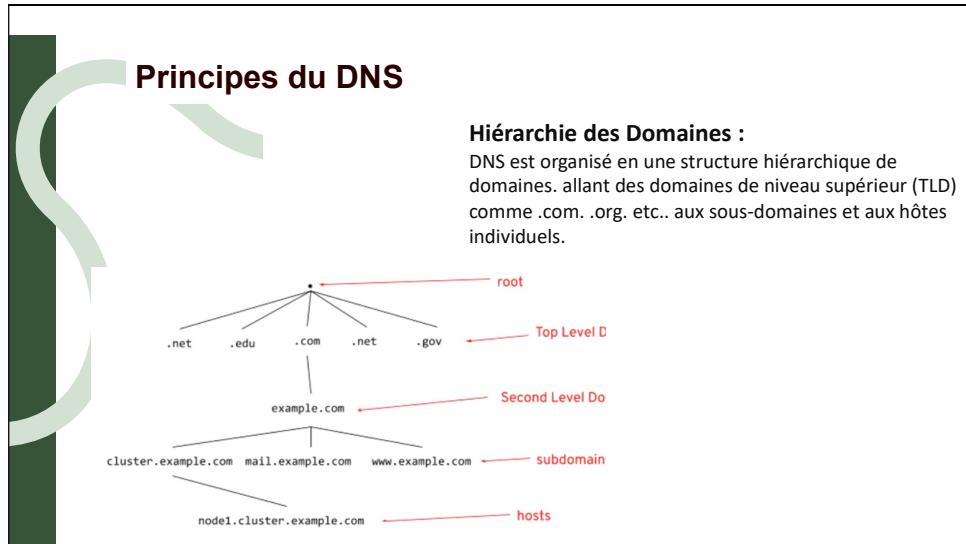
•**Fondation d'Internet** : Le DNS est une pierre angulaire d'Internet. garantissant que les utilisateurs peuvent naviguer sur le Web et accéder à d'autres services en ligne de manière transparente et efficace.

**Comprendre le Système de Noms de Domaine** Le système de noms de domaine (DNS) est un élément fondamental de l'infrastructure Internet. jouant un rôle crucial dans la façon dont les utilisateurs accèdent aux ressources en ligne. Voici quelques points essentiels à retenir sur le DNS :

**1. Traduction Noms de Domaine en Adresses IP** : Le DNS permet de traduire les noms de domaine. tels que [www.example.com](http://www.example.com). en adresses IP. comme 192.0.2.1. Cette traduction est indispensable pour que les utilisateurs puissent accéder aux serveurs et services en ligne en utilisant des noms faciles à retenir plutôt que des adresses IP complexes.

**2. Structure Hiérarchique** : Le DNS est organisé en une structure hiérarchique de domaines. similaire à l'arborescence d'un système de fichiers. Au sommet se trouvent les domaines de niveau supérieur (TLD). tels que .com. .org. .net. etc.. suivis des sous-domaines et des hôtes individuels. Cette hiérarchie facilite la gestion et la résolution des noms de domaine.

**3. Importance Fondamentale** : Le DNS est souvent décrit comme la "table des traductions" d'Internet. et pour cause. Sans le DNS. la navigation sur le Web et l'accès à d'autres services en ligne seraient considérablement plus compliqués. voire impossibles. Il est donc essentiel de comprendre son fonctionnement pour tirer pleinement parti des ressources disponibles sur Internet.

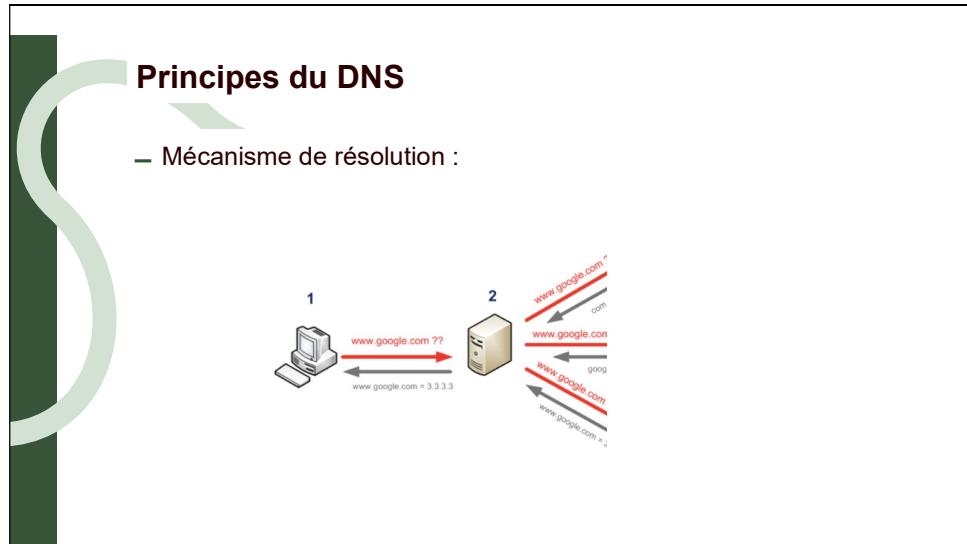


**Hiérarchie des Domaines :** Le DNS est organisé en une structure hiérarchique de domaines, allant des domaines de niveau supérieur (TLD) comme .com, .org, etc.. aux sous-domaines et aux hôtes individuels.

**Structure Hiérarchique :** Le DNS est organisé en une structure hiérarchique de domaines, similaire à l'arborescence d'un système de fichiers. Au sommet se trouvent les domaines de niveau supérieur (TLD), tels que .com, .org, .net, etc.. suivis des sous-domaines et des hôtes individuels. Cette hiérarchie facilite la gestion et la résolution des noms de domaine.

### Explication des différents niveaux de cette arborescence :

- **Root (racine) :**
  - La racine de l'arborescence DNS est le niveau le plus élevé de la hiérarchie.
  - Elle est représentée par un point (.) et contient les serveurs racine, qui sont au nombre de 13 et sont gérés par diverses organisations à travers le monde.
  - Les serveurs racine fournissent des informations sur les serveurs de noms autoritaires pour les TLD (Top-Level Domains) de premier niveau.
- **TLD (Top-Level Domain - Domaine de premier niveau) :**
  - Les TLD sont les niveaux de domaine juste en dessous de la racine.
  - Ils se trouvent à droite du point (.) dans un nom de domaine.
  - Il existe deux types de TLD :
    - **TLD génériques (gTLD)** : Ce sont des TLD qui représentent des catégories générales de noms de domaine, comme .com, .org, .net, etc.
    - **TLD de code de pays (ccTLD)** : Ce sont des TLD qui représentent des pays ou des territoires, comme .fr pour la France, .uk pour le Royaume-Uni, .us pour les États-Unis, etc.
- **SLD (Second-Level Domain - Domaine de deuxième niveau) :**
  - Les SLD sont les niveaux de domaine situés directement sous les TLD.
  - Ils sont généralement le nom choisi par l'entité enregistrant le domaine pour représenter son identité ou son activité sur Internet.
  - Par exemple, dans le domaine exemple.com, "exemple" est le SLD



Le client fait la demande à son serveur DNS d'entreprise en premier lieu, voici comment le processus de résolution DNS se déroulerait :

