

🎓 Formations et vidéos gratuites recommandées

📺 Networking Fundamentals & VLAN / Routing

- 🔗 **Complete Practical Networking Course (YouTube)** – cours complet avec subnetting, VLANs, routage et plus (Practical Networking playlist) [Complete Networking Course on YouTube](#)
- 🔗 **Free CCNA VLANs (Inter-VLAN Routing)** – vidéo focalisée sur le routage entre VLANs sur YouTube [CCNA VLAN Inter-VLAN Routing Video](#)

📺 Proxy & Reverse Proxy

- 🔗 **Proxies & Reverse Proxies (YouTube course)** – couverture des concepts de proxy et reverse proxy, load balancing, SSL, HAProxy, NGINX, etc. [Free Proxy & Reverse Proxy Video Course](#)

🎓 Cours complémentaires (structures / playlists)

- 📌 **Computer Networks (YouTube playlist)** – vidéos réseaux complètes incluant OSI, TCP/IP, routage, sécurité [Computer Networks Full Playlist](#)
- 📌 **VLAN courses & certifications** – ressources listées pour apprendre VLANs sur YouTube et autres plateformes [VLAN Courses & Tutorials](#)
- 📌 **Reverse Proxy courses & certifications** – ressources pour apprendre et configurer reverse proxies (NGINX, Traefik, Squid, etc.) [Reverse Proxy Courses & Tutorials](#)

■ Améliorer ses compétences en réseaux informatiques.

Pour acquérir des **compétences de base en réseaux informatiques**, il existe de nombreuses ressources de qualité gratuites en ligne. Une excellente série vidéo pédagogique est la **Complete Practical Networking Course** sur *YouTube*, qui couvre les fondamentaux du *packet traveling*, de l'adressage IP, du *subnetting*, des VLANs, de la cryptographie et de la traduction d'adresses réseau (NAT) — idéale pour maîtriser les concepts essentiels du routage et de la segmentation de réseau.

Pour approfondir la gestion des VLANs et apprendre à router entre différents segments logiques, une excellente vidéo librement accessible est la **session CCNA sur l'inter-VLAN routing**, qui illustre la configuration sur des commutateurs multicouches.

En ce qui concerne les serveurs *proxy* et *reverse proxy*, des cours vidéo gratuits existent également : ces ressources expliquent les différences entre un serveur proxy (qui sert d'intermédiaire pour les clients demandant des ressources externes) et un reverse proxy (qui sert de façade sécurisée pour des serveurs internes), ainsi que des concepts avancés comme le *load balancing*, la terminaison SSL/TLS, et l'utilisation de solutions comme HAProxy ou NGINX.

D'autres playlists gratuites disponibles sur YouTube permettent de consolider sa compréhension du *networking* dans son ensemble — depuis le modèle OSI jusqu'à la sécurité réseau — et des plateformes listent des cours focalisés sur les VLANs ou les reverse proxies pour approfondir les compétences.

Concepts clés expliqués simplement

Routage

Le routage permet à des paquets IP de voyager entre différents réseaux ou sous-réseaux. Les routeurs utilisent des tables de routage et des protocoles (statique, OSPF, BGP, etc.) pour déterminer le meilleur chemin.

VLAN (Virtual LAN)

Un VLAN segmente un réseau physique en plusieurs *réseaux logiques* afin d'isoler le trafic, améliorer la sécurité et optimiser les performances. Le routage inter-VLAN permet la communication entre ces segments distincts.

Proxy serveur

Un **proxy** agit comme intermédiaire entre un client et le reste du réseau (internet ou services internes). Il peut être utilisé pour filtrer, cacher, ou anonymiser des requêtes.

Reverse Proxy

Un **reverse proxy** se situe devant un ou plusieurs serveurs et gère les requêtes clients pour ces services, offrant équilibrage de charge, sécurité (terminaison TLS) et optimisation de trafic.

