Introduction to 802.1X Operations for Cisco Security Professionals

Introduction to 802.1X Operations for Cisco Security Professionals

In this Introduction to 802.1X Operations for Cisco Security Professionals course provides a practical, end-to-end introduction to Cisco Identity-Based Networking Services, focusing on secure network access using 802.1X across wired and wireless environments. It is designed for network and security professionals who need to implement consistent, identity-driven access control across Cisco Catalyst switches, wireless LAN controllers, and Meraki devices. The course builds from foundational authentication concepts into real-world deployment and troubleshooting scenarios.

Students begin with an overview of Cisco IBNS and 802.1X EAP authentication methods, including modern approaches such as TEAP. The curriculum then explores detailed configuration of 802.1X on wired Catalyst switches, Cisco wireless LAN controllers, and Meraki platforms, highlighting similarities and key differences in implementation. Special attention is given to handling non-supplicant devices through MAC Authentication Bypass, ensuring secure access for printers, phones, and IoT devices without compromising network posture.

Hands-on labs reinforce each module by guiding students through supplicant configuration, network device setup, and end-to-end authentication testing. The course concludes with design considerations and structured troubleshooting techniques, enabling students to diagnose authentication failures, policy misconfigurations, and integration issues. By the end of the course, learners are prepared to design, deploy, and support scalable Cisco IBNS and 802.1X-based access control solutions in enterprise networks.

How you'll benefit

This class will help you:

- Gain in-depth knowledge of 802.1X protocol fundamentals, configuration, and integration within Cisco environments
- Learn to configure 802.1X on Cisco Catalyst switches, Cisco Wireless LAN Controllers, and Meraki devices through real-world labs
- Understand Cisco IBNS operations and how 802.1X functions as a foundational element for secure network access
- Acquire the ability to integrate non-supplicant devices (devices without native 802.1X support) using MAC Authentication Bypass (MAB) and guest services
- Compare and select the most appropriate Extensible Authentication Protocol (EAP) methods for your organization's deployment needs
- Learn best practices for designing 802.1X-enabled networks and troubleshooting IBNS deployments to ensure reliable, secure access
- Earn 18 CE credits toward recertification

Course Duration
3 days
Course Price
$3,495.00 or 27 CLCs
Methods of Delivery
- Instructor Led
- Virtual ILT
- On-Site

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The primary audience for this course is as follows:

- Security Administrators
- Security Consultants
- Network Administrators
- System Engineers
- Technical Support Personnel
- Channel Partners and Resellers

Prerequisites

To fully benefit from this course, you should have knowledge of these topics:

- Basic routing and switching knowledge

OUTLINE

Module 1: Introduction to Cisco IBNS

Module 2: 802.1X EAP Authentication

Module 3: 802.1X on Cisco Catalyst Switches

Module 4: 802.1X on Cisco Wireless LAN Controllers

Module 5: 802.1X on Meraki Devices

Module 6: Network Access for Non-Supplicant Devices

Module 7: Design Considerations and Troubleshooting for Cisco IBNS Networks

Lab Outline

- Lab 1: Configure an 8021.X Supplicant for Tunneled EAP (TEAP)
- Lab 2: Configure Cisco Catalyst Switch for IEEE 802.1X
- Lab 3: 802.1X Configuration on Cisco Wireless LAN Controllers
- Lab 4: 802.1X Configuration on Meraki Devices
- Lab 5: Configure MAC Authentication Bypass on Cisco Network Devices
- Lab 6: Troubleshoot Cisco IBNS Networks