

Mis à jour le 04/12/2025

S'inscrire

# Formation Certification JNCIS-SP

3 jours (21 heures)

## Présentation

La certification Juniper JNCIS-SP est une formation avancée destinée aux professionnels des réseaux opérateurs et infrastructures backbone. Conçue pour les environnements Service Provider, elle valide des compétences clés en conception, déploiement et dépannage d'architectures MPLS modernes basées sur Junos OS.

Notre formation JNCIS-SP vous permettra d'approfondir les technologies essentielles aux réseaux opérateurs : MPLS, LDP, RSVP-TE, services L2VPN/L3VPN, MP-BGP, ainsi que la supervision avancée du dataplane MPLS. Vous découvrirez comment les opérateurs construisent des topologies multiservices performantes, résilientes et hautement scalables.

Vous apprendrez à déployer des circuits L2/L3, à gérer la distribution de labels, à mettre en place des tunnels Traffic Engineering et à superviser les flux MPLS avec les outils Junos dédiés. Les ateliers pratiques, présents à chaque chapitre, permettent d'ancrer les compétences dans des scénarios réels d'exploitation opérateur.

La dernière partie est entièrement dédiée à la préparation à la certification, comprenant un examen blanc complet, des questions types et un atelier final de déploiement bout-en-bout pour vous permettre d'aborder sereinement l'examen JNCIS-SP.

Comme toutes nos formations, celle-ci s'appuie sur la dernière version stable du [Junos OS](#) et privilégie une approche résolument pratique, opérationnelle et orientée compétences.

Note : Ambient IT n'est pas propriétaire de la certification JNCIS-SP, elle appartient à Juniper Networks Inc.

## Objectifs

- Comprendre l'architecture Service Provider MPLS.
- Maîtriser LDP, RSVP-TE, MP-BGP, L2/L3VPN/.

- Déployer des environnements MPLS multi-services.
- Superviser et diagnostiquer un backbone opérateur.
- Mettre en œuvre les bonnes pratiques Juniper SP.
- Se préparer efficacement à la certification JNCIS-SP.

## Public visé

- Ingénieurs Réseaux
- Ingénieurs Service Provider
- Administrateurs backbone/MPLS
- Professionnels visant la certification JNCIS-SP

## Pré-requis

- Connaissances réseau avancées L2/L3
- Compétences en routage dynamique (OSPF/BGP)
- Première expérience souhaitée avec Junos OS

## Programme de formation JNCIS-SP - Service Provider

[Jour 1 - Matin]

### Introduction au Service Provider et aux fondamentaux Juniper

- Comprendre l'architecture d'un réseau Service Provider
- Différences entre plan de contrôle et plan de données
- Notions essentielles du Junos OS
- Modes Operational et Configuration
- Périmètre de la certification JNCIS-SP
- Atelier pratique : Prise en main de Junos et commandes SP.

[Jour 1 - Après-midi]

### Architecture MPLS et fonctionnement du forwarding

- Principes du MPLS : labels, LSP, LFIB
- Fonctionnement push / swap / pop
- Concept de PHP (Penultimate Hop Popping)
- Différence entre forwarding IP et MPLS
- Intégration MPLS dans un réseau opérateur
- Atelier pratique : Analyser le dataplane MPLS dans la LFIB.

### LDP : découverte et distribution de labels

- Fonctionnement du protocole LDP
- Établissement et suivi des sessions (hello, keepalive)
- Gestion des FEC et des labels
- Relation entre IGP et LDP
- Diagnostic des erreurs LDP
- Atelier pratique : Configurer LDP et corriger les erreurs courantes.

[Jour 2 - Matin]

## MPLS Traffic Engineering

- Concepts clés du Traffic Engineering
- Fonctionnement du protocole RSVP-TE
- Création et signalisation des tunnels TE
- Gestion de la protection et de la préemption
- Utilisation du TE dans les réseaux opérateurs
- Atelier pratique : Déployer un LSP TE avec chemin principal et secours.

[Jour 2 - Après-midi]

## Services L2VPN

- Comprendre les services L2VPN dans MPLS
- Encapsulation Martini et services CCC
- Fonctionnement d'un VPLS et rôle du split horizon
- Transport L2 dans les environnements SP
- Dépannage des services L2VPN
- Atelier pratique : Déployer un VPLS complet entre plusieurs provider edge.

## Services L3VPN : architecture et VRF

- Comprendre le fonctionnement d'un L3VPN MPLS
- Rôle des VRF et des route-target
- Comment fonctionnent les mécanismes d'import/export
- Intégration entre MP-BGP et MPLS
- Connexion Provider Edge - Customer Edge : statique, OSPF ou BGP
- Atelier pratique : Mise en place complète d'un L3VPN PE-CE.

[Jour 3 - Matin]

## MP-BGP dans les environnements Service Provider

- Familles d'adresses VPNv4 et VPNv6
- Fonction des extended communities

- Configuration d'un Route Reflector SP
- Dépannage MP-BGP
- Optimisation du transport des routes VPN
- Atelier pratique : Configurer un RR et échanger des routes VPNv4.

## [Jour 3 - Après-midi]

### Outils de supervision et troubleshooting SP

- Utilisation de ping mpls et traceroute mpls
- Analyse du comportement du dataplane MPLS
- Lire la table MPLS (LFIB) et vérifier les routes VPN dans BGP
- Méthodologie de diagnostic opérateur
- Vérification totale des services SP
- Atelier pratique : Résolution d'incidents MPLS / LDP / RSVP.

### Préparation à la certification JNCIS-SP

- Structure détaillée de l'examen JNCIS-SP
- Thèmes les plus évalués : MPLS, LDP, RSVP-TE, L2VPN / L3VPN
- Conseils, pièges et stratégie de réussite
- Révision des commandes essentielles Junos
- Simulation de questions types
- Atelier pratique : Passage de l'examen blanc + correction.

## 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.