- **Requête au serveur DNS d'entreprise :**
- Le client DNS envoie une requête à son serveur DNS d'entreprise pour résoudre le nom de domaine "www.exemple.com".
- **Cache locale du serveur DNS d'entreprise :**
- Le serveur DNS d'entreprise vérifie d'abord sa propre cache locale pour voir s'il dispose déjà d'une entrée pour "www.exemple.com".  
S'il trouve une entrée dans sa cache et qu'elle est encore valide, il renvoie directement l'adresse IP associée à ce nom de domaine au client.
- **Requête récursive :**
- Si le serveur DNS d'entreprise n'a pas l'entrée dans sa cache locale, il effectue une requête récursive.
- Il envoie une requête au serveur DNS racine pour obtenir l'adresse IP des serveurs DNS autoritaires pour le TLD ".com".
- **Suivi des étapes de résolution :**
- Le serveur DNS d'entreprise suit ensuite les mêmes étapes que décrites précédemment pour résoudre le nom de domaine "www.exemple.com" en effectuant des requêtes auprès des serveurs DNS appropriés, y compris les serveurs DNS autoritaires pour le TLD ".com" et le domaine "exemple.com".
- **Réponse au client :**
- Une fois que le serveur DNS d'entreprise obtient l'adresse IP associée à "www.exemple.com" à partir des serveurs DNS autoritaires, il renvoie cette information au client DNS



## Définitions : les types d'enregistrements, le fichier de zones.

– Les types d'enregistrement :

- A (Address Record)
- AAAA (IPv6 Address Record)
- CNAME (Canonical Name Record)
- MX (Mail Exchange Record)
- NS (Name Server Record)
- PTR (Pointer Record)
- SOA (Start of Authority Record)
- TXT (Text Record)
- SRV (Service Record)
- CAA (Certification Authority Authorization)

### Types d'Enregistrements

- **A (Address Record) :**
  - Associe un nom de domaine à une adresse IPv4.
  - Par exemple : exemple.com IN A 192.0.2.1
- **AAAA (IPv6 Address Record) :**
  - Associe un nom de domaine à une adresse IPv6.
  - Par exemple : exemple.com IN AAAA 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- **CNAME (Canonical Name Record) :**
  - Crée un alias pour un nom de domaine (canonical name).
  - Par exemple : www IN CNAME exemple.com
- **MX (Mail Exchange Record) :**
  - Spécifie le serveur de messagerie (MTA) qui gère les e-mails pour le domaine.
  - Par exemple : exemple.com IN MX 10 mail.exemple.com
- **NS (Name Server Record) :**
  - Indique les serveurs de noms autoritaires pour le domaine.
  - Par exemple : exemple.com IN NS ns1.exemple.com
- **PTR (Pointer Record) :**
  - Utilisé pour créer des enregistrements de retour (reverse DNS) pour une adresse IP.
  - Par exemple : 1.2.3.4 IN PTR exemple.com
- **SOA (Start of Authority Record) :**
  - Indique le serveur DNS autoritaire pour la zone et d'autres paramètres de la zone.
  - Par exemple : exemple.com IN SOA ns1.exemple.com admin.exemple.com 2022042301 3600 1800 604800 86400
- **TXT (Text Record) :**
  - Permet de stocker du texte arbitraire associé à un nom de domaine.
  - Souvent utilisé pour le SPF (Sender Policy Framework) et d'autres types de données.
  - Par exemple : exemple.com IN TXT "v=spf1 mx -all"
- **SRV (Service Record) :**
  - Utilisé pour spécifier des services disponibles sur le réseau.
  - Par exemple : \_service.\_proto.name TTL class SRV priority weight port target
- **CAA (Certification Authority Authorization) :**
  - Spécifie quelles autorités de certification (CA) sont autorisées à émettre des certificats pour le domaine.
  - Par exemple : exemple.com IN CAA 0 issue "ca1.example.com"



### Définitions : les types d'enregistrements, le fichier de zones.

– Fichier de Zone DNS

```
; Exemple de fichier de zone
TTL 60400
@ IN SOA

; Définition des serveurs de noms
@ IN NS
ns1 IN NS
ns2 IN NS

; Définition des enregistrements A
ns1 IN A
ns2 IN A

; Définition des enregistrements MX
@ IN MX 10

; Définition des enregistrements A pour les hôtes
www IN A
mail IN A

; Définition d'un alias de nom
ftp IN CNAME
```

Un fichier de zone est un fichier de configuration utilisé par les serveurs DNS pour décrire les paramètres de résolution DNS pour un domaine spécifique. Il contient des informations sur les enregistrements DNS associés à ce domaine, tels que les adresses IP des hôtes, les enregistrements de messagerie (MX), les serveurs de noms (NS), les alias de noms (CNAME), etc.

Dans cet exemple :

- La première ligne définit le TTL (Time to Live) par défaut pour les enregistrements de cette zone.
- La ligne @ IN SOA définit l'enregistrement SOA (Start of Authority) pour la zone, spécifiant les serveurs de noms autoritaires, l'adresse e-mail de l'administrateur et d'autres paramètres de la zone.
- Les lignes @ IN NS définissent les serveurs de noms autoritaires pour la zone.
- Les lignes ns1 et ns2 définissent les enregistrements A pour les serveurs de noms.
- Les lignes @ IN MX définissent les enregistrements MX pour les e-mails.
- Les lignes www et mail définissent les enregistrements A pour les hôtes.
- La ligne ftp IN CNAME définit un alias de nom (CNAME) pour le sous-domaine "ftp" qui pointe vers "[www.exemple.com](http://www.exemple.com)".

A retenir sur les zones DNS :

- **Délimitation de l'espace d'adressage** : Une zone DNS définit une partie spécifique de l'espace d'adressage d'un domaine. Par exemple, le domaine "exemple.com" peut avoir plusieurs zones DNS, chacune pour un sous-domaine spécifique comme "[www.exemple.com](http://www.exemple.com)", "[blog.exemple.com](http://blog.exemple.com)", etc.
- **Serveurs DNS autoritaires** : Chaque zone DNS a un ensemble de serveurs DNS autoritaires qui ont l'autorité finale pour répondre aux requêtes DNS concernant les enregistrements pour cette zone. Ces serveurs DNS autoritaires sont configurés pour héberger les enregistrements DNS spécifiques à cette zone.
- **Enregistrements DNS** : Les enregistrements DNS contenus dans une zone DNS comprennent des enregistrements de type A (adresses IPv4), AAAA (adresses IPv6), MX (enregistrements de courrier), CNAME (alias de nom), NS (serveurs de noms), etc. Ces enregistrements définissent les différents aspects de la résolution DNS pour les hôtes et les services dans cette zone.
- **Définition dans la configuration du serveur DNS** : La configuration d'une zone DNS est généralement définie dans les fichiers de configuration du serveur DNS, tels que le fichier de zone dans le cas de serveurs DNS comme BIND, ou via une interface graphique dans le cas de serveurs DNS plus conviviaux.



