



COURSE SYLLABUS

Cisco Certified Network Professionals

CCNP ISCW (Exam 642-825)



50 Cragwood Rd, Suite 350
South Plainfield, NJ 07080

Victoria Commons, 613 Hope Rd Building #5,
Eatontown, NJ 07724

130 Clinton Rd,
Fairfield, NJ 07004

Avtech Institute of Technology Course

Instructor:

Course Duration:

Date/Time:

Training Location:

Course Description

This course is designed to help the students get to the point that who can pass the **CCNP ISCW Exam 642-825** based on the skills, knowledge, and experience already have obtained, with the least amount of time required. Also, it makes students much more knowledgeable about how to do the job.

The teaching material and method help the students to pass the ISCW exam:

- Helps the students discover which test topics have not master
- Provides explanations and information to fill in the knowledge gaps
- Supplies exercises and scenarios that enhance the ability to recall and deduce the answer to test questions
- Provide practice exercises on the topics and the testing process via test questions

Learning Objectives

Part1: Remote Connectivity Best Practices

1.0 The requirements in a Converged Network

- 1.1. Describes four technological architecture for SONA (Service-Oriented Network Architecture), Service Provider Architecture (IP Next-Generation-Networks or IP-NGN), Commercial Architecture and Consumer Architecture
- 1.2. Explains the Cisco vision of the Intelligent Information Network (IIN) composition features: Network resource and information asset integration into the network, Cross-platform/cross-product intelligence spanning all layers of infrastructure, a network that actively participates in the delivery of services and applications. Also, describes Three essential phases of the IIN offers: Integrated transport phase, Integrated service phase, and Integrated applications phase
- 1.3. Discuss the Cisco Network Models: Cisco Hierarchical Network Model, Campus Network Architecture, Branch Network Architecture, Data Center Architecture, Enterprise Edge Architecture, Tele-worker Architecture, and WAN/MAN Architecture. The Remote Evaluate factors and details necessary to effectively design and deploy the Remote Connection Requirements in a Converged Network to a Central Site, Branch Office, SOHO Site, and the Integrated Services for Secure Remote Access also discussed.

2.0 The connection access methodology and topologies for Remote-Teleworker

- 2.1. Describes how to facilitate remote connections that an enterprise network has to support; which including IIN and the Teleworker, Enterprise Architecture Framework, Remote Connection Options. Lists connection types and bandwidths typically available (DSL, Cable, and Fiber Optic)
- 2.2. The Challenges faces in connecting teleworker to the enterprise network, and the solutions that exist to address these challenges; which including the connection speeds and technologies available of Infrastructure Options (Remote-access VPN and IPsec VPN) and Services, Teleworker Components, and Traditional Teleworker versus Business-Ready Teleworker

3.0 Using the Cable Access Technologies to Connect to a Central Site

- 3.1. Defines basic terminology and standards (NTSC, PAL, and SECAM) relevant to cable technology, the components (Antenna site, Headend, Transportation network, Distribution network, and Subscriber drop) of a cable system that provide data services, and features of cable technology
- 3.2. Describes digital cable use of radio frequency bands for signal transmission, including the specification of DOCSIS (Data-Over-Cable Service Interface Specifications), and how it provides the data service interface standard for data carried over RF interfaces and dictates the process by which CMs are provisioned
- 3.3. Describes how data over cable services can be delivered using an HFC architecture, including Hybrid Fiber-Coaxial (HFC) Networks, Data Transmission
- 3.4. Describes the combination of technologies necessary for cable systems to function, and cable Technology Issues
- 3.5. Describes the cable provision process in a customer network; including the operational provision servers such as DHCP and TFTP of headend CMT (Cable Modem Termination Systems), the steps defined by DOCSIS also discussed

