



Concevoir un Réseau Local Performant et Sécurisé

Cette présentation explore les étapes clés pour la conception et la mise en œuvre d'un réseau local (LAN) efficace, sécurisé et flexible, en se basant sur des pratiques techniques solides.




Défis des Méthodes Classiques

Les approches traditionnelles de réseau souffrent de limitations comme l'absence de partage de ressources, la collaboration manuelle, et les coûts de maintenance élevés.




Sélection des Périphériques et Topologie

Le choix judicieux des composants (PC, routeurs, switches, modems) est crucial pour l'interconnexion et la centralisation des données.



Subnetting, VLAN et Configurations IP

L'implémentation de subnets, VLANs et IPs statiques assure une gestion optimisée du trafic et une sécurité accrue.



Implémentation des Règles ACL

Les listes de contrôle d'accès (ACL) sont essentielles pour définir des privilèges et des restrictions, renforçant la sécurité du réseau.


Les Défis des Méthodes Classiques

- Absence de partage de fichiers ou d'imprimantes.
- Échange de données manuel (USB, CD, etc.).
- Aucun travail collaboratif en temps réel.
- Maintenance et mise à jour poste par poste.
- Coût élevé dû à la duplication des équipements.




L'approche classique des réseaux engendre des frictions opérationnelles significatives, limitant la productivité et la sécurité.

Choix des Périphériques et Topologie




Postes de Travail (PC)

Gèrent les processus utilisateurs. Le cœur de l'interaction quotidienne.



Switchs

Assurent l'interconnexion entre les différentes parties du réseau.



Imprimante

Son rôle pour l'impression est bien connu.



Routeur

Agit comme le "cerveau" du réseau, responsable des privilèges utilisateurs et machines.



Modem ADSL

Fournit la connexion à Internet.



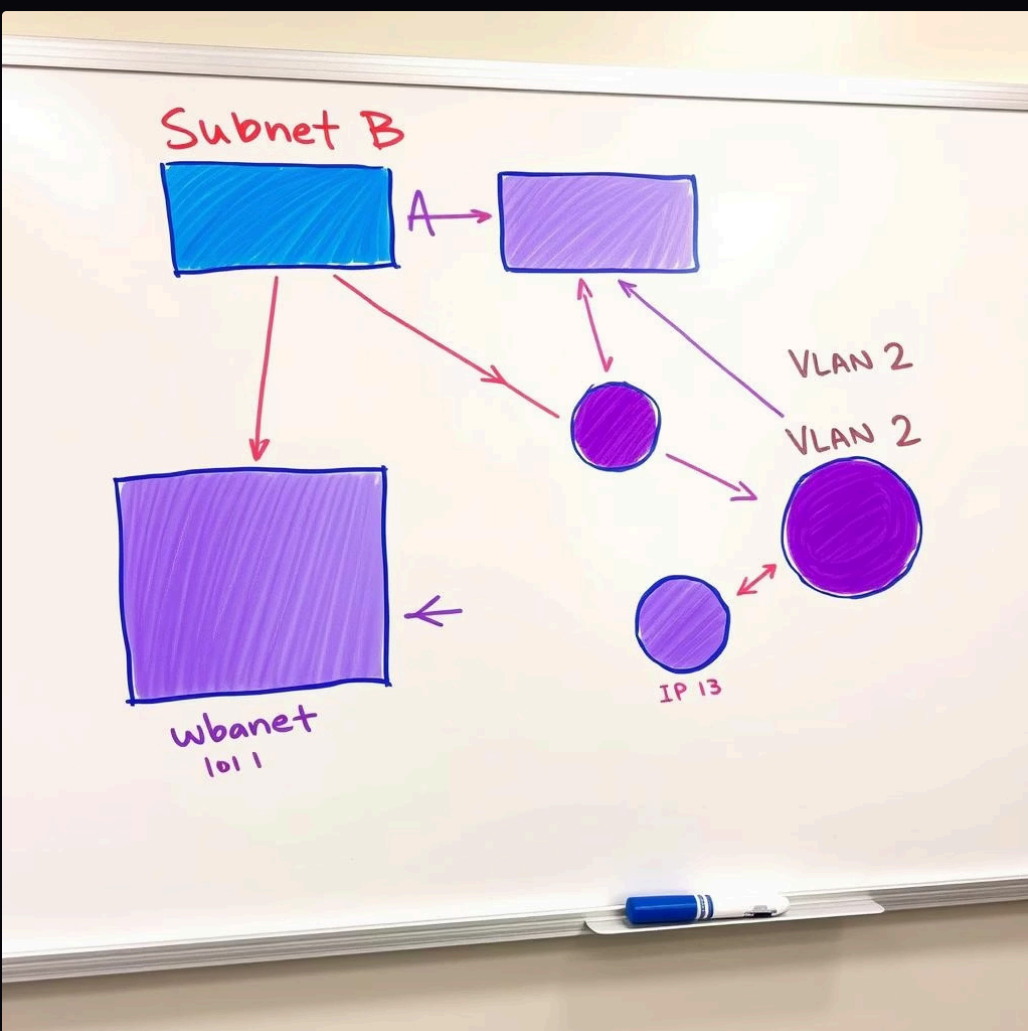
Serveur Centralisé

Point de sauvegarde et d'échange de données.

Étapes Clés : Subnetting, VLAN et Configuration IP

Pour optimiser le réseau, nous avons implémenté des configurations avancées garantissant efficacité et sécurité.

- **Subnetting** : Garantit l'absence de perte de plage réseau, accélère la séparation des LAN, réduit la congestion et améliore la sécurité.
- **IP Statique** : Attribuée aux dispositifs importants (serveur, PC admin, imprimante) pour un accès permanent et connu.
- **Réseaux Principaux** :
 - **192.168.10.0/28** : Masque 255.255.255.240. Choisi pour accommoder le nombre maximal de PC par cluster.
 - **200.100.100.0/30** : Masque 255.255.255.252. Relie le routeur au modem DSL et au cloud pour l'accès Internet.



- **Sub-interfaces (Router-on-a-Stick)** : Permettent d'ajuster la passerelle virtuelle et d'associer chaque VLAN à sa passerelle appropriée. Elles garantissent la communication inter-VLAN au niveau de la couche 3.
- **Configuration des Ports** :
 - **Mode Trunk** : Associe l'interface du switch à celle du routeur, créant un "tunnel" pour le trafic inter-VLAN.
 - **Mode Accès** : Permet à l'interface du switch de recevoir les paquets des VLAN appropriés.
- **Vérification** : Utilisez "show vlan brief" sur le switch et "show ip interface brief" sur le routeur pour vérifier les configurations.
- **Configuration des Dispositifs** : Statique ou DHCP pour assurer la distribution des IPs, passerelles et masques de sous-réseau.

Règles ACL pour la Sécurité et les Droits d'Accès

Les Listes de Contrôle d'Accès (ACL) sont fondamentales pour implémenter une sécurité granulaire et des privilèges sur le routeur. Elles permettent de bloquer ou d'autoriser le trafic entre différents segments du réseau.

```
ip access-list extended BLOCK_V20_TO_V10
permit icmp 192.168.10.16 0.0.0.15 192.168.10.0 0.0.0.15 echo-reply
deny ip 192.168.10.16 0.0.0.15 192.168.10.0 0.0.0.15
permit ip any any
```

L'ACL ci-dessus sur le VLAN 10 permet les réponses ICMP (echo-reply) provenant du VLAN 20, tout en bloquant tout autre trafic IP initié par le VLAN 20 vers le VLAN 10. Les paquets ICMP "echo-reply" sont spécifiquement autorisés pour permettre la fonctionnalité de ping bidirectionnel, même si les communications générales sont bloquées.

```
interface GigabitEthernet0/0.20
ip access-group BLOCK_V20_TO_V10 in
```

Cette ACL est ensuite appliquée à la sous-interface associée au VLAN 20 en direction "in", ce qui signifie qu'elle filtre le trafic entrant sur cette interface.

Les ACLs simples peuvent interdire définitivement le contact entre les VLANs. Pour des besoins spécifiques, comme le "ping", des exceptions comme "echo-reply" doivent être explicitement configurées pour éviter de bloquer entièrement la communication de réponse.

Pourquoi les LANs et Leurs Bénéfices Spécifiques

- **Partage des Ressources** : Imprimantes, fichiers, accès Internet – centralisé et accessible à tous.
- **Communication Rapide** : Interconnexion fluide entre les appareils, améliorant l'efficacité.
- **Contrôle et Sécurité Accrus** : Gestion centralisée des données et des accès.
- **Réduction des Coûts** : Optimisation des équipements en restant sur un réseau local.



Les réseaux locaux modernes sont essentiels pour une infrastructure informatique performante, sécurisée et économiquement viable, favorisant la collaboration et l'accès efficace aux ressources.