- Montrer les syntaxes  
ipconfig/displaydns  
et ipconfig/flushdns

## Démonstration

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

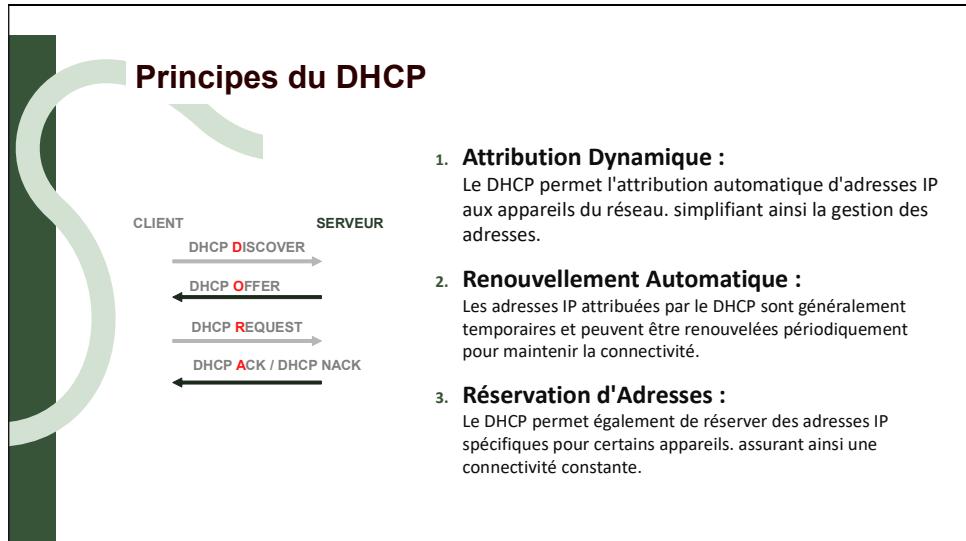
---

---

---

---

---

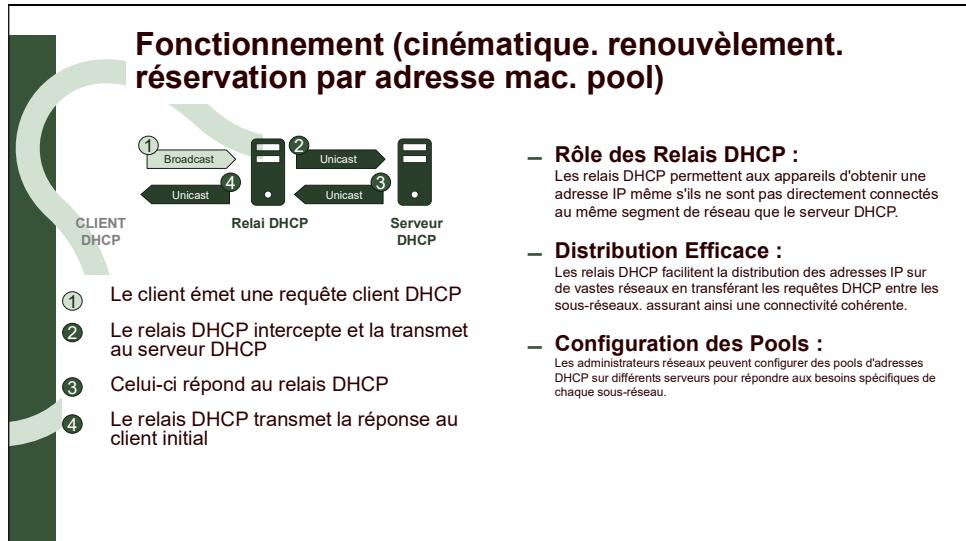


**Principes du DHCP** Le protocole DHCP (Dynamic Host Configuration Protocol) est essentiel pour la gestion dynamique des adresses IP dans un réseau. Voici quelques principes fondamentaux à retenir :

**1. Attribution Dynamique :** Le DHCP permet l'attribution automatique d'adresses IP aux appareils connectés au réseau. Au lieu de configurer manuellement chaque appareil avec une adresse IP statique. le DHCP simplifie ce processus en fournissant automatiquement une adresse IP disponible.

**2. Renouvellement Automatique :** Les adresses IP attribuées par le DHCP sont généralement temporaires. Pour maintenir la connectivité des appareils. le DHCP offre la possibilité de renouveler automatiquement ces adresses à des intervalles définis. Cela garantit que les appareils conservent une adresse IP valide et peuvent continuer à communiquer sur le réseau.

**3. Réservation d'Adresses :** En plus de l'attribution dynamique. le DHCP permet également de réservé des adresses IP spécifiques pour certains appareils. Cette fonctionnalité est utile pour garantir qu'un appareil particulier reçoive toujours la même adresse IP lors de sa connexion au réseau. ce qui peut être nécessaire pour des raisons de configuration ou de sécurité.



**Fonctionnement des Relais DHCP et Configuration des Pools** Dans les architectures réseau d'entreprise, les relais DHCP jouent un rôle crucial dans la distribution efficace des adresses IP. Voici quelques points à retenir :

**1. Rôle des Relais DHCP :** Les relais DHCP permettent aux appareils de recevoir une adresse IP même s'ils ne sont pas directement connectés au même segment de réseau que le serveur DHCP. Ils agissent comme des intermédiaires en transférant les demandes DHCP entre les sous-réseaux.

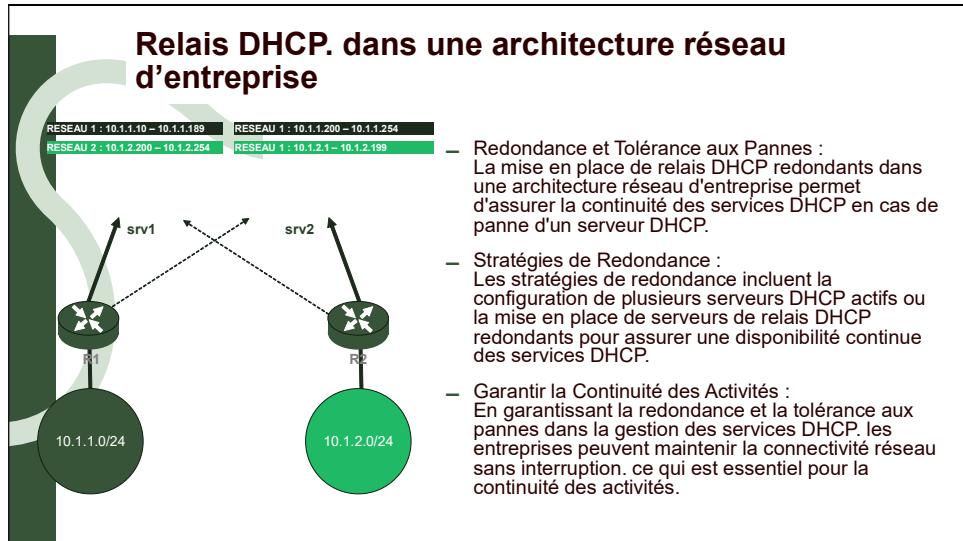
**2. Distribution Efficace :** Grâce aux relais DHCP, la distribution des adresses IP peut être gérée de manière efficace sur de vastes réseaux. Les requêtes DHCP émises par les appareils sur différents sous-réseaux sont relayées vers les serveurs DHCP appropriés, assurant ainsi une connectivité cohérente pour tous les appareils du réseau.

**3. Configuration des Pools :** Les administrateurs réseaux peuvent configurer des pools d'adresses DHCP sur différents serveurs pour répondre aux besoins spécifiques de chaque sous-réseau. Cette configuration permet de garantir une distribution équilibrée des adresses IP et une gestion efficace des ressources réseau.



