



Cisco CCNA Security Certification Online – IT111 90 hours

CCNA

The Cisco Certified Network Associate (CCNA) certification is Cisco's entry-level Network Installation and Support certification. CCNAs exhibit basic networking skills, and should be able to install simple LAN and WAN networks. This program provides a comprehensive introduction to deploying Cisco routers in an inter-networked environment. Through extensive hands-on exercises, students gain the fundamental knowledge and skills needed to install, configure and troubleshoot Cisco routers. A single exam must be passed to attain this certification.

Basic Networking Concepts

Overview/Description

To identify the major components of a computer system, to define basic computer and networking terminology, and to describe the benefits and functions of the OSI reference model

Target Audience

Individuals new to networking concepts and terminology; individuals preparing to take the Interconnecting Cisco Network Devices (ICND) learning path; anyone preparing for the Introduction to Cisco Networking Technologies (INTRO) exam, the Interconnecting Cisco Network Devices (ICND) exam, or the Cisco Certified Network Associate (CCNA) exam

Lesson Objectives

Basic Networking Concepts

- identify the major components of a computer system and their functionality, and list the resources required to install a NIC.
- identify the main purposes and functions of networking.
- distinguish between the OSI reference model and the TCP/IP stack.
- distinguish between basic computer and networking terms, and between the principles of the OSI reference model and the TCP/IP protocol stack.



Creating a Simple Ethernet Network

Overview/Description

To demonstrate how to build a simple Ethernet network

Target Audience

Individuals new to networking concepts and terminology; individuals preparing to take the Interconnecting Cisco Network Devices (ICND) learning path; anyone preparing for the Introduction to Cisco Networking Technologies (INTRO) exam, the Interconnecting Cisco Network Devices (ICND) exam, or the Cisco Certified Network Associate (CCNA) exam

Lesson Objectives

Creating a Simple Ethernet Network

- identify the standards, functions, and operation of important LAN technologies.
- differentiate between the different network media types.
- differentiate between the different network media types.
- determine the appropriate network media type to use in a given scenario.

Extending Ethernet Networks

Overview/Description

To describe the functions and operations of switched LANs and virtual LANs

Target Audience

Individuals new to networking concepts and terminology; individuals preparing to take the Interconnecting Cisco Network Devices (ICND) learning path; anyone preparing for the Introduction to Cisco Networking Technologies (INTRO) exam, the Interconnecting Cisco Network Devices (ICND) exam, or the Cisco Certified Network Associate (CCNA) exam

Lesson Objectives

Extending Ethernet Networks

- distinguish between the features of different network topologies.
- identify the functions, features, and operation of network devices used at different layers of the OSI model.
- match network devices to their function and distinguish between different network topologies.
- recall methods used to extend Ethernet LANs and reduce the size of collision domains.
- determine how to resolve problems with bridging loops in a switched environment, for a given scenario.



- differentiate between the features and characteristics of shared and switched LANs.
- identify the components of a VLAN and the benefits and advantages provided by VLANs.
- relate the benefits and costs of establishing a VLAN for a given scenario.

Networks with Cisco Devices

Overview/Description

To identify the basic operations of routing and to describe the operations of routing protocols, and to identify the functions of specific network layer protocols

Target Audience

Individuals new to networking concepts and terminology; individuals preparing to take the Interconnecting Cisco Network Devices (ICND) learning path; anyone preparing for the Introduction to Cisco Networking Technologies (INTRO) exam, the Interconnecting Cisco Network Devices (ICND) exam, or the Cisco Certified Network Associate (CCNA) exam

Lesson Objectives

Connecting Networks with Cisco Devices

- distinguish between different network layer protocols and their functions, and identify the fields of the IP datagram.
- differentiate between the functions of protocols used at the network layer.
- identify the basic operations involved in the routing process.
- distinguish between different routing protocol classes.
- describe the features and operations of interior and exterior routing protocols.
- distinguish between the functions and application of common interior and exterior routing protocols.**

Constructing IP Network Addresses

Overview/Description

To describe the major aspects of IP addressing and calculate valid IP subnet addresses and masks

Target Audience

Individuals new to networking concepts and terminology; individuals preparing to take the Interconnecting Cisco Network Devices (ICND) learning path; anyone preparing for the Introduction to Cisco Networking Technologies (INTRO) exam, the Interconnecting Cisco Network Devices (ICND) exam, or the Cisco Certified Network Associate (CCNA) exam

Lesson Objectives



Constructing IP Network Addresses

- distinguish between the processes used to convert between decimal, binary, and hexadecimal numbering systems.
- interpret numerical systems.
- distinguish between the types of IP address classes and between the types of reserved IP addresses.
- recognize how the use of IPv4, IPv6, and CIDR affects IP address availability.
- convert a 32-bit binary number to its corresponding IP address.
- recognize how to calculate the number of usable subnets and host addresses.
- recognize how to calculate a subnet number.
- calculate a subnet assignment.

