Introduction to 802.1X Operations for Cisco Security Professionals (CPLL-802.1X) v3.0

Duration: 180 days

The Introduction to 802.1X Operations for Cisco Security Professionals (802.1X) Learning Path shows you how to configure and prepare to deploy Cisco® Identity-Based Networking Services (IBNS) solutions based on Cisco Catalyst switches, Cisco 9800 LAN Controllers, and Cisco Meraki deployments. You will learn the fundamentals of the 802.1X protocol and configuration, Cisco IBNS, configuring access for non-supplicant devices, architectural components, and considerations with 802.1X.

Skills You'll Learn:

- Understand the fundamentals and operation of the 802.1X protocol within Cisco environments
- Identify and describe Cisco Identity-Based Networking Services (IBNS) and how 802.1X functions as a foundational security element
- Compare different Extensible Authentication Protocol (EAP) methods and select the most appropriate for deployment needs
- Configure 802.1X authentication on Cisco Catalyst switches
- Configure 802.1X authentication on Cisco 9800 Wireless LAN Controllers using the GUI
- Configure 802.1X authentication on Cisco Meraki devices
- Integrate non-supplicant devices (devices without native 802.1X support) using MAC Authentication Bypass (MAB) and guest services
- Verify device authentication and network access using Cisco ISE live logs
- Apply best practices for designing 802.1X-enabled networks
- Troubleshoot Cisco IBNS deployments, including configuration and live log analysis
- Gain hands-on experience through real-world labs on configuring and troubleshooting IBNS and 802.1X across multiple Cisco platforms

Learning Path Objectives:

1. Cisco IBNS and 802.1X Overview: Explore how Cisco Identity-Based Networking Services (IBNS) leverages IEEE 802.1X and AAA frameworks to enable dynamic, secure, and scalable access control policies across enterprise networks.
2. 802.1X Configuration for Network Devices: Discover how to configure and manage IEEE 802.1X authentication on Cisco Catalyst, wireless controllers, and Meraki networks for secure, scalable enterprise access.
3. Non-Supplicant Network Access and Cisco IBNS Design: Describe how to implement and validate MAB and 802.1X client configurations on Cisco devices to securely onboard diverse endpoints and enforce identity-based access controls.