4.0 Deploying DSL (Digital Subscriber Line) technology to Connect to a Central Site

- 4.1. Describe the features POTS Coexistence, the terminology used in dealing with DSL, the distance limitations of DSL technology (ADSL, VDSL, IDSL, SDSL, and G.SHDSL), and the various implementation of DSL (DSL Variants) , including symmetric DSL (SDSL) and asymmetric DSL(ASDL) types
- 4.2. Describes the basics of ADSL technology and ADSL modulation technology; including Carrier-less Amplitude Phase (CAP) and Discrete Multi-Tone (DMT), and data transmission over ADSL; including RFC 1483/2684 Bridging and PPP Background
- 4.3. Describes the architecture and deployment models of PPPoE (PPP over Ethernet); Including Discovery Phase and PPP Session Phase, and Optimizing PPPoE MTU. The architecture and deployment models of PPPoA (PPP over ATM) also discussed

5.0 Configuring DSL Access with PPPoE

- 5.1. Describes the steps for Configure a Cisco Router as a PPPoE (Point-to-Point Protocol over ATM) Client Connectivity, the information required for Configuring an Ethernet/ATM (Asynchronous Transfer Mode) Interface for PPPoE, the Configuring of the PPPoE DSL Dialer Interface and Virtual Template Interface, the PPPoE

Configuration Elements , such as Ethernet interface, ATM interface, Dialer interface, NAT/PAT, Inside local address, Inside global address, Outside local address, Outside global address, DHCP server, and static default route also provided

- 5.2. Configuring NAT (Network Address Translation) /PAT (Port Address Translation), Have an understanding of Inside/outside local address and global address
- 5.3. Configuring DHCP (Dynamic Host Configuration Protocol) for DSL Router Users, Configuring Static default route with PPPoE and the Overall CPE Router Configuration

6.0 Configuring DSL Access with PPPoA

- 6.1. Describe the requirement of configuring a Cisco Router as a PPPoA Client, which including PPP over AAL5 Connections and LLC Encapsulated PPP over AAL5, and Cisco PPPoA
- 6.2. Describe the tasks involved in configuring a ATM Interface for PPPoA Connection, giving the examples of Subscriber-Facing Ethernet Interface Configuration, AAL5MUX Configuration, and AAL5SNAP configuration
- 6.3. Configure the PPPoA DSL Dialer and Virtual Template Interfaces, the commands for the configuration and the examples also provided
- 6.4. Configure Additional PPPoA Elements and the Overall CPE Router Configuration are provided

7.0 Verifying and Troubleshooting ADSL Configurations

- 7.1. Describes basic DSL troubleshooting principles: the OSI reference model “bottom up” troubleshooting (Network layer, Datalink layer, and Physical layer), the troubleshooting debug commands also introduced
- 7.2. Isolating Physical Layer Issues; including the topics of Layer 1 Anatomy, ADSL Physical Connectivity, Playing with Colors, Tangled Wires, Keeping the Head on Straight, DSL Operating Mode
- 7.3. Isolating Data Link Layer Issues, the examples to reveal PPP Negotiation also giving

Part II: Implementing Frame Mode MPLS

8.0 Implementing Frame Mode MPLS (Multiprotocol Label Switching architecture) Network

- 8.1. Introducing MPLS Networks; Introducing the terminology and features of Traditional WAN Connections, MPLS WAN Connectivity
- 8.2. Cisco IOS Router Switching Mechanisms (Planes and Information Bases), discuss the IS switching mechanisms first (Process switching, Cache-driven switching, and Topology-driven switching), then Standard IP Switching and configuring CEF (Cisco Express Forwarding) and MPLS on a Frame Mode Interface

9.0 MPLS Architecture

- 9.1. Covers the most of the terminology involved with MPLS (Multiprotocol Label Switching) , the two basic underlying architecture components as Control plane and Data Plane of MPLS mechanisms also described

- 9.2. Describe label format and use: The concept of the manner; that Frame Headers, labels, Layer 3 Protocol, and Payload involved in Label Stacking, and Frame Mode MPLS also covered
- 9.3. Describe the role of LSRs (Label Switching Routers) in an MPLS network. The MPLS Information Bases-Label Allocation in Frame Mode MPLS Network, including LIB (Label Information Bases), LFIB (Label Forwarding Information Bases) and FIB (Forwarding Information Bases) also explained, and some examples are provided
- 9.4. Label Distribution: Describes the extend functionality of existing protocols and how to create a new protocol or protocols dedicated to the task of label exchange. Packet Propagation, Interim Packet Propagation, Further Label Allocation also explained