Ensuring Data Delivery in Networks

Overview/Description

To demonstrate how to ensure the reliability of data delivery through the transport layer

Target Audience

Individuals new to networking concepts and terminology; individuals preparing to take the Interconnecting Cisco Network Devices (ICND) learning path; anyone preparing for the Introduction to Cisco Networking Technologies (INTRO) exam, the Interconnecting Cisco Network Devices (ICND) exam, or the Cisco Certified Network Associate (CCNA) exam

Lesson Objectives

Ensuring Data Delivery in Networks

- identify the functionality of common transport layer protocols and recognize the applications supported by TCP/IP.
- recognize the functionality of the TCP/IP transport layer.
- After completing this topic, you should be able to sequence the steps required to establish, maintain, and terminate a TCP connection in a TCP/IP network environment.

Remote Network Connectivity

Overview/Description

To describe the functions of major WAN technologies



Target Audience

Individuals new to networking concepts and terminology; individuals preparing to take the Interconnecting Cisco Network Devices (ICND) learning path; anyone preparing for the Introduction to Cisco Networking Technologies (INTRO) exam, the Interconnecting Cisco Network Devices (ICND) exam, or the Cisco Certified Network Associate (CCNA) exam

Lesson Objectives

Remote Network Connectivity

- recognize the functions, operation, and primary components of a WAN.
- identify the features and functions of major WAN technologies.
- determine the WAN connection types and multiplexing used in a given scenario.
- recognize the structure and functionality of the Internet.
- identify the characteristics and functions of the PPP and HDLC protocols.
- identify the function and operation of ISDN, DSL, Frame Relay, ATM, and SONET connection technologies.
- identify the function and operation of analog modems and cable modems.
- determine the appropriate connection medium to use when connecting a WAN in a given scenario.
- distinguish between the functions, operations, and primary components of a MAN, SAN, CN, and VPN.
- match an appropriate WAN connection technology and modem to a corporate network, for a given scenario.

Operation and Configuration of Cisco IOS Switches

Overview/Description

To use the available configuration tools to establish connectivity to the appropriate network device in order to complete initial switch configurations and to verify the default configuration and status of switch devices

Target Audience

Individuals new to networking concepts and terminology; individuals preparing to take the Interconnecting Cisco Network Devices (ICND) learning path; anyone preparing for the Introduction to Cisco Networking Technologies (INTRO) exam, the Interconnecting Cisco Network Devices (ICND) exam, or the Cisco Certified Network Associate (CCNA) exam

Lesson Objectives

Operation and Configuration of Cisco IOS Switches

- recognize the setup of console connections for Cisco devices.
- identify the requirements for configuring a Cisco network device from an external source.



- start a Cisco IOS EXEC session and change EXEC modes.
- recognize the LED sequence that verifies successful POST completion for a Catalyst switch.
- interpret initial boot-up output and use the CLI help facilities on a Catalyst switch.
- use the command line interface to configure basic switch details, and to examine the status and configuration of the switch.
- implement the initial configuration for a Catalyst 2950 switch.

Operation and Configuration of Cisco IOS Routers

Overview/Description

To use available configuration tools to establish connectivity to a router in order to complete the initial router configuration and to verify the default configuration and status of a functioning access-layer router

Target Audience

Individuals new to networking concepts and terminology; individuals preparing to take the Interconnecting Cisco Network Devices (ICND) learning path; anyone preparing for the Introduction to Cisco Networking Technologies (INTRO) exam, the Interconnecting Cisco Network Devices (ICND) exam, or the Cisco Certified Network Associate (CCNA) exam

Operation and Configuration of Cisco IOS Routers

- recognize the router startup sequence and the initial router setup.
- recognize the keyboard help, enhanced editing key functions, and command history feature associated with the command line interface.
- use the router command line interface to locate and complete commands, correct command line errors, and observe and verify the status of a router.
- identify the router status commands used to verify initial startup of a router.
- verify the initial router startup sequence and configuration process.
- identify the different router configuration modes and their functions.
- configure basic router features and interfaces.
- implement a basic router configuration.
- modify the configuration files to configure a router in a given scenario.

Managing the Cisco Network Environment

Overview/Description

To discover and determine the status of connected devices on a network and enable connections to these devices

Target Audience

Individuals new to networking concepts and terminology; individuals preparing to take the Interconnecting Cisco Network Devices (ICND) learning path; anyone preparing for the Introduction to Cisco Networking Technologies (INTRO) exam, the Interconnecting Cisco Network Devices (ICND) exam, or the Cisco Certified Network Associate (CCNA) exam



Lesson Objectives

Managing the Cisco Network Environment

- use CDP to determine the host names and addresses of neighboring Cisco devices, and recognize how to create a network map of the environment.
- use CDP to determine the host names and addresses of neighboring Cisco devices and create a map of the network environment, given operational access-layer switches and routers.
- identify how to connect to a remote device using Telnet.
- use CDP and Telnet to collect information from network devices.
- use IOS commands to manage Telnet sessions.

