

CISCO CERTIFIED NETWORK ASSOCIATE (CCNA) TRAINING

Objective: This training is aimed to give a foundation in and apprenticeship of networking to your Company's Computer Administrators and Support Staff. They will be able to efficiently install, configure and operate Local Area Networks, Wide Area Networks and dial access services for small networks (100 nodes or fewer) using various protocols like IP, IGRP, Serial Frame relay, IP RIP, VLANs, RIP, Ethernet, Access Lists

The Cisco Certified Network Associate (CCNA) course consists of semesters 1 to 4 of the Cisco Networking Academy Program.

Module 1

- OSI model and industry standards
- Network topologies
- IP addressing, including subnet masks
- Networking components
- Basic network design

Module 2

- Beginning router configurations
- Routed and routing protocols

Module 3

- Advanced router configurations
- LAN switching theory and VLANs
- Advanced LAN and LAN switched design
- Novell IPX
- Threaded case studies

Module 4

- WAN theory and Design
- WAN technology, PPP, Frame Relay, ISDN
- Network troubleshooting
- National SCANS Skills
- Threaded case study

CISCO CERTIFIED NETWORK PROFESSIONAL

The Cisco Certified Network Professional (CCNP) course consists of semesters 5 to 8 of the Cisco Networking Academy Program. (Note: academic students should not get these confused with University semesters).

Module 5

- Overview of Scalable Internet works
- Introduction to Managing Traffic and Access
- Managing IP Traffic
- Configuring Queuing to Manage Traffic
- Routing Protocols Overview
- Extending IP Addresses Using VLSMs
- Configuring OSPF in a Single Area

- Interconnecting Multiple OSPF Areas
- Configuring Enhanced IGRP
- Optimizing Routing Update Operation
- Configuring BGP
- Quality of Service

Module 6

- Selecting Cisco Products for Remote Connections
- Assembling and Cabling the WAN Components
- Configuring Asynchronous Connections with Modems
- Accessing the Central Site with Windows 95
- Configuring PPP and Controlling Network Access with PAP or CHAP
- Using ISDN and DDR to Enhance Remote Connectivity
- Optimizing Use of DDR Interfaces
- Configuring a Cisco 700 Series Router
- Establishing a Dedicated Frame Relay Connection and Controlling Traffic Flow with Traffic Shaping
- Enabling a Backup to the Permanent Connection
- Optimizing Traffic on Dedicated WAN Connections
- Scaling IP Addresses with PAT and NAT
- Troubleshooting the Remote Access Network

Module 7

- Introduction to Switching Concepts
- Virtual LANs
- Placing Catalyst® Switches in your Network
- Catalyst Switch Overview
- Catalyst Switch Architecture
- Catalyst Switch Hardware
- Configuring the Supervisor Module and Fast Ethernet
- Catalyst Switch Software
- Managing the Catalyst Switch
- Troubleshooting the Catalyst Switch
- Catalyst 2900 Series Features
- Configuring Catalyst 2900 Series Switches

Module 8

- Support Resources for Troubleshooting
- Using Troubleshooting Methods
- Identifying Troubleshooting Targets
- Applying Cisco Troubleshooting Tools
- Workgroup Discovery Lab and CCO
- Using a Troubleshooting Method
- Documenting Symptoms, Actions and Results
- Tracking Log-ins and Connections
- Using Cisco Show and Debug Commands
- Diagnosing and Correcting Campus TCP/IP Problems
- Diagnosing and Correcting Catalyst Problems
- Troubleshooting VLANs on Routers and Switches

- Diagnosing and Correcting Frame Relay Problems
- Diagnosing and Correcting ISDN BRI Problems studies

Securing Cisco IOS Networks (Secure) – 5-day Hands-on Authorized Cisco Course

Course Description

SECUR is a five-day, leader-led, lab-intensive course, which will be delivered by Cisco Learning Partners (CLPs). This task-oriented course teaches the knowledge and skills needed to secure Cisco IOS router networks.

Course Objectives

After completing this course the student should be able to:

- Identify network security threats.
- Secure remote access using Cisco Secure ACS for Windows 2000 and Cisco IOS AAA software features.
- Protect Internet access by configuring a Cisco perimeter router.
- Configure the Cisco IOS Firewall Feature Set Context-Based Access Control.
- Configure Cisco IOS Firewall Authentication Proxy
- Configure Cisco IOS Firewall Intrusion Detection System
- Use IPSec features in Cisco IOS software to create a secure site-to-site VPN using pre-shared keys and digital certificates.
- Use Cisco Easy VPN features to create a secure remote access VPN solution.
 - Use Cisco Router Management Center to manage Cisco Router VPN implementations.

Cisco Secure Pix Firewall Advanced (CSPFA) – 4-day Hands-on Authorized Cisco Course

Course Description

The CSPFA course is a four-day, leader-led, lab-intensive course. The CSPFA course is designed for delivery by Cisco Training Partners. This task-oriented course teaches the knowledge and skill needed to describe, configure, verify and manage the PIX Firewall product family.

Course Objectives

After completing this course the student should be able to:

- Describe the features, functions, and benefits of the Cisco PIX Firewall.
- Identify PIX Firewall features, models, components, and benefits.
- Describe PIX Firewall installation procedures.
- Perform basic configuration.
- Explain the routing functionality of the PIX Firewall.
- Configure routing on the PIX Firewall.
- Configure the PIX Firewall to send messages to a Syslog server.
- Configure the PIX Firewall as a DHCP client.

