

Mis à jour le 18/08/2025

S'inscrire

# Formation Network Basics Support

3 jours (21 heures)

## Présentation

Network Basics Support est une formation pensée pour les équipes de support et d'exploitation souhaitant acquérir des bases solides en réseaux informatiques.

Elle permet de comprendre les concepts fondamentaux (adressage IP, routage, protocoles), de manipuler les équipements réseau (switches, routeurs, firewalls), et de développer des compétences concrètes en supervision et dépannage.

Notre formation vous aidera à maîtriser les outils essentiels (ping, tracer, Wireshark, monitoring), sécuriser les environnements (VLAN, ACL, VPN), et accompagner efficacement les utilisateurs en cas d'incident réseau.

À l'issue, vous serez capable de déployer et dépanner des réseaux simples, d'intégrer des environnements cloud (Azure, AWS, GCP), et d'industrialiser vos pratiques de support grâce à la documentation et l'automatisation.

Comme toutes nos formations, celle-ci présente les dernières versions stables des outils étudiés et leurs nouveautés.

## Objectifs

- Comprendre l'architecture et les protocoles réseaux essentiels
- Configurer IP, VLAN et VPN de base
- Diagnostiquer avec Wireshark et résoudre des incidents
- Mettre en place une supervision simple (Zabbix/Nagios)
- Appliquer les bonnes pratiques de sécurité (ACL, segmentation)
- Documenter et industrialiser le support réseau

## Public visé

- Techniciens support/helpdesk
- Administrateurs systèmes
- Responsables IT
- Développeurs/intégrateurs

## Pré-requis

- Connaissances informatiques générales
- Notions de base Windows/Linux recommandées

## Programme de formation notre Network Basics Support

### Introduction aux réseaux et concepts fondamentaux

- Rôle d'un réseau informatique dans l'entreprise
- Panorama LAN, WAN, WLAN, VPN
- Équipements : switches, routeurs, pare-feu
- Modèles OSI et TCP/IP expliqués simplement
- Adressage IPv4/IPv6, masques et sous-réseaux
- atelier : créer un mini-réseau local simulé

### Adressage, routage et connectivité

- Comprendre IP, CIDR et sous-réseaux
- Notions de routage statique vs dynamique
- Services essentiels : ARP, DHCP, DNS
- Passerelles et interconnexion de réseaux
- Outils de test : ping, traceroute, nslookup
- atelier : configurer IP manuellement et valider la connectivité

### Protocoles réseau essentiels

- Transports : TCP, UDP, ICMP
- Applicatifs : HTTP/HTTPS, FTP, SMTP/IMAP, DNS
- Fiabilité, ports et états de connexion
- Sécurité de base : SSL/TLS et chiffrement
- Bonnes pratiques support (check-lists et triage)
- atelier : analyser des trames avec Wireshark

### Équipements et infrastructures réseau

- Rôle des switches et routeurs
- Wi-Fi d'entreprise : AP, canaux, roaming
- Pare-feu matériels & logiciels (principes)
- Câblage, RJ45, fibre et topologies

- Virtualisation & SDN (aperçu)
- atelier : mise en route d'un switch + point d'accès

## Sécurité et bonnes pratiques réseau

- Menaces : sniffing, spoofing, DDoS
- Politiques d'accès & mots de passe
- Segmentation par VLAN
- ACL et filtrage de base
- Supervision & journaux : pourquoi et comment
- atelier : créer un VLAN + règles de pare-feu simples

## Supervision et dépannage réseau

- Méthodes de résolution d'incidents (L1/L2)
- Outils : Nagios, Zabbix, PRTG
- Lecture de logs et corrélation d'événements
- Identifier pannes physiques vs logicielles
- Escalade et communication
- atelier : simuler une panne et la résoudre

## Réseaux d'entreprise et connectivité avancée

- Architecture réseau d'entreprise (couches & zones)
- MPLS, VPN, SD-WAN : cas d'usage
- Haute dispo & redondance
- Qualité de service QoS
- Services critiques : DNS interne, DHCP centralisé
- atelier : configurer un VPN site-à-site (démonstration guidée)

## Cloud et virtualisation réseau

- VPC/VNet : AWS, Azure, GCP
- Réseaux hybrides et connectivité
- Overlays : VXLAN, GRE (aperçu)
- Conteneurs & réseau Kubernetes (bases)
- Sécurité & gouvernance dans le cloud
- atelier : créer un réseau virtuel simple (cloud)

## Bonnes pratiques et roadmap pour le support

- Standardiser : modèles & documentation
- Automatiser (scripts, Ansible)
- Gestion d'incidents et escalade
- Communication avec utilisateurs & métiers
- Veille : 5G, IoT, Zero Trust

- atelier : rédiger un runbook réseau d'équipe

## Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

## Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

## Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

## Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

## Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

## Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.