Cisco Network Device Administration

Overview/Description

To manage devices on a network according to designated best practices

Target Audience

Individuals new to networking concepts and terminology; individuals preparing to take the Interconnecting Cisco Network Devices (ICND) learning path; anyone preparing for the Introduction to Cisco Networking Technologies (INTRO) exam, the Interconnecting Cisco Network Devices (ICND) exam, or the Cisco Certified Network Associate (CCNA) exam

Cisco Network Device Administration

- use Cisco IOS commands to manage device configuration files.
- manage Cisco IOS image files and device configuration files.
- implement the correct methods for managing device configurations.
- recognize how to execute adds, moves, and changes on a router, and troubleshoot operational Cisco devices.
- execute adds, moves, or changes on a router, and use the debug troubleshooting tool to minimize potentially adverse impacts on Cisco devices.

Configuring Cisco Catalyst Switch Operations

Overview/Description

To discuss and implement specific bridging and VLAN Catalyst switch configurations, which provide for scalability, security, and enhanced management of the local area switched network



Target Audience

Network administrators responsible for implementing and managing small and medium-sized business networks; network technicians who install network devices in small business environments; Cisco channel resellers who are new to Cisco products and services

Lesson Objectives

Configuring Cisco Catalyst Switch Operations

- explain the fundamentals of layer 2 switching.
- describe redundant topologies in switched environments.
- describe how the spanning-tree algorithm is used to eliminate switching loops.
- describe how the Spanning-Tree and Rapid Spanning-Tree Protocols affect frame forwarding on bridges and switch ports.

- discuss Spanning-Tree Protocol operation.
- describe how to configure ports on a switch.
- configure port security, add, move, and change MAC addresses and manage device configuration files.
- explain how to implement port and MAC security on a switch.
- configure a Catalyst 2950 series switch.
- describe the operation of VLANs.
- explain how VTP is used to manage VLANs.
- determine the appropriate commands used in VLAN configuration and trunking.
- scale the size and number of VLANs and troubleshoot their operation.
- verify VLAN configuration on a switch.

Routing in Cisco Networks

Overview/Description

To describe the different forms of routing and explain the concepts of distance vector and link state routing

Target Audience

Network administrators responsible for implementing and managing small and medium-sized business networks; network technicians who install network devices in small business environments; Cisco channel resellers who are new to Cisco products and services

Lesson Objectives

Routing in Cisco Networks

- outline the basic principles of routing.
- distinguish the features and operation of dynamic routing protocols.



- discuss the operation and method used for routing between VLANs and choose the commands used to configure trunking modes.
- analyze the operation of distance vector routing protocols.
- explain the mechanisms used to eliminate routing loops.
- describe the features and operation of link state and balanced hybrid routing protocols.
- use IOS software commands to discover routing protocols supported and in use on a router.

Implementing Routing Protocols on Cisco Networks

Overview/Description

To describe the operation and configuration of popular modern routing protocols

Target Audience

Network administrators responsible for implementing and managing small and medium-sized business networks; network technicians who install network devices in small business environments; Cisco channel resellers who are new to Cisco products and services

Lesson Objectives

Implementing Routing Protocols on Cisco Networks

- enable RIP on a router.
- configure and verify RIP operation on Cisco routers.

- explain the operation of IGRP.
- describe how to enable IGRP on a router.
- configure IGRP on a router.
- distinguish the various features and functions of EIGRP.
- describe the commands used to configure EIGRP.
- verify EIGRP configuration on routers.
- identify the features of OSPF and how they compare to distance vector routing protocols.
- describe the commands used to configure OSPF in a single area.
- configure and verify configuration of OSPF.
- explain the operation of variable-length subnet masks (VLSM) on Cisco routers.

Managing IP Traffic on Cisco Networks

Overview/Description

To describe and configure efficient network traffic restrictions and security using properly implemented access list management and address translation



Target Audience

Network administrators responsible for implementing and managing small and medium-sized business networks; network technicians who install network devices in small business environments; Cisco channel resellers who are new to Cisco products and services

Lesson Objectives

Managing IP Traffic on Cisco Networks

- explain the requirement for access lists.
- describe access list operation and configuration.
- describe how access lists filter by protocols and packet details.
- explain how wildcards are used in access list configuration.
- explain the rules governing access list configuration.
- demonstrate how to control network access using access control lists.
- implement and manage standard access lists using IOS commands.
- describe extended access lists, and explain how to configure them and determine their effectiveness.
- implement and manage standard access control lists (ACL) using IOS commands.
- explain the ideal implementation of access lists.
- describe the features and operation of Network Address Translation (NAT) and Port Address Translation (PAT).
- describe the commands used to configure address translation and overloading.
- verify and troubleshoot NAT and PAT configurations.