- Configure special protocol handling on the PIX Firewall.
- Describe how the PIX Firewall supports call handling sessions and VoIP call signaling.
- Configure AAA on the PIX Firewall.
- Configure shunning on the PIX Firewall.
- Configure a site-to-site VPN using the PIX Firewall.
- Configure a VPN Client-to-PIX Firewall VPN.
- Configure the PIX Firewall's PPPoE client.
- Perform password recovery on the PIX Firewall.
- Install the PIX Device Manager and use it to configure the PIX Firewall.
- Use the PIX Device Manager to monitor the PIX Firewall.
- Configure a site-to-site VPN using the PIX Device Manager.
- Test and verify PIX Firewall operations.

Cisco Secure Intrusion Detection System (CSIDS) – 4-day Hands-on Authorized Cisco Course

Course Description

This task-oriented course teaches the knowledge and skills needed to design, install, and configure a Cisco Intrusion Protection solution for small, medium, and enterprise networks. The course covers CIDS detection platforms including the 4200 series Sensors, and the Catalyst 6000 series Intrusion Detection Module (IDSM). The Cisco IDS Host Sensor is introduced but is not discussed in detail. The Cisco Secure Intrusion Detection Host Sensor (CSIHS) course is recommended for those students seeking in-depth discussions and hands-on lab exercises. The IDS Device Manager and IDS Management center are used to configure and manage Cisco IDS Sensor platforms. The IDS Event Viewer and IDS Security Monitor Center are used to view and respond to IDS alarms.

Course Objectives

After completing this course the student should be able to:

- Describe the basic intrusion detection terminology.
- Explain the different intrusion detection technologies and evasive techniques.
- Design a Cisco IDS protection solution for small, medium, and enterprise customers.
- Identify the Cisco IDS Sensor platforms and describe their features.
- Install and configure a Cisco IDS Sensor including a network appliance and IDS module.
- Tune CIDS signatures to work optimally in unique network environments.
- Create and implement customized intrusion detection signatures.
- Create alarm exceptions to reduce alarms and possible false positives.
- Configure a CIDS Sensor to perform device management of supported blocking devices.
- Describe the CIDS signatures and determine the immediate threat posed to the network.
- Perform maintenance operations such as signature updates, software upgrades, data archival, and license updates.
- Describe the CIDS architecture including supporting services and configuration files.
- Manage a large scale deployment of CIDS Sensors with CIDS Management and Monitoring software.

Cisco Secure VPN (CSVPN) – 4-day Hands-on Authorized Cisco Course

Course Description

CSVPN 3.0 is a four-day, leader-led, lab-intensive course, which will be delivered by Cisco Learning Partners (CLPs). This task-oriented course teaches the knowledge and skills needed to describe, configure, verify, and manage the Cisco VPN 3000 Concentrator, Cisco VPN Software Client, and Cisco VPN 3002 Hardware Client feature set.

Course Objectives

After completing this course the student should be able to:

- Describe the features, functions, and benefits of Cisco VPN products.
- Explain the IPsec and IKE component technologies that are implemented in Cisco Secure VPN products.
- Install and configure the Cisco IPsec VPN Software client.
- Configure Cisco VPN 3000 for remote access using pre-shared keys
- Configure Cisco VPN 3000 for remote access using digital certificates
- Configure Cisco VPN 3000 firewall feature.
- Configure Cisco VPN 3002 for remote access using pre-shared keys
- Configure Cisco VPN 3002 for software auto-update.
- Configure Cisco VPN 3002 for interactive unit and individual user authentication.
- Configure Cisco VPN 3002 for backup server and load balancing.
- Configure Cisco VPN 3000 for IPsec over TCP or IPsec over UDP.
- Configure Cisco VPN 3000 for LAN-to-LAN with pre-shared keys.
- Configure Cisco VPN 3000 for LAN-to-LAN with digital certificates.

Cisco Safe Implementation (CSI) – 4-day Hands-on Authorized Cisco Course

Course Description

CSI 1.0 is a four-day, leader-led, lab-intensive course, which will be delivered by Cisco Learning Partners (CLPs). This task-oriented course teaches the knowledge and skills needed to implement and use the principles and axioms presented in the SAFE Small, Midsize and Remote User White Paper on specific devices. The primary focus is on the labs, which allow the students to build complete end-to-end security solutions using SAFE SMR as the blueprint. The following devices are covered and their configuration and functionality in a SAFE SMR network are described in detail; IOS routers, PIX Firewalls, VPN Concentrators, Cisco IDS Sensors, Cisco Host IDS, and the Cisco VPN Client

Course Objective

After completing this course the student should be able to:

- Describe the four types of security threats.
- Describe common attack methods and techniques used by hackers.
- List the general recommendations for mitigating common attack methods and techniques.
- Identify the components of a complete security policy.
- Identify the security issues implicit in common management protocols.

- Discuss the SAFE design philosophy and how it impacts the decision making process.
- List the devices that are part of Cisco's security portfolio.
- Understand the basic guidelines to use for product selection.
- Identify the functions of the key modules and key devices in a small network.
- Identify the specific threats to the small network.
- Describe the mitigation roles of Cisco's devices in a small network.
- Implement specific configurations to apply the mitigation roles in a small network.
- Recommend alternative devices that can fulfill the same mitigation roles in a small network.
- Recommend alternative devices that can fulfill the same mitigation roles in a medium network.