IPv6 Fundamentals, Design and Deployment (IP6FD) v3.0

What you'll learn in this course

IPv6 Fundamentals, Design, and Deployment (IP6FD) v3.0 is an instructor-led course that is presented by Cisco Learning Partners to end-user customers. This five-day course provides network engineers and technicians who are working in the enterprise sector with the knowledge and skills that are needed to study and configure the IP version 6 (IPv6) features of Cisco IOS Software. The course also provides an overview of IPv6 technologies; covers IPv6 design and implementation; describes IPv6 operations, addressing, routing, services, and transition; and describes deployment of IPv6 in enterprise networks as well as in service provider networks. The course also includes case studies that are useful for deployment scenarios and remote labs.

Course duration

- Instructor-led training: 5 days in the classroom with hands-on practice
- E-learning: 5 days of hands-on practice, plus equivalent of 3 days of content with practice and challenges

How you'll benefit

This course will help you:

- Gain an advanced understanding of the tasks involved for senior-level roles in a security operations center
- Configure common tools and platforms used by security operation teams via practical application
- Respond like a hacker in real-life attack scenarios and submit recommendations to senior management
- Prepare for the **350-201 CBRCOR** core exam
- Earn 40 CE credits toward recertification

Who should enroll

Although there are no mandatory prerequisites, the course is particularly suited for the following audiences:

- Cybersecurity engineer
- Cybersecurity investigator
- Incident manager
- Incident responder
- Network engineer
- SOC analysts currently functioning at entry level with a minimum of 1 year of experience

Course details

Objectives

Upon completing this course, the learner will be able to meet these overall objectives:

- Describe the factors that led to the development of IPv6, and the possible uses of this new IP structure.
- Describe the structure of the IPv6 address format, how IPv6 interacts with data link layer technologies, and how IPv6 is supported in Cisco IOS Software.
- Describe the nature of changes to DNS and DHCP to support IPv6, and how networks can be renumbered using both services.
- Understand the updates to IPv4 routing protocols needed to support IPv6 topologies.
- Understand multicast concepts and IPv6 multicast specifics.
- Describe IPv6 transition mechanisms and which methods will be most effective in your network.
- Describe the standards bodies that define IPv6 address allocation, as well as one of the leading IPv6 deployment issues, multihoming.
- Describe the deployment strategies that service providers are facing when deploying IPv6.
- Describe case studies for enterprise, service provider, branch, and access networks.

Recommended knowledge and training

The knowledge and skills that a learner must have before attending this course are as follows:

- Cisco Certified Network Associate (CCNA) certification.
- Understanding of networking and routing (on CCNP level, but no certification required).
- Working knowledge of the Microsoft Windows operating system.

• Module 1: Introduction to IPv6
o Lesson 1-1: Explaining the Rationale for IPv6
o Lesson 1-2: Evaluating IPv6 Features and Benefits
o Lesson 1-3: Understanding Market Drivers
• Module 2: IPv6 Operations
o Lesson 2-1: Understanding the IPv6 Addressing Architecture
o Lesson 2-2: Describing the IPv6 Header Format
oLesson 2-3: Enabling IPv6 on Hosts
oLesson 2-4: Enabling IPv6 on Cisco Routers
oLesson 2-5: Using ICMPv6 and Neighbor Discovery
oLesson 2-6: Troubleshooting IPv6
• Module 3: IPv6 Services
o Lesson 3-1: IPv6 Mobility
o Lesson 3-2: Describing DNS in an IPv6 Environment
o Lesson 3-3: Understanding DHCPv6 Operations
o Lesson 3-4: Understanding QoS Support in an IPv6 Environment
o Lesson 3-5: Using Cisco IOS Software Features
• Module 4: IPv6-Enabled Routing Protocols
o Lesson 4-1: Routing with RIPng
o Lesson 4-2: Examining OSPFv3
o Lesson 4-3: Examining Integrated IS-IS
o Lesson 4-4: Examining EIGRP for IPv6
o Lesson 4-5: Understanding MP-BGP
o Lesson 4-6: Configuring IPv6 Policy-Based Routing
o Lesson 4-7: Configuring FHRP for IPv6
o Lesson 4-8: Configuring Route Redistribution
• Module 5: IPv6 Multicast Services
o Lesson 5-1: Implementing Multicast in an IPv6 Network
o Lesson 5-2: Using IPv6 MLD
• Module 6: IPv6 Transition Mechanisms
o Lesson 6-1: Implementing Dual-Stack
o Lesson 6-2: Describing IPv6 Tunneling Mechanisms
• Module 7: IPv6 Security
o Lesson 7-1: Configuring IPv6 ACLs
o Lesson 7-2: Using IPsec, IKE, and VPNs
o Lesson 7-3: Discussing Security Issues in an IPv6 Transition Environment
o Lesson 7-4: Understanding IPv6 Security Practices
o Lesson 7-5: Configuring Cisco IOS Firewall for IPv6
• Module 8: Deploying IPv6
o Lesson 8-1: Examining IPv6 Address Allocation
o Lesson 8-2: Understanding the IPv6 Multihoming Issue
o Lesson 8-3: Identifying IPv6 Enterprise Deployment Strategies
• Module 9: IPv6 and Service Providers
o Lesson 9-1: Identifying IPv6 Service Provider Deployment
o Lesson 9-2: Understanding Support for IPv6 in MPLS
o Lesson 9-3: Understanding 6VPE
o Lesson 9-4: Understanding IPv6 Broadband Access Services
• Module 10: IPv6 Case Studies
o Lesson 10-1: Planning and Implementing IPv6 in Enterprise Networks
o Lesson 10-2: Planning and Implementing IPv6 in Service Provider Networks
o Lesson 10-3: Planning and Implementing IPv6 in Branch Networks

How to enroll

To enroll in the CBRCOR course or explore our larger catalog of courses on Cisco Digital Learning, contact us at <training@fastlane-mea.com>

Outline

- Understanding Risk Management and SOC Operations
- Understanding Analytical Processes and Playbooks
- Investigating Packet Captures, Logs, and Traffic Analysis
- Investigating Endpoint and Appliance Logs
- Understanding Cloud Service Model Security Responsibilities
- Understanding Enterprise Environment Assets
- Implementing Threat Tuning
- Threat Research and Threat Intelligence Practices
- Understanding APIs
- Understanding SOC Development and Deployment Models
- Performing Security Analytics and Reports in a SOC
- Malware Forensics Basics
- Threat Hunting Basics
- Performing Incident Investigation and Response

Lab outline

- Explore Cisco SecureX Orchestration
- Explore Splunk Phantom Playbooks
- Examine Cisco Firepower Packet Captures and PCAP Analysis
- Validate an Attack and Determine the Incident Response
- Submit a Malicious File to Cisco Threat Grid for Analysis
- Endpoint-Based Attack Scenario Referencing MITRE ATTACK
- Evaluate Assets in a Typical Enterprise Environment
- Explore Cisco Firepower NGFW Access Control Policy and Snort Rules
- Investigate IOCs from Cisco Talos Blog Using Cisco SecureX
- Explore the ThreatConnect Threat Intelligence Platform
- Track the TTPs of a Successful Attack Using a TIP
- Query Cisco Umbrella Using Postman API Client
- Fix a Python API Script
- Create Bash Basic Scripts
- Reverse Engineer Malware
- Perform Threat Hunting
- Conduct an Incident Response