Extending a Cisco Network to a WAN

Overview/Description

To describe the implementation and configuration of the different technologies used on Cisco devices to enable wide area connections

Target Audience

Network administrators responsible for implementing and managing small and medium-sized business networks; network technicians who install network devices in small business environments; Cisco channel resellers who are new to Cisco products and services

Lesson Objectives

Extending a Cisco Network to a WAN

- discuss the elements of a wide-area network.
- describe the protocols used for WAN connectivity and how devices are connected to the network.
- detail HDLC and PPP protocol operation.



- detail the authentication and encapsulation processes used by PPP.
- configure PPP on a Cisco device interface.
- describe the terminology of Frame Relay and how it operates.
- describe the purpose and command syntax for defining static Frame Relay map entries on a router.
- configure Frame Relay subinterfaces on a router.
- discuss the typical types of Frame Relay connections made to service providers.
- configure a subinterface on a Cisco router.
- configure a Frame Relay connection.

Completing ISDN Calls on Cisco Networks

Overview/Description

To detail the operation and configuration of ISDN and DDR

Target Audience

Network administrators responsible for implementing and managing small and medium-sized business networks; network technicians who install network devices in small business environments; Cisco channel resellers who are new to Cisco products and services

Lesson Objectives

Completing ISDN Calls on Cisco Networks

- describe the characteristics of ISDN.
- detail the functional elements of ISDN and describe the commands used to configure BRI and PRI interfaces.
- identify the different ISDN switch types and configure basic ISDN.
- configure ISDN PRI on a router.
- discuss the commands used to verify and troubleshoot ISDN connections.
- explain how DDR operates.
- detail the steps for configuring DDR.
- describe the configuration of dialer profiles on ISDN interfaces.
- configure and troubleshoot a given ISDN DDR connection.
- use context sensitive help and set up IP static routes.

TestPrep 640-801 Cisco Certified Network Associate (CCNA)

Overview/Description

Generally taken near the end of a program of certification-orientated study, the 640-801 Cisco Certified Network Associate (CCNA) TestPrep enables the learner to test their knowledge in a simulated certification testing environment. Learners can take TestPrep in two different modes:

Study and Certification. Study mode is designed to maximize learning by providing feedback, while Certification mode is designed to mimic a certification exam.



Target Audience

Individuals seeking practice in a simulated testing environment, covering the skills and competencies being measured by the actual certification exam.

Lesson Objectives

TestPrep 640-801 Cisco Certified Network Associate (CCNA)

- Introduction to Networking
- Network Types
- Network Media
- Switching Fundamentals
- TCP/IP
- IP Addressing and Routing
- WAN Technologies
- Operating and Configuring Cisco IOS Devices
- Managing Your Network Environment
- Configuring Catalyst Switch Operations
- Extending Switched Networks with VLANs
- Determining IP Routes
- Managing IP Traffic with Access Lists
- Establishing Serial Point-to-Point Connections
- Establishing Frame Relay Connections
- Completing ISDN Calls

Cisco IINS 1.0: Network Security Principles I

Overview/Description

The open nature of the Internet makes it increasingly important for growing businesses to pay attention to the security of their networks. As companies move more of their business functions to the public network, they need to take precautions to ensure that their data remains uncompromised. With the challenges of increased availability requirements and growing regulatory requirements, establishing and maintaining a secure network computing environment is becoming increasingly difficult.

This course provides an explanation of the core principles that are part of the secure network environment. It explains how sophisticated attack tools and open networks generate an increased need for network security and dynamic security policies, the primary objectives of security and primary types of security controls, as well as some of the factors that are involved in responding to a security breach. Examining who hackers are, what motivates them, and how they do what they do, as well as variety of attacks against confidentiality, integrity, and availability and some of the best practices to defeat them are also covered. This course is one of a series from the IINS 1.0 SkillSoft learning paths which cover the objectives for Cisco exam 640-553 IINS 1.0.