10.0 Configuring Frame Mode MPLS

- 10.1. Describes the requirements and process for configuring CEF (Cisco Express Forwarding); A Cisco proprietary switching mechanism. How CEF runs in central mode or distributed mode and additional options available for CEF configuration include CEF load balancing, CEF network accounting, CEF distributed tunnel switching also introduced
- 10.2. Describes the process of configuring MPLS on a Frame Mode Interface, and how to enabling label distribution protocols by using the mpls label protocol command (the old version is tag-switching commands), such as both, ldp, tdp after enabling MPLS on the interface
- 10.3. Describe the process of configuring a proper MTU Size on a MPLS-enabled interface, and provide the examples of MTU Configuration, and shows sample output of using the commands, such as show mpls ldp neighbor, debug mpls ldp bindings, and debug mpls ldp bindings

11.0 MPLS VPN Technologies

- 11.1. Describe the basic architecture behind MPLS VPNs, the evolutionary path of the VPN and how it has come to encompass a very different set of technologies depending on how it is to be deployed: the VLAN (Virtual local-area networks) and VPDN (Virtual Private dialup networks). Te essentially two models of a typical VPN implementation stand point—Overlay VPNs and Peer-to-Peer VPNs
- 11.2. Have an understanding of Traditional VPNs –The benefits of being able to deploy a fully Layers 3-aware WAN topology with built in redundancy. The diversity and possibilities for service and application offerings by both providers and enterprise customers
- 11.3. Peer-to-Peer VPNs—The benefits and drawbacks of VPN, the idea of how Peer-to-Peer VPNs provide optimal routing solutions and full mesh topological redundancy for WAN-connected sites, the traffic engineered the network based on services offered and SLA (service level agreements)
- 11.4. Knowing the characteristics and basic architecture of MPLS VPN—The MPLS VPN Terminology (C/CE/P network, LSP, P/PE router, PHP, PoP, RD, RT, and End Routing Update Flow, MPLS VPN Packet Forwarding and MPLS VPN PHP). Provides a

snapshot review of the MPLS VPN Router Roles and MPLS VPN Related Protocols, as they pertain to the MPLS technologies

Part III: Ipvsec VPNs

12.0 IPsec VPNs Overview

- 12.1. Understanding the features of IPsec (Internet Protocol Security) suite protocols how it works to provide data confidentiality, data integrity, and data origin authentication to IP packets
- 12.2. Describing VPNs and IKE (Internet Key Exchange), Encryption Algorithms and PKI (Public Key Infrastructure) protocol and frame works; used to exchange security parameters and authentication keys between IPsec endpoints
- 12.3. Explaining of Encryption Algorithms---Mathematical algorithms (and the associated keys) used to make data unreachable to everyone except those who have the proper keying material. Symmetric encryption algorithms as DES, 3DES and AES, HMAC algorithms like MD5 and SHA
- 12.4. Describing a Public Key Infrastructure-A hierarchical framework for managing the security attributes for devices that engage in secure communications across a network. Applying the steps necessary to creating and configuring a Site-to-Site IPsec VPN in SDM (Security Device Manager), using a Site-to-Site VPN Wizard, and monitoring the IPsec VPN tunnel

13.0 Site-to-Site VPN Operations

- 13.1. Site-to-Site VPN Overview---Describes how a single VPN between sites permits various devices to have secure communications
- 13.2. Creating a Site-to-Site IPsec Configuration Steps---Describes what is needed and what is the steps to create a site-to-site VPN. The five generic steps in the lifecycle of any IPsec VPN: Specify interesting traffic, IKE phase 1, IKE phase 2, secure data transfer, and IPsec tunnel termination. Site-to-Site IPsec Configuration Steps---Covers the steps needed to create a site-to-site VPN: Configure the ISAKMP Policy, Configure the IPsec Transform Sets, Configure the Crypto ACL, Configure the Crypto Map, Apply the Crypto Map to the Interface, Configure the Interface ACL
- 13.3. Security Device Manager Features and Interface---Describes how SDM is used to configure a Cisco IOS device, the installation wizard to simplify the router configuration tasks of Initial router configuration, Firewall Setup, Site-to-site VPN, Router lockdown and Security audit, and Testing the IPsec VPN Tunnel
- 13.4. Configuring a Site-to-Site VPN in SDM---Explains the specific steps within SDM to create a site-to-site VPN. List the configuration options as Interfaces and Connections, Firewall and ACL, VPN, Security Audit, Routing, NAT, Intrusion Prevision, Quality of Service, NAC, and Additional Tasks
- 13.5. Monitoring the IPsec VPN Tunnel---Describes how to examine and monitor the VPN tunnel after it has been created, the options on the Tasks bar for the changes to be made:

