



Course Title: Securing Networks with Cisco Routers and Switches (SNRS)
Duration: 5 days

Certification

This course forms a part of the CCSP and completes course material for exam **642-503 SNRS**

Objectives

After completing this course the delegate will be able to:

- Implement Layer 2 security features
- Implement the Cisco Trust and Identity Management model to control network access
- Implement command line Network Foundation Protection to protect infrastructure devices
- Implement command line Network Foundation Protection to protect infrastructure devices
- Implement secure IPsec VPNs and GRE tunnels using Cisco routers
- Install, configure, and troubleshoot Cisco IOS Firewall features, including CBAC, Cisco IOS Firewall authentication proxy, and Cisco IOS IPS on a Cisco router
- Secure tunnels using generic routing encapsulation (GRE) and IP Security (IPsec) technology
- Basic switch access security
- The Cisco Trust and Identity Management model to control network access Command Line (CLI) Cisco Network Foundation Protection (NFP)

Pre-Requisites

- Cisco Certified Networking Associate (CCNA)
- Securing Network Devices (SND)
- Basic knowledge of Windows operating system

Content

Aimed at providing the knowledge and skills needed to secure Cisco IOS router and switch networks, the course has been updated for Cisco IOS Release 12.4(6)T.

- Module 1 Layer 2 Security
- Module 2 Trust and Identity
- Module 3 Cisco Network Foundation Protection
- Module 4 Secured Connectivity
- Module 5 Adaptive Threat Defense