Target Audience

Network designers, administrators, engineers, and managers; systems engineers; individuals seeking the Implementing Cisco IOS Network Security (IINS) v1.0 640-553 certification

Prerequisites

Knowledge and skills equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1); a working knowledge of the Windows operating system and Cisco IOS networking and concepts

Expected Duration - 2.0 hours

Lesson Objectives:

Combating Threats to Security

- Recognize why there's an increased need for network security and dynamic security policies
- Recognize the three primary objectives of security

Data Classification and Security Controls

- Recognize how data is classified
- Recognize the primary types of security controls

Security breaches, laws, and ethics

- Recognize the factors involved in responding to a security breach
- Recognize key codes of ethics that are binding to INFOSEC professionals

Adversaries, Motivations, and Classes of Attack

- Recognize the motivations of different types of hackers
- Recognize typical attacks that hackers use

Defense in Depth

- Recognize the principles of defense in depth

IP Spoofing Attacks

- Recognize how attackers use IP spoofing to launch various types of attacks

Confidentiality Attacks

- Recognize how attackers can compromise confidentiality

Integrity Attacks

- Recognize the methods that attackers can use to compromise integrity

Availability Attacks

- Recognize how attackers can compromise availability

Responding to a Security Breach

Course ID: cc_iins_a01_it_enus

Cisco IINS 1.0: Network Security Principles II



Overview/Description

Operations security concerns the day-to-day practices necessary to first deploy and later maintain a secure system. As an administrator, it's very important to understand the principles behind operations security. It's equally important to know that the security policy that's developed in your organization drives all of the steps taken to secure network resources. In order to create an effective security policy, it is necessary to do a risk analysis in order to maximize the effectiveness of the policy. Also, it is essential that everyone is aware of the policy, or it is doomed to fail. This course explains the principles behind operations security and how correct practices increase security, including security testing, a secure life cycle, and business continuity planning. In addition, it reviews how increasing network security threats demand comprehensive network security policies, and describes the main activities in each phase of a secure network life cycle. Implementing the Cisco Self-Defending Network strategy by enhancing the existing network infrastructure with Cisco technologies, products, and solutions is also covered. This course is one of a series from the IINS 1.0 SkillSoft learning paths which cover the objectives for Cisco exam 640-553 IINS 1.0.

Target Audience

Network designers, administrators, engineers, and managers; systems engineers; individuals seeking the Implementing Cisco IOS Network Security (IINS) v1.0 640-553 certification

Prerequisites

Knowledge and skills equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1); a working knowledge of the Windows operating system and Cisco IOS networking and concepts

Expected Duration - 2.0 hours

Lesson Objectives:

Operations Security Principles

- Recognize how to use SDLC to design a secure network life cycle management process
- Identify key operations security principles

Security Testing and Disaster Recovery

- Recognize how network security testing works
- Recognize the principles of disaster recovery planning

Security Policy Overview

- Recognize the function of a security policy
- Recognize the functions and characteristics of security standards, guidelines, and procedures

Risk Management

- Recognize the role that risk management plays in the development of a security policy



Principles of Secure Network Design

- Recognize the principles of secure network design

Security Awareness

- Recognize how security awareness, education, and training can help to increase the effectiveness of a security policy

Threats and Challenges

- Recognize how changing threats and challenges demand a new approach to network security

The Cisco Self-Defending Network

- Recognize the benefits of a Cisco Self-Defending Network
- Recognize the solution components of a Cisco Self-Defending Network

Implementing Network Security Principles

Course ID: cc_iins_a02_it_enus

Cisco IINS 1.0: Perimeter Security

Overview/Description

Traffic from outside a closed network that has a destination inside a closed network passes through the network perimeter. The routers at the network perimeter are an important initial point of network security. This course explains how to use the CLI to configure routers on the network perimeter with Cisco IOS Software security features, including securing the physical installation of and administrative access to Cisco routers based on different network requirements. It explores the features and uses of SDM, and how to configure a Cisco router to perform AAA authentication with a local database using the Cisco SDM. This course also covers the operation of external AAA sources such as RADIUS and TACACS+ servers, how to configure a Cisco router to perform AAA, and how to securely implement the management and reporting features of syslog, SNMP, SSH, and NTP. This course is one of a series from the IINS 1.0 SkillSoft learning paths which cover the objectives for Cisco exam 640-553 IINS 1.0.

Target Audience

Network designers, administrators, engineers, and managers; systems engineers; individuals seeking the Implementing Cisco IOS Network Security (IINS) v1.0 640-553 certification

Prerequisites

Knowledge and skills equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1); a working knowledge of the Windows operating system and Cisco IOS networking and concepts



Expected Duration - 1.5 hours

Lesson Objectives:

Router Security Features

- Recognize the security features of the Cisco IOS Software
- Recognize the features of the Cisco Integrated Services Routers

Configuring Secure Administrative Access

- Recognize how to configure secure administrative access

Multiple Privilege Levels and Role-Based CLI Access

- Recognize how to configure multiple privilege levels
- Recognize how to configure role-based CLI access

Image Files, Virtual Logins, and Banner Messages

- Recognize how to configure the Cisco IOS Resilient Configuration feature, virtual login connection security, and a banner message