## Démonstration

- Montrer la capture wireshark du reboot d'un PC windows dans la salle

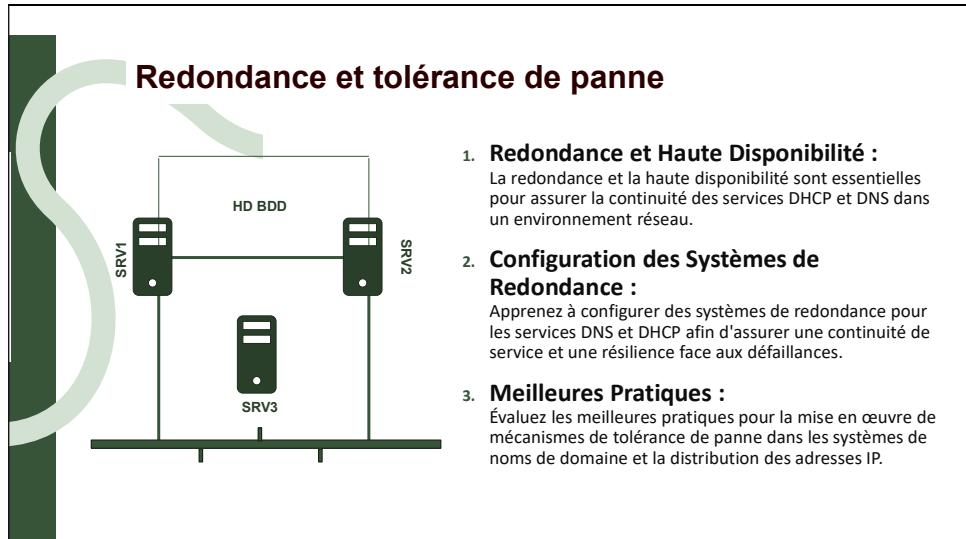


**Stratégies de Redondance pour les Relais DHCP** Dans une architecture réseau d'entreprise, la redondance et la tolérance aux pannes sont des éléments essentiels pour assurer la continuité des activités. Voici quelques points à considérer :

**1. Redondance et Tolérance aux Pannes** : La mise en place de relais DHCP redondants permet de garantir la continuité des services DHCP en cas de panne d'un serveur DHCP. Cette redondance assure une disponibilité continue des services réseau, même en cas de défaillance d'un composant.

**2. Stratégies de Redondance** : Les entreprises peuvent élaborer différentes stratégies de redondance pour assurer la disponibilité des services DHCP. Cela peut inclure la configuration de plusieurs serveurs DHCP actifs, chacun prenant en charge une partie des clients, ou la mise en place de serveurs de relais DHCP redondants pour relayer les requêtes DHCP vers plusieurs serveurs DHCP.

**3. Continuité des Activités** : En garantissant la redondance et la tolérance aux pannes dans la gestion des services DHCP, les entreprises peuvent maintenir la connectivité réseau sans interruption, ce qui est essentiel pour assurer la continuité des activités. La mise en place de stratégies de redondance efficaces contribue à minimiser les temps d'arrêt et à assurer une disponibilité continue des services réseau.



**Redondance et Tolérance de Panne dans les Services DHCP et DNS** La redondance et la tolérance de panne sont des aspects critiques de la gestion des services DHCP et DNS dans un environnement réseau. Voici les points clés à retenir :

- Importance de la Redondance et de la Haute Disponibilité :** La redondance et la haute disponibilité garantissent que les services DHCP et DNS restent disponibles même en cas de défaillance matérielle ou logicielle. Cela permet d'assurer une continuité de service et de réduire les temps d'arrêt.
- Configuration des Systèmes de Redondance :** Apprenez à configurer des systèmes de redondance pour les services DHCP et DNS en mettant en place des architectures distribuées avec des serveurs de secours ou des clusters. Cette configuration permet de garantir une disponibilité continue des services même en cas de panne d'un composant.
- Meilleures Pratiques pour la Tolérance de Panne :** Évaluez les meilleures pratiques pour la mise en œuvre de mécanismes de tolérance de panne dans les systèmes de noms de domaine et la distribution des adresses IP. Cela peut inclure l'utilisation de protocoles de routage redondants, la configuration de serveurs de secours et la mise en place de stratégies de basculement automatique pour assurer une continuité de service optimale.



Paramétrage de serveur  
DNS et DHCP sur un  
émulateur de réseau

## Démonstration



Interroger des serveurs  
DNS : Nslookup, dig

## Démonstration

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

- Ce qu'il faut retenir



- DHCP Simplifie la Configuration Réseau
- DNS : La Cartographie d'Internet
- Gestion Dynamique et Flexible des Adresses
- Résolution de Noms Rapide et Fiable
- Sécurité et Stabilité des Services Réseau

**DHCP Simplifie la Configuration Réseau :**

"Le DHCP (Dynamic Host Configuration Protocol) automatise l'attribution des adresses IP, simplifiant la configuration réseau pour les appareils et garantissant une gestion efficace de l'espace d'adressage."

**DNS : La Cartographie d'Internet :**

"Le DNS (Domain Name System) transforme les noms de domaine faciles à retenir en adresses IP numériques, agissant comme un système de cartographie essentiel qui guide le trafic Internet."

**Gestion Dynamique et Flexible des Adresses :**

"Grâce au DHCP, les réseaux peuvent gérer de manière dynamique et flexible les adresses IP, facilitant l'ajout ou la modification d'appareils sans intervention manuelle."

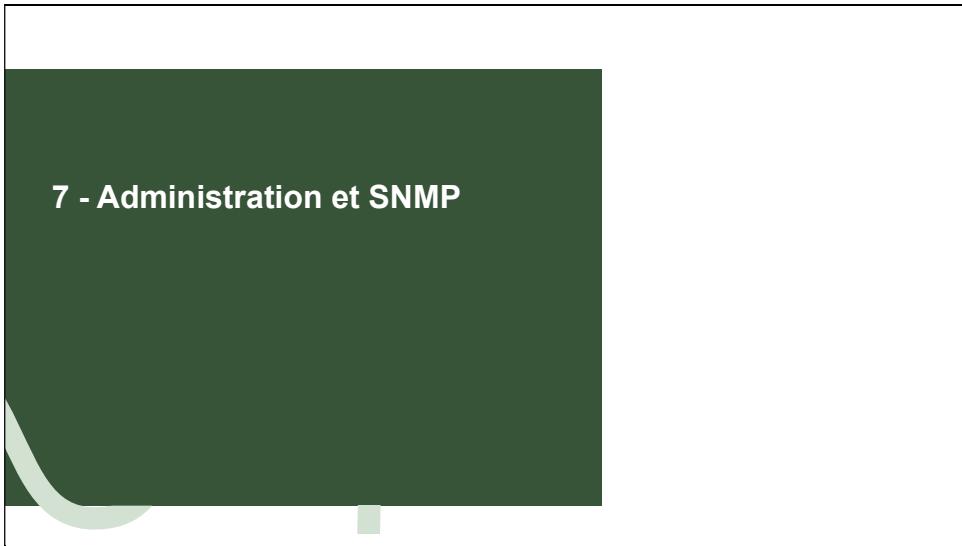
**Résolution de Noms Rapide et Fiable :**

"Le DNS permet une résolution de noms rapide et fiable, essentielle pour l'accès aux services Internet et la navigation Web, tout en soutenant des fonctions avancées comme le load balancing."

**Sécurité et Stabilité des Services Réseau :**

"La configuration et la maintenance appropriées des services DHCP et DNS sont cruciales pour la sécurité et la stabilité des réseaux, nécessitant une attention constante pour prévenir les abus et les attaques."