Serveurs sécurisés, VPN et bonnes pratiques réseau

Dans les environnements modernes, la **sécurité des serveurs et du réseau** est un aspect critique. Un serveur sécurisé utilise des méthodes de protection telles que les **pare-feux**, le **chiffrement des communications (TLS/SSL)**, les systèmes de **détection d'intrusion (IDS/IPS)** et la gestion stricte des **droits et permissions** des utilisateurs. Les **VPN (Virtual Private Network)** permettent de créer des tunnels chiffrés entre un utilisateur ou un site distant et le réseau principal, garantissant confidentialité et intégrité des données échangées sur Internet ou des réseaux publics.

Les bonnes pratiques incluent :

- Utiliser des serveurs dédiés pour les services critiques (web, base de données, messagerie)
- Appliquer des **mise à jour régulières** et patchs de sécurité
- Mettre en place des systèmes de **journalisation et supervision** pour détecter les anomalies
- Séparer les environnements sensibles par des **réseaux isolés** (VLAN, DMZ, sous-réseaux sécurisés)
- Préférer l'utilisation de **protocoles sécurisés** (HTTPS, SFTP, SSH, IPsec) pour toutes les communications

Pour trouver des formations de qualité sur ces sujets, il est conseillé de rechercher des cours gratuits abordant :

- Les **bases des réseaux sécurisés** et configuration de pare-feux
- La mise en place de **VPN site-à-site et client-à-site**
- La gestion de **serveurs Linux ou Windows sécurisés**
- La configuration de **reverse proxies sécurisés**, load balancing et terminaux TLS

Sur YouTube et plateformes gratuites, il existe des playlists axées sur : réseaux sécurisés, VPN OpenVPN/IKEv2, serveurs web sécurisés (NGINX/Apache), et bonnes pratiques de sécurité réseau. Les mots-clés pour les recherches efficaces incluent : "network security basics", "VPN configuration tutorial", "secure server setup", "firewall configuration tutorial", "reverse proxy security".

Certificats numériques et génération

Les **certificats numériques** sont essentiels pour sécuriser les communications sur un réseau. Ils permettent de :

- **Authentifier** un serveur ou un service auprès des clients
- **Chiffrer** les données échangées via TLS/SSL (HTTPS, VPN, e-mails sécurisés, etc.)
- Garantir l'intégrité et la confidentialité des informations transitant sur le réseau

Types de certificats

- **Certificats publics** : délivrés par des autorités de certification reconnues (CA) comme Let's Encrypt, DigiCert ou GlobalSign. Utilisés principalement pour sécuriser des sites web ou des services accessibles publiquement.
- **Certificats internes** : générés en interne via une infrastructure PKI (Public Key Infrastructure). Utilisés pour sécuriser des services internes, VPN, messagerie d'entreprise, ou authentification interne.

Génération de certificats

1. Création d'une **clé privée** sur le serveur
2. Génération d'une **CSR (Certificate Signing Request)** incluant les informations du serveur et de l'organisation
3. Soumission de la CSR à une **autorité de certification** pour signature (ou signature interne pour les certificats internes)
4. Installation du certificat signé sur le serveur et configuration des services concernés

Bonnes pratiques

- Renouveler régulièrement les certificats avant expiration
- Protéger strictement les clés privées
- Surveiller la chaîne de confiance et la validité des certificats
- Utiliser des certificats distincts pour chaque service critique pour limiter les risques

Pour l'apprentissage, il existe des formations et tutoriels gratuits sur :

- La **génération de certificats SSL/TLS avec OpenSSL**
- La **mise en place de PKI interne**
- L'utilisation de certificats dans des **VPN sécurisés** et reverse proxies

Mots-clés pour recherches et vidéos YouTube :

"generate SSL certificate tutorial", "OpenSSL certificate tutorial", "PKI internal certificate setup", "HTTPS server certificate setup", "VPN SSL certificate configuration"