Securing Cisco Router Administrative Access

Introducing Cisco SDM

- Recognize the features of Cisco SDM
- Recognize how to configure existing routers so that Cisco SDM can access them properly

Configuring AAA on a Cisco Router

- Recognize how to use local services to authenticate router access
- Recognize how to configure a Cisco router to perform AAA using a local database for authentication

Course ID: cc_iins_a03_it_enus

Cisco IINS 1.0: Network Security Using Cisco IOS Firewalls

Overview/Description

Implementing network-wide security can be a daunting task depending on the size and business of the company. Organizations must balance the cost in staff

and equipment to implement a network security policy against the potential costs of network security breaches. Cisco provides several router-based solutions for implementing firewall features: basic traffic filtering capabilities using access control lists (ACLs), Cisco IOS Firewalls, and Cisco IOS zone-based policy firewalls. This course explains the operations of the different types of firewall technologies and describes the firewall technologies that are embedded in Cisco routers and Cisco security appliances. The processes of creating static packet filters using ACLs, and configuring a Cisco IOS zone-based policy firewall on your network using the Cisco SDM wizard are also covered. This course is one of a series from the IINS 1.0 SkillSoft learning paths which cover the objectives for Cisco exam 640-553 IINS 1.0.



Target Audience

Network designers, administrators, engineers, and managers; systems engineers; individuals seeking the Implementing Cisco IOS Network Security (IINS) v1.0 640-553 certification

Prerequisites

Knowledge and skills equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1); a working knowledge of the Windows operating system and Cisco IOS networking and concepts

Expected Duration - 2.5 hours

Lesson Objectives:

Firewall Fundamentals

- Recognize the role of firewalls in securing networks
- Recognize how a static packet filter allows or blocks data packets as they pass through a network interface

Application Layer Gateways

- Recognize how application layer or proxy firewalls control or monitor inbound and outbound traffic

Firewall Types and Features

- Recognize how dynamic or stateful inspection packet filtering provides improved network security and performance
- Recognize how application inspection firewalls, transparent firewalls, and Cisco IOS firewalls function

Access Control List Fundamentals

- Recognize how ACLs are used to control access in networks

ACL Wildcard Masking and Traffic Control

- recognize how to use wildcard masks with ACLs
- recognize how to configure ACLs to control traffic using a variety of protocols

ACL Considerations

- Recognize the considerations for creating ACLs

Security Device Manager ACL Configuration

- Recognize how to configure standard and extended ACLs using Cisco SDM
- Recognize how to configure ACLs to protect common network services

Creating Static Packet Filters Using ACLs

Zone-Based Policy Firewalls Basics

- Recognize the principles of Zone-Based Policy Firewalls
- Recognize how to configure a Zone-Based Policy Firewall using the Cisco SDM Basic Firewall Configuration Wizard

Configuring and Verifying Zone-Based Firewalls

- Recognize how to use the Cisco SDM to manually configure a Zone-Based Policy Firewall

Course ID: cc_iins_a04_it_enus



Cisco IINS 1.0: Cryptography, Encryption, and Digital Signatures

Overview/Description

Cryptographic services form the foundation for many security implementations and provide both confidentiality and integrity of data when that data might be exposed to untrusted parties. Understanding the basic functions of cryptography

and how encryption and hashing provide confidentiality and integrity help in the creation of a successful security policy. It is also important to have a good understanding of the issues involved in key management. Cryptographic hashes and digital signatures play a major role in modern cryptosystems, and it is important to have a good understanding of the basic mechanisms of these algorithms and some of the issues that are involved in choosing a particular hashing algorithm or digital signature method. This course provides a primer on the theory of cryptography. It discusses the principles behind symmetric encryption, provides examples of major symmetric encryption algorithms, and examines their operations, strengths, and weaknesses. This course also touches on the major hashing algorithms that use Hashed Message Authentication Code (HMAC), and the digital signature technologies that are widely used in modern computing and networking. It also describes some of the real-world implications of using various algorithms and technologies. The principles behind asymmetric encryption and provides examples of major asymmetric encryption algorithms, including Rivest, Shamir, and Adleman (RSA); Diffie-Hellman (DH); and public key infrastructure (PKI) are also covered. This course is one of a series from the IINS 1.0 SkillSoft learning paths which cover the objectives for Cisco exam 640-553 IINS 1.0.

