




Recommended Free Training & Video Resources




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](#)

General Computer Networking 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](#)

Improve Your Networking Skills

To build a strong foundation in **computer networking**, start with the **Complete Practical Networking Course** which explains how data travels through networks, covering subnetting, VLANs, routing, cryptography basics, and network address translation — ideal for understanding essential concepts of routing and network segmentation.

For structured networking knowledge from beginner to advanced topics, including routing protocols, VLAN configuration, DHCP/NAT, and network troubleshooting, the **CCNA Topics** videos provide an excellent free resource with practical configuration examples.

Proxy and reverse proxy servers are covered extensively in free video series that explain the differences between forwarding proxies (which act on behalf of clients) and reverse proxies (which act as secure frontends for backend servers), including advanced topics like load balancing and SSL/TLS termination using tools such as HAProxy and NGINX.

Other free YouTube playlists on **general computer networking** reinforce your understanding of core concepts — from the OSI model to network security — and can be used alongside practical configuration labs.

Key Concepts Explained Simply

Routing

Routing enables IP packets to travel between different networks or subnets. Routers use routing tables and protocols (such as static routes, OSPF, and BGP) to determine the best path for traffic.

VLAN (Virtual Local Area Network)

A VLAN partitions a physical network into multiple logical networks to isolate traffic, improve performance, and enhance security. Inter-VLAN routing allows devices in different VLANs to communicate.

Proxy Server

A proxy server acts as an intermediary between clients and other network services. It can filter traffic, cache content, enforce policies, and even anonymize requests in certain contexts.

Reverse Proxy

A reverse proxy sits in front of backend servers and handles inbound traffic, providing benefits such as load balancing, secure TLS termination, and centralized access control.

Secure Servers, VPNs & Best Practices

In modern IT environments, **secure server and network design** is critical. A secure server leverages protections such as firewalls, **TLS/SSL encryption**, intrusion detection/prevention systems (IDS/IPS), and strict access controls.

VPNs (Virtual Private Networks) create encrypted tunnels that secure traffic between remote users or sites and the primary network, ensuring data confidentiality and integrity over public or untrusted connections.

Recommended practices include:

- Deploying dedicated servers for critical services (web, database, email)
- Regular security patching and updates
- Logging and monitoring to detect anomalies
- Isolating sensitive resources via VLANs, DMZs, or secure subnets
- Using secure protocols (HTTPS, SFTP, SSH, IPsec) for all communications

To learn these topics, look for free courses covering:

- Network security fundamentals and firewall configuration
- Site-to-site and client-to-site VPN setup
- Secure server configuration (Linux/Windows)
- Secure reverse proxy and load balancing implementation

Search keywords on YouTube or free platforms that work well include:

"network security basics", "VPN configuration tutorial", "secure server setup", "firewall configuration tutorial", "reverse proxy security".

Digital Certificates & Generation

Digital certificates are crucial for **securing network communications**. They allow:

- **Authentication** of servers or services
- **Encryption** of data using TLS/SSL (e.g., HTTPS, secure email, VPN)
- **Integrity and confidentiality** of sensitive transactions

Certificate types:

- **Public certificates** — issued by trusted Certificate Authorities (CAs) like Let's Encrypt, DigiCert, or GlobalSign.
- **Internal certificates** — generated within an organization's PKI (Public Key Infrastructure) for internal services, secure VPNs, or corporate apps.

Typical generation steps:

1. Create a **private key** on the server
2. Generate a **CSR (Certificate Signing Request)** with server and organization data
3. Submit the CSR to a CA (or self-sign for internal use)
4. Install the signed certificate and configure the appropriate service

Best practices:

- Renew certificates before expiration
- Protect private keys carefully
- Monitor certificate validity and trust chains
- Use unique certificates for critical services

For learning, there are **free tutorials on generating SSL/TLS certificates** with OpenSSL, setting up an internal PKI, and integrating certificates into VPNs and reverse proxy configurations — for example, tutorials on CA server creation with OpenSSL on YouTube.

Keywords for YouTube search:

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