## Chapitre 7 – Administration et SNMP



- Objectifs du chapitre



### Les objectifs du chapitre

- Comprendre les fondamentaux du Simple Network Management Protocol (SNMP) et son rôle dans la supervision et la gestion des périphériques réseau.
- Explorer les Management Information Bases (MIBs) et différencier entre les MIBs publics et privés, en comprenant leur structure et leur utilisation dans la collecte d'informations sur les périphériques réseau.
- Apprendre à configurer les communautés SNMP, y compris la création de communautés de lecture et d'écriture, pour sécuriser l'accès aux informations des périphériques réseau.
- Examiner les différents types de messages SNMP par version (SNMPv1, SNMPv2c, SNMPv3) et comprendre leurs fonctionnalités et leurs limitations.
- Acquérir les compétences nécessaires pour configurer un agent SNMP sur un périphérique réseau, permettant ainsi la surveillance et la gestion à distance via SNMP.



- **Gestion des Appareils Réseau :**  
"Avez-vous déjà eu à vérifier l'état ou la performance d'un appareil réseau. comme un routeur ou un switch ? Comment avez-vous procédé ?"
- **Compréhension des Performances Réseau :**  
"Pouvez-vous décrire une situation où la performance de votre réseau a soudainement changé ? Quelles étaient vos premières étapes pour identifier le problème ?"
- **Sécurité et Surveillance Réseau :**  
"Quelles méthodes utilisez-vous pour surveiller la sécurité de votre réseau ? Avez-vous déjà rencontré des outils ou des protocoles spécifiques pour cela ?"
- **Expérience avec les Données de Configuration :**  
"Avez-vous déjà eu besoin d'accéder aux configurations ou aux données de gestion d'un dispositif réseau pour un dépannage ou une mise à jour ? Quel a été le processus ?"
- **Utilisation des Outils de Gestion Réseau :**  
"Quels outils ou logiciels avez-vous utilisés pour gérer ou surveiller les réseaux ? Quelles fonctionnalités trouvez-vous les plus utiles dans ces outils ?"

**Gestion des Appareils Réseau :**

"Avez-vous déjà eu à vérifier l'état ou la performance d'un appareil réseau. comme un routeur ou un switch ? Comment avez-vous procédé ?"

**Compréhension des Performances Réseau :**

"Pouvez-vous décrire une situation où la performance de votre réseau a soudainement changé ? Quelles étaient vos premières étapes pour identifier le problème ?"

**Sécurité et Surveillance Réseau :**

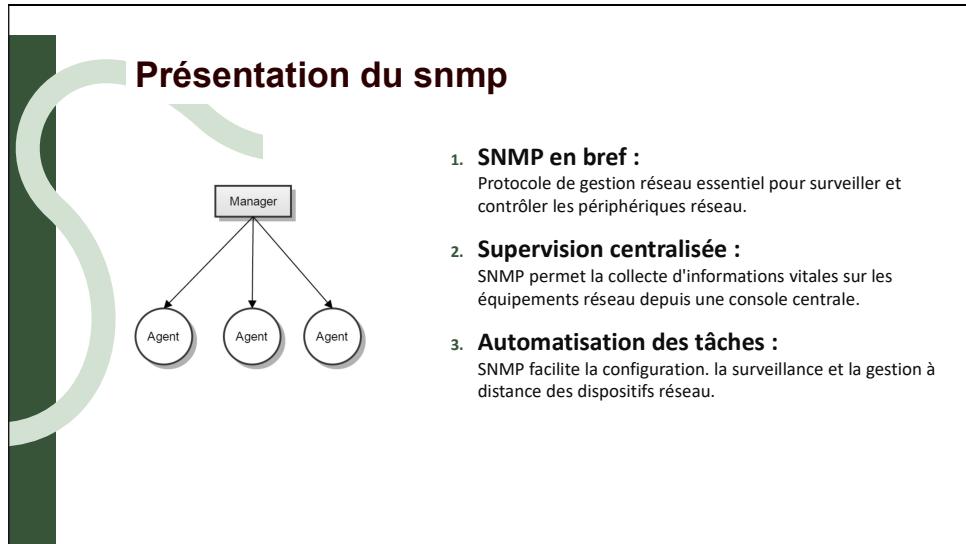
"Quelles méthodes utilisez-vous pour surveiller la sécurité de votre réseau ? Avez-vous déjà rencontré des outils ou des protocoles spécifiques pour cela ?"

**Expérience avec les Données de Configuration :**

"Avez-vous déjà eu besoin d'accéder aux configurations ou aux données de gestion d'un dispositif réseau pour un dépannage ou une mise à jour ? Quel a été le processus ?"

**Utilisation des Outils de Gestion Réseau :**

"Quels outils ou logiciels avez-vous utilisés pour gérer ou surveiller les réseaux ? Quelles fonctionnalités trouvez-vous les plus utiles dans ces outils ?"



Le SNMP, ou Simple Network Management Protocol, est un protocole standardisé largement utilisé dans les réseaux informatiques pour surveiller et gérer les périphériques réseau tels que les routeurs, les commutateurs et les serveurs. Son rôle principal est de permettre la supervision centralisée des équipements réseau en collectant des informations sur leur état, leurs performances et leur utilisation des ressources.

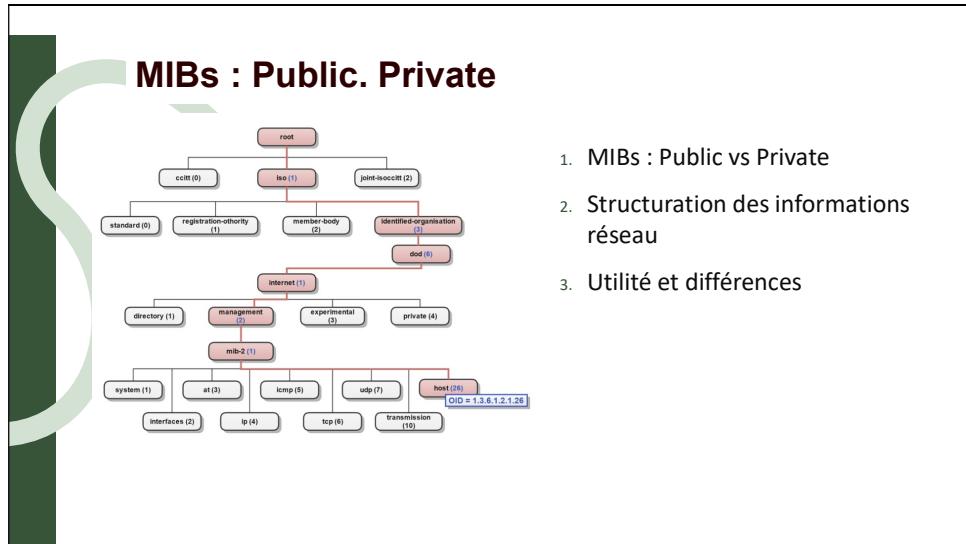
Le fonctionnement du SNMP repose sur un modèle client-serveur, où les périphériques réseau agissent en tant qu'agents SNMP et transmettent des données de gestion à un système de gestion réseau centralisé, appelé le NMS (Network Management System). Le NMS recueille ces données à l'aide de requêtes SNMP et prend des décisions en fonction des informations reçues.