Target Audience

Network designers, administrators, engineers, and managers; systems engineers; individuals seeking the Implementing Cisco IOS Network Security (IINS) v1.0 640-553 certification

Prerequisites

Knowledge and skills equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1); a working knowledge of the Windows operating system and Cisco IOS networking and concepts

Expected Duration - 2.5 hours

Lesson Objectives

Cryptology and Encryption Basics

- Recognize how cryptography works
- Recognize how cryptanalysis works

Algorithms, Ciphers, and Hashes

- Recognize how symmetric and asymmetric encryption algorithms function
- Recognize the differences between and benefits of the basic encryption algorithms



Key Management and SSL VPNs

- Recognize the considerations of key management
- Recognize how SSL VPNs work

Examining Symmetric Encryption

- Recognize the features of symmetric encryption

Hash Algorithms

- Recognize how hash algorithms and the HMAC variant function

MD-5, SHA-1, and Digital Signatures

- Recognize the features of the MD5 and SHA-1 algorithms
- Recognize the features of digital signatures

Asymmetric Encryption Algorithms

- Recognize the generic functionality of asymmetric encryption algorithms
- Recognize the features of the RSA and DH key exchange algorithms

PKI

- Recognize how PKI algorithms function
- Recognize PKI standards

Certificate Authorities

- Recognize the role of CAs in a PKI

Comparing Encryption Methods

Course ID: cc_iins_a05_it_enus

Cisco IINS 1.0: IP Security Site-to-Site Virtual Private Networks

Overview/Description

An IPsec VPN uses the Internet to connect branch offices, remote employees, and business partners to your company's resources. It is a reliable way to maintain your company privacy while streamlining operations, reducing costs, and allowing flexible network administration.

This course explains the fundamental VPN-related concepts and technologies, and describes how to configure an IPsec site-to-site VPN tunnel using both the command-line interface (CLI) and the Cisco Router and Security Device Manager (SDM). This course is one of a series from the IINS 1.0 SkillSoft learning paths which cover the objectives for Cisco exam 640-553 IINS 1.0.

Target Audience

Network designers, administrators, engineers, and managers; systems engineers; individuals seeking the Implementing Cisco IOS Network Security (IINS) v1.0 640-553 certification

Prerequisites

Knowledge and skills equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1); a working knowledge of the Windows operating system and Cisco IOS networking and concepts



Expected Duration - 1.5 hours

Lesson Objectives

VPN Fundamentals

- Recognize the features of Cisco VPNs

IPsec Concepts and Framework

- Recognize the advantages IPsec has over SSL
- Recognize how encryption, integrity, and authentication are applied to the IPsec protocol suite

Internet Key Exchange Protocols

- Recognize how the IKE protocol works

Configuring Site-to-Site IPsec VPNs I

- Recognize how to configure a site-to-site IPsec VPN by configuring the interface ACL
- Recognize how to configure a site-to-site IPsec VPN by creating an ISAKMP policy
- Recognize how to configure a site-to-site IPsec VPN by defining the IPsec transform set

Configuring Site-to-Site IPsec VPNs II

- Recognize how to configure a site-to-site IPsec VPN by creating a crypto ACL
- Recognize how to configure a site-to-site IPsec VPN by creating and applying a crypto map

IPsec Site-to-Site VPN Using Cisco SDM

- Recognize how to configure a site-to-site IPsec VPN with PSK authentication using Cisco SDM

Configuring a Site-to-Site IPsec VPN

Course ID: cc_iins_a06_it_enus

Cisco IINS 1.0: Network Security Using Cisco IOS IPS

Overview/Description

In technological environments, Internet worms and viruses can spread across the world in a matter of minutes. Without the luxury of time to react, a network needs to be able to instantaneously recognize and mitigate worm and virus threats. A networking architecture paradigm shift is required to defend against these fast-moving attacks. It's no longer possible to contain the intrusions at a few points in the network. Intrusion prevention is required throughout the entire network to detect and stop an attack at every ingress and egress point in the network. The most scalable and cost-effective way to accomplish this is by integrating intrusion prevention systems (IPSs) into the access points of the network. This course provides the knowledge and skills required to configure IPSs on Cisco routers.

This course is one of a series from the IINS 1.0 SkillSoft learning paths, which cover the objectives for Cisco exam 640-553 IINS 1.0.



Target Audience

Network designers, administrators, engineers, and managers; systems engineers; individuals seeking the Implementing Cisco IOS Network Security (IINS) v1.0 640-553 certification

Prerequisites

Knowledge and skills equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1); a working knowledge of the Windows operating system and Cisco IOS networking and concepts

Expected Duration - 1.5 hours

Lesson Objectives

Intrusion Prevention System Overview

- Recognize the differences between and similarities of IDS and IPS
- Recognize how IPS may respond to an attack

Intrusion Prevention System Management

- Recognize the role of IPS event monitoring and management
- Recognize how host-based and network-based IPS monitoring operate

Intrusion Prevention System Solutions

- Recognize the features of Cisco IPS appliances
- Recognize how an IDS or IPS can use signatures

Cisco IOS IPS Features and Configuration

- Recognize the IPS features of Cisco IOS Software
- Recognize how to configure Cisco IOS IPS using Cisco SDM