Overviews, Interface Status, /Firewall Status, VPN Status, QoS Status, NAC Status, and Logging

14.0 GRE Tunneling over IPsec

- 14.1. GRE Characteristics---Using GRE (Generic Routing Encapsulation) to encapsulate virtually any routed or routing protocol to carry a non- packets or IP packet through an IP network
- 14.2. GRE Header---Describes the GRE header that defines what is carried inside the GRE tunnel, understand the three phases of the IPsec VPN configuration: VPN authentication, IKE proposals, IPsec transform sets
- 14.3. Basic GRE Tunnels---How to define and configure the GRE tunnel source, destination, mode and contents across the network. The basic configuration components of a GRE tunnel included: A tunnel source, A tunnel destination, a tunnel mode, and Tunnel traffic; the four routing options supported within the GRE tunnel: EIGRP, OSPF, RIP, and Static routing
- 14.4. Securing and configure GRE over IPsec Using SDM---Describes how SDM wizards permit easy configuration of GRE over IPsec. Understand the six basic steps of the Secure GRE Wizard---Create the GRE tunnel, create a backup GRE tunnel, select the IPsec VPN authentication method, select the IPsec VPN IKE proposals, select the IPsec VPN transform sets, select the routing method for the GRE over IPsec tunnel, and validate the GRE over IPsec configuration

15.0 IPsec High Availability Options

- 15.1. Understanding the sources of IPsec failures---Describes how to determine the source of a network failure in an IPsec VPN. Knowing where failure should occur can help you plan for quick recovery, such as the failure mitigation, and failover strategies
- 15.2. Failure Migration---Describes how to avoid a failure, or how best to react when one occurs, understand the primary failure points and some preventive solutions as Access link failure, Remote peer failure, Device failure, and Path failure
- 15.3. Failover Strategies---Describes how alternative paths are used to continue the flow of data. The two ways (Stateless and Stateful) that IPsec failover can be executed and three failure detection methods (Dead peer detection(DPD), and IGP within GRE over IPsec, and Hot Standby Routing Protocol (HSRP)(or one of the related protocols), and know how to use some typical host-based HSRP interface commands
- 15.4. WAN Backed Up by an IPsec VPN---Describes how a non-protected link can use an established VPN to mitigate failure configuring, monitoring and troubleshooting the Cisco Easy VPN server

16.0 Installing and configuring Cisco VPN Client

- 16.1. Cisco Easy VPN Components---Describes the constituent elements of the Easy VPN solution: Easy VPN Remote and Easy VPN Server , understand Easy VPN Automated Tasks and Cisco Easy VPN Client Modes (Client, Network Extension, and Network Extension Plus)

- 16.2. Easy VPN Connection Establishment---Describes the process of connecting to another site with easy VPN, presents a step-by-step method used to establish Easy VPN remote Client connectivity with an Easy VPN Server gateway: IKE Phase 1, Establishing an ISAKMP SA, SA Proposal Acceptance, Easy VPN User Authentication, Mode Configuration, Reverse Route Injection, IPsec Quick Mode
- 16.3. Easy VPN Server Configuration---Describes the Easy VPN Server configuration process, such as User Configuration and Easy VPN Server Wizard. The policies, pre-shared keys, DNS/WINS servers. DNS domain(s), and IP address pools all need to be preconfigured in the group policy to facilitate VPN Client connections
- 16.4. Monitoring the Easy VPN