Le SNMP utilise des structures de données hiérarchiques appelées MIB (Management Information Base) pour organiser les informations collectées. Les MIB se présentent sous deux formes : publiques et privées. Les MIB publiques sont standardisées et définies par des organisations telles que l'IANA (Internet Assigned Numbers Authority), tandis que les MIB privées sont spécifiques à chaque fabricant.

La configuration du SNMP implique généralement la définition de communautés, qui sont essentiellement des chaînes de caractères utilisées pour authentifier et autoriser les communications SNMP entre les agents et le NMS. Il est important de configurer soigneusement les communautés SNMP pour garantir la sécurité du réseau.

Le SNMP peut fonctionner selon différentes versions, telles que SNMPv1, SNMPv2 et SNMPv3. Chaque version apporte des améliorations en termes de sécurité, de fonctionnalités et de performances. Les messages SNMP échangés entre les agents et le NMS suivent un certain format défini par la version SNMP utilisée.

**En résumé.** le SNMP est un outil puissant pour la gestion des réseaux informatiques, offrant une surveillance centralisée, des fonctionnalités d'automatisation et une gestion efficace des périphériques réseau. En comprenant ses principes de base et ses fonctionnalités, les administrateurs réseau peuvent optimiser la performance, la disponibilité et la sécurité de leurs réseaux.



Les MIBs, ou Management Information Bases, sont des bases de données qui stockent des informations sur les périphériques réseau et les systèmes informatiques. Elles sont utilisées par le SNMP (Simple Network Management Protocol) pour organiser et présenter ces informations de manière hiérarchique.

Les MIBs publiques sont des structures de données standardisées et ouvertes qui sont définies et maintenues par des organismes de normalisation tels que l'IANA (Internet Assigned Numbers Authority) ou l'ITU (International Telecommunication Union). Elles contiennent des informations générales sur les équipements réseau, telles que les interfaces, les adresses IP, les performances, etc. Les MIBs publiques sont accessibles à tous et sont largement utilisées dans les outils de gestion réseau.

En revanche, les MIBs privées sont spécifiques à un fabricant ou à un fournisseur de matériel réseau particulier. Elles contiennent des informations propres à leurs produits et sont souvent utilisées pour surveiller et gérer les fonctionnalités spécifiques des équipements d'un même fabricant. Les MIBs privées ne sont pas standardisées et ne sont généralement pas accessibles publiquement.

Les MIBs, qu'elles soient publiques ou privées, jouent un rôle crucial dans la gestion des réseaux informatiques en fournissant une structure organisée pour collecter, stocker et présenter les données sur les périphériques réseau. En comprenant la différence entre les MIBs publiques et privées, les administrateurs réseau peuvent mieux utiliser les outils de gestion réseau et optimiser la performance et la disponibilité de leurs infrastructures.

**Paramétrage des communautés**

1. Paramétrage des communautés SNMP
2. Communautés "public" et "private"
3. Création de communautés personnalisées

Agent Windows

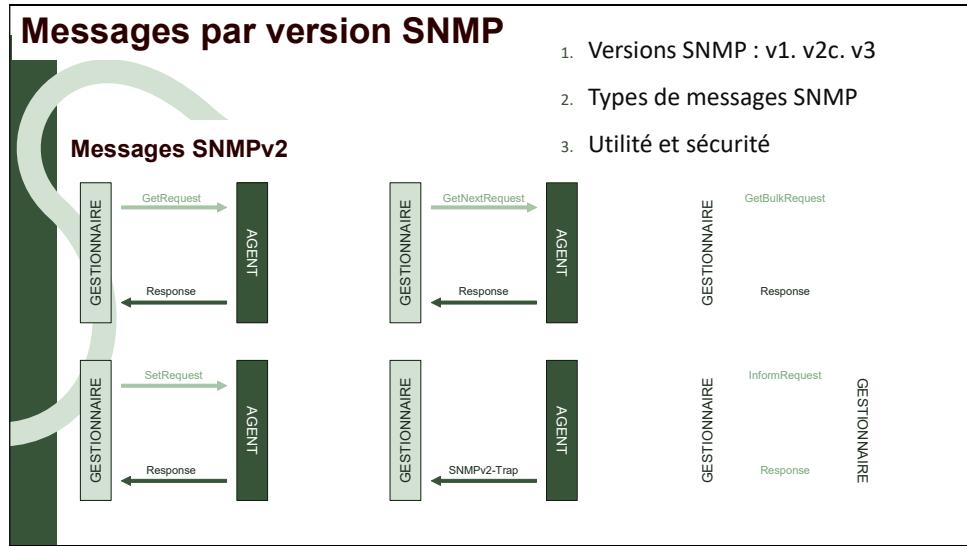
Les communautés SNMP sont des chaînes de caractères utilisées pour authentifier et contrôler l'accès aux informations SNMP sur les périphériques réseau. Elles sont essentielles pour la sécurité et la gestion des équipements réseau.

La communauté "public" est une communauté SNMP par défaut qui offre un accès en lecture seule aux informations SNMP. Elle est largement utilisée pour les opérations de surveillance et de collecte de données, mais ne permet pas de modifier la configuration des périphériques.

En revanche, la communauté "private" est une communauté SNMP plus sécurisée qui offre un accès complet en lecture et en écriture aux informations SNMP. Elle est utilisée pour les opérations de configuration et de gestion des périphériques réseau et doit être protégée par des mesures de sécurité appropriées.

Outre les communautés par défaut, il est également possible de créer des communautés SNMP personnalisées avec des autorisations spécifiques. Ces communautés sur mesure permettent de mieux contrôler l'accès aux informations SNMP en fonction des besoins spécifiques de l'organisation.

En configurant correctement les communautés SNMP, les administrateurs réseau peuvent sécuriser efficacement l'accès aux informations SNMP et garantir que seuls les utilisateurs autorisés peuvent surveiller et gérer les périphériques réseau.

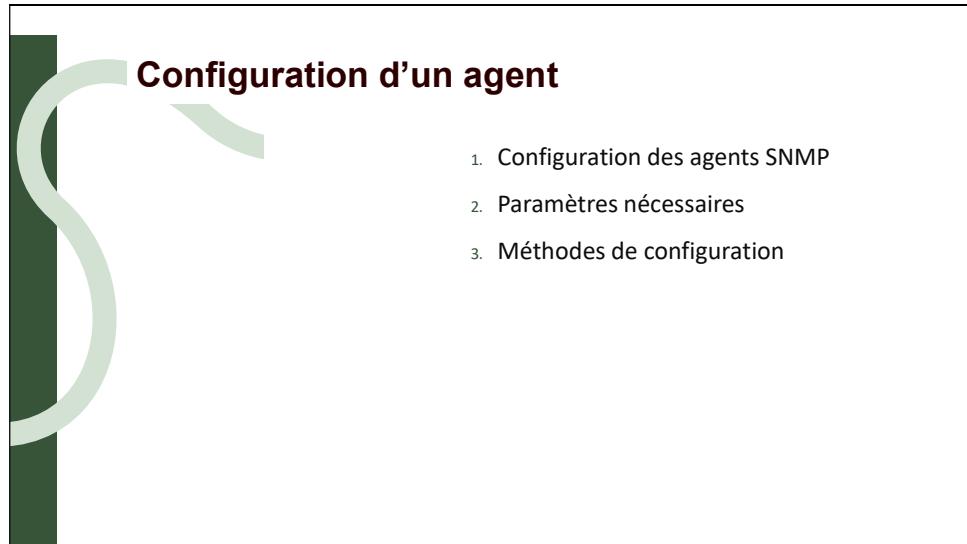


Le protocole SNMP (Simple Network Management Protocol) est disponible en différentes versions, notamment v1, v2c et v3, chacune offrant des fonctionnalités et des niveaux de sécurité différents.