Tuning, Monitoring, & Verifying Cisco IOS IPS

- Recognize how to configure IPS signatures using Cisco SDM
- Recognize how to monitor a Cisco IOS IPS router using Cisco SDM and the CLI

Configuring Cisco IOS IPS

Course ID: cc_iins_a07_it_enus

Cisco IINS 1.0: LAN, SAN, Voice, and Endpoint Security

Overview/Description

It is important to have a good understanding of the additional aspects of network security, such as LAN, storage area network (SAN), voice, and endpoints. An understanding of how to place emphasis on Layer 2 and host security to provide a much more comprehensive coverage of the important issues involved in securing an enterprise is also crucial. This course explains how to configure LAN devices to control access, resist attacks, shield other network devices and systems, and protect the integrity and confidentiality of network traffic. This course also provides an overview of the basic principles of SANs and SAN security. The implications of implementing security measures in IP networks that transport voice are also covered. This course is one of a



series from the IINS 1.0 SkillSoft learning paths which cover the objectives for Cisco exam 640-553 IINS 1.0.

Target Audience

Network designers, administrators, engineers, and managers; systems engineers; individuals seeking the Implementing Cisco IOS Network Security (IINS) v1.0 640-553 certification

Prerequisites

Knowledge and skills equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1); a working knowledge of the Windows operating system and Cisco IOS networking and concepts

Expected Duration - 2.0 hours

Lesson Objectives

Endpoint Security Fundamentals

- Recognize how endpoint security works
- Recognize how buffer overflows present a threat

IronPort and Cisco NAC Security Products

- Recognize the features of IronPort security products
- Recognize how the Cisco NAC products enhance and complement endpoint security

Cisco Security Agent

- Recognize how Cisco Security Agent provides endpoint security

SAN Security

- Recognize the basic principles of SANs
- Recognize security strategies you can use to compartmentalize data for security purposes

VoIP Fundamentals and Threats

- Recognize fundamental VoIP concepts
- Recognize security threats to VoIP networks

IP Telephony Risks

- Recognize the security risks that voice-enabled networks face
- Recognize how to prevent hacking on VoIP networks

Defending Against Endpoint Attacks

Course ID: cc_iins_a08_it_enus



Cisco IINS 1.0: Mitigating Layer 2 Attacks

Overview/Description

Like routers, both Layer 2 and Layer 3 switches have their own set of network security requirements. Access to switches is a convenient entry point for attackers who are intent on illegally gaining access to a corporate network. With access to a switch, an attacker can set up rogue access points and protocol analyzers, and launch all types of attacks from within the network. Attackers can even spoof the MAC and IP addresses of critical servers to do a great deal of damage. This course examines various Layer 2 attacks and strategies to mitigate them. This course is one of a series from the IINS 1.0 SkillSoft learning paths which cover the objectives for Cisco exam 640-553 IINS 1.0.

Target Audience

Network designers, administrators, engineers, and managers; systems engineers; individuals seeking the Implementing Cisco IOS Network Security (IINS) v1.0 640-553 certification

Prerequisites

Knowledge and skills equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1); working knowledge of the Windows Operating System; working knowledge of Cisco IOS networking and concepts.

Expected Duration - 1.0 hours

Lesson Objectives

Layer 2 Vulnerabilities and VLAN Attacks

- Recognize how to mitigate VLAN attacks

Types of Layer 2 Attacks

- Recognize how to prevent STP manipulation
- Recognize how to mitigate STP vulnerabilities

Using Port Security

- Recognize how to use port security to defend networks from Layer 2 attacks

Switch Security Features and Best Practices

- Recognize features available in Cisco switch security

Using Cisco Catalyst Switch Security Features

Course ID: cc_iins_a09_it_enus

Mentoring 640-553 Implementing Cisco IOS Network Security (IINS)

Overview/Description

SkillSoft Mentors are available to help students with their studies for exam 640-553 Implementing Cisco IOS Network Security (IINS). You can reach them by entering a Mentored Chat Room or by using the E-mail My Mentor service.



Target Audience

Individuals who are studying the associated SkillSoft content in preparation for, or to become familiar with, the skills and competencies being measured by the actual certification exam.

Objectives

Mentoring 640-553 Implementing Cisco IOS Network Security (IINS)

- Describe the security threats facing modern network infrastructures
- Secure Cisco routers
- Implement AAA on Cisco routers using local router database and external ACS
- Mitigate threats to Cisco routers and networks using ACLs
- Implement secure network management and reporting
- Mitigate common Layer 2 attacks
- Implement the Cisco IOS firewall feature set using SDM
- Implement the Cisco IOS IPS feature set using SDM
- Implement site-to-site VPNs on Cisco Routers using SDM

Course ID: mnt640553