- **SNMPv1 :** La première version de SNMP est la plus ancienne et la moins sécurisée. Elle utilise une simple authentification basée sur des chaînes de caractères communément appelées "communautés". Les messages SNMPv1 sont principalement utilisés pour la surveillance et la collecte de données.
- **SNMPv2c :** Cette version est une amélioration de SNMPv1, offrant de nouvelles fonctionnalités telles que la récupération de tables MIB et la notification des événements. Cependant, elle conserve la même méthode d'authentification basée sur les communautés et présente donc des problèmes de sécurité similaires.
- **SNMPv3 :** La version la plus récente et la plus sécurisée de SNMP. SNMPv3 introduit des fonctionnalités avancées telles que l'authentification et le chiffrement des messages, garantissant une meilleure confidentialité et intégrité des données échangées entre les agents SNMP et les consoles de gestion. Cette version est recommandée pour les environnements où la sécurité est une priorité.

Les types de messages SNMP comprennent les requêtes (get, get-next, get-bulk), les réponses, les notifications et les traps. Chaque type de message a un rôle spécifique dans la gestion et le contrôle des périphériques réseau.

En compréhension les différences entre les versions de SNMP et les types de messages qu'elles prennent en charge, les administrateurs réseau peuvent choisir la version la plus adaptée à leurs besoins en matière de gestion et de sécurité des réseaux.



## Configuration d'un agent

1. Configuration des agents SNMP
2. Paramètres nécessaires
3. Méthodes de configuration

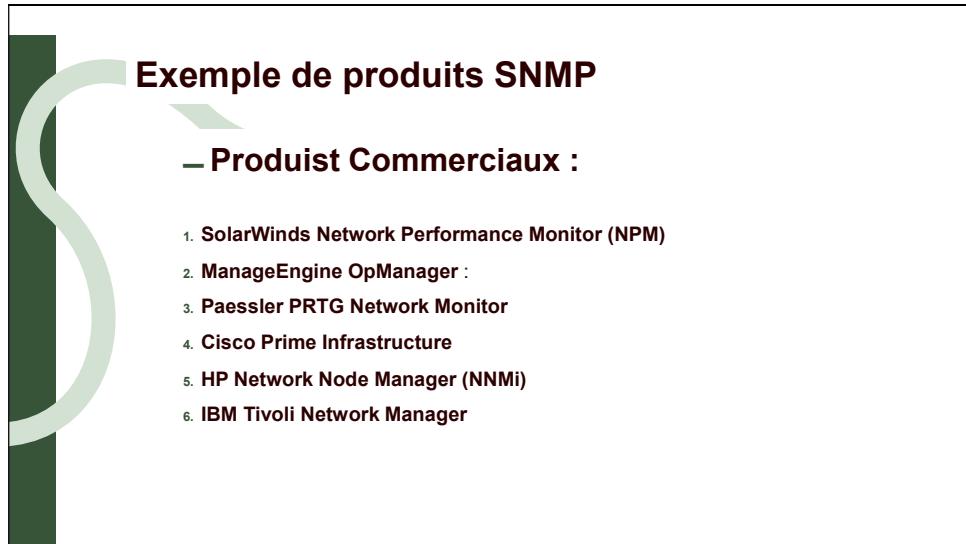
La configuration des agents SNMP sur les dispositifs réseau est essentielle pour permettre la surveillance et la gestion à distance de ces dispositifs. Voici les principales étapes pour configurer un agent SNMP :

- **Accès aux paramètres** : Tout d'abord, accédez à l'interface de configuration de votre dispositif réseau. Selon le dispositif, cela peut se faire via une interface en ligne de commande (CLI) ou une interface graphique utilisateur (GUI).
- **Activation du service SNMP** : Localisez les paramètres de gestion ou de supervision et activez le service SNMP. Vous devrez peut-être spécifier la version SNMP que vous souhaitez utiliser (v1, v2c ou v3).
- **Configuration des communautés** : Définissez les communautés SNMP, notamment les communautés "public" et "private", qui seront utilisées pour l'authentification des requêtes SNMP. Vous pouvez également configurer des communautés personnalisées pour un accès plus restreint et sécurisé.
- **Attribution des autorisations** : Configurez les autorisations d'accès pour chaque communauté SNMP. Vous pouvez spécifier si une communauté est autorisée à effectuer des opérations de lecture seule (lecture) ou à modifier les paramètres (écriture) sur le dispositif.

**Définition des MIBs** : Sélectionnez les MIBs (Management Information Base) que vous souhaitez rendre accessibles via l'agent SNMP. Les MIBs fournissent des informations sur les paramètres et les performances du dispositif.

• **Sauvegarde de la configuration** : Une fois que vous avez terminé la configuration de l'agent SNMP, assurez-vous de sauvegarder les modifications pour qu'elles persistent après un redémarrage du dispositif.

En suivant ces étapes, vous serez en mesure de configurer avec succès des agents SNMP sur vos dispositifs réseau, ce qui permettra une surveillance et une gestion efficaces de votre infrastructure.



**Produit commerciaux :**

- **SolarWinds Network Performance Monitor (NPM)** : SolarWinds NPM est un logiciel de surveillance réseau qui prend en charge SNMP pour la surveillance des périphériques réseau, y compris la surveillance du STP pour la détection des problèmes de boucle réseau.
- **ManageEngine OpManager** : OpManager est une plate-forme de gestion réseau qui prend en charge SNMP pour la surveillance et la gestion des périphériques réseau, y compris la prise en charge du STP pour la gestion des réseaux Ethernet.
- **Paessler PRTG Network Monitor** : PRTG est un outil de surveillance réseau complet qui prend en charge SNMP pour la surveillance des périphériques réseau, avec une prise en charge du STP pour la surveillance des topologies de réseau et la détection des boucles.
- **Cisco Prime Infrastructure** : Cisco Prime Infrastructure est une plate-forme de gestion de réseau conçue pour les environnements Cisco. Elle prend en charge SNMP pour la surveillance et la gestion des périphériques réseau Cisco, y compris la surveillance du STP pour la gestion des réseaux Ethernet.
- **HP Network Node Manager (NNMi)** : NNMi est une solution de gestion de réseau qui prend en charge SNMP pour la surveillance et la gestion des périphériques réseau, y compris la prise en charge du STP pour la surveillance des réseaux Ethernet.
- **IBM Tivoli Network Manager** : Tivoli Network Manager est une solution de gestion de réseau d'entreprise qui prend en charge SNMP pour la surveillance et la gestion des périphériques réseau, y compris la surveillance du STP pour la gestion des réseaux Ethernet.

**Produit OpenSource :**

- **Zabbix** : Zabbix est une plate-forme de surveillance réseau open source qui prend en charge SNMP pour la surveillance des périphériques réseau. Il offre une prise en charge étendue des protocoles de surveillance et peut être étendu pour prendre en charge STP.
- **Nagios Core** : Nagios Core est un système de surveillance et de gestion de réseau open source. Bien qu'il nécessite des plugins pour la surveillance SNMP et STP, il offre une grande flexibilité et une large communauté de support.
- **OpenNMS** : OpenNMS est une plate-forme de gestion de réseau open source qui prend en charge SNMP pour la surveillance et la gestion des périphériques réseau. Il offre également une prise en charge avancée des protocoles de surveillance et de gestion.
- **LibreNMS** : LibreNMS est un fork de Observium Community Edition et est une solution de surveillance réseau open source basée sur PHP/MySQL/SNMP. Il peut surveiller une large gamme de dispositifs réseau et prendre en charge le protocole STP.
- **Cacti** : Cacti est un logiciel de surveillance réseau open source basé sur RRDTool et PHP. Bien qu'il nécessite des plugins pour la surveillance SNMP et STP, il offre une interface web conviviale pour la visualisation des données de surveillance.
- **NetXMS** : NetXMS est une plate-forme de gestion de réseau open source qui prend en charge SNMP pour la surveillance et la gestion des périphériques réseau. Il offre une large gamme de fonctionnalités de surveillance et de gestion, y compris la surveillance du STP.



Utilisation d'un browser de MIB sur des machines windows

### Démonstration

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

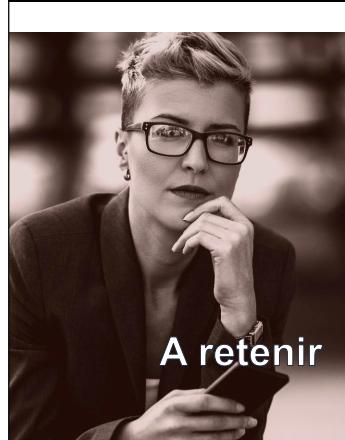
---



## Observation de trace SNMP avec « wireshark »

## Démonstration

- Ce qu'il faut retenir



- SNMP : Pilier de la Gestion Réseau
- MIBs : La Structure des Informations Réseau
- Flexibilité et Évolutivité de SNMP
- Surveillance en Temps Réel et Alertes
- Sécurité et Authentification avec SNMPv3

**SNMP : Pilier de la Gestion Réseau :**

"Simple Network Management Protocol (SNMP) est un outil essentiel pour l'administration réseau, permettant la surveillance, la gestion et la configuration à distance des dispositifs réseau."

**MIBs : La Structure des Informations Réseau :**

"Les Management Information Bases (MIBs) fournissent une structure organisée pour stocker les données de gestion des équipements réseau, facilitant l'accès et la manipulation d'informations spécifiques via SNMP."

**Flexibilité et Évolutivité de SNMP :**

"Grâce à sa conception flexible et ses différentes versions, SNMP s'adapte à divers environnements et exigences de sécurité, rendant la gestion réseau évolutive et sécurisée."

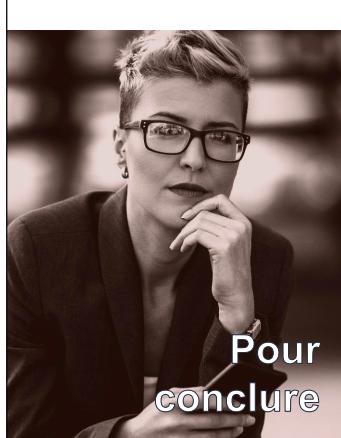
**Surveillance en Temps Réel et Alertes :**

"SNMP permet une surveillance en temps réel du statut et de la performance des équipements réseau, avec la capacité de générer des alertes automatiques en cas d'anomalies ou de problèmes."

**Sécurité et Authentification avec SNMPv3 :**

"SNMP version 3 (SNMPv3) améliore significativement la sécurité de la gestion réseau en introduisant des fonctionnalités d'authentification et de chiffrement, protégeant les communications de gestion contre les accès non autorisés."

## Ce qu'il faut retenir de la formation



1. "Le SNMP est votre allié pour surveiller et gérer efficacement vos réseaux informatiques à distance."
2. "Les MIBs fournissent une structure organisée pour collecter et interpréter les données de gestion réseau."
3. "Les communautés SNMP 'public' et 'private' sont les clés d'accès à vos dispositifs. veillez à leur sécurité."
4. "La redondance et la tolérance de panne sont cruciales pour assurer la continuité des activités dans votre infrastructure réseau."
5. "TCP et UDP sont les piliers du transfert de données. comprenez leurs différences pour choisir le bon protocole."
6. "Le DHCP automatise la configuration des adresses IP. simplifiant ainsi la gestion des périphériques sur votre réseau."
7. "Le DNS traduit les noms de domaine en adresses IP. facilitant ainsi la navigation sur Internet."
8. "Les topologies de bornes professionnelles offrent des configurations flexibles pour une connectivité Wi-Fi optimale."
9. "Le VLAN segmente efficacement le trafic réseau. améliorant la sécurité et les performances."
10. "L'IOS des switchs Cisco offre une multitude de fonctionnalités pour configurer et gérer vos réseaux avec précision."

Alors que nous arrivons au terme de notre formation sur les pratiques des réseaux. prenons un moment pour récapituler le chemin parcouru. les connaissances acquises et envisager les prochaines étapes pour chacun d'entre vous.

### Cheminement Parcouru :

Nous avons débuté notre voyage avec une exploration des fondamentaux des réseaux. comprendre pourquoi nous les utilisons et comment ils ont évolué pour devenir l'épine dorsale de notre monde connecté. Nous avons ensuite plongé dans le monde de l'Ethernet. apprenant comment les données sont transférées à travers les câbles et les dispositifs pour atteindre leur destination. L'étude de la commutation Ethernet nous a permis de comprendre l'importance de la gestion du trafic dans les réseaux locaux. Le passage au WiFi nous a ouvert les portes de la connectivité sans fil. avec ses défis et ses solutions. Nous avons abordé les protocoles TCP/IP. essentiels pour le routage et la transmission des données sur Internet. Ensuite. l'importance cruciale de DHCP et DNS dans la gestion des adresses et la résolution des noms a été soulignée. Finalement. nous avons exploré le SNMP. outil clé pour l'administration et la surveillance des réseaux.

**Messages Forts à Retenir :**

La connectivité réseau facilite notre quotidien et notre travail.

La sécurité et la fiabilité sont au cœur de la gestion réseau efficace.

Les technologies de réseau évoluent pour répondre aux besoins croissants en bande passante et en performances.

L'administration réseau requiert une surveillance continue et une adaptation aux nouvelles menaces et technologies.

Chaque professionnel a le pouvoir et la responsabilité d'utiliser les technologies de manière éthique et durable.

**Mise en Œuvre Post-Formation :**

Suite à cette formation, chaque stagiaire est désormais équipé pour :

Diagnostiquer et résoudre des problèmes de réseau avec une compréhension approfondie des principes sous-jacents.

Appliquer des mesures de sécurité élémentaire pour protéger les infrastructures réseau.

Optimiser les performances du réseau en utilisant les technologies et protocoles appropriés.

Promouvoir l'utilisation responsable des ressources informatiques, en gardant à l'esprit les considérations environnementales et sociétales.

Continuer à apprendre et à s'adapter aux évolutions technologiques, restant ainsi à l'avant-garde du domaine des réseaux.

En gardant ces principes en tête, chacun peut non seulement contribuer à l'efficacité et à la sécurité de son environnement de travail, mais également œuvrer pour un avenir numérique plus inclusif et durable. La fin de cette formation n'est que le début d'un voyage continu d'apprentissage et d'innovation dans le vaste domaine des réseaux.

**Merci pour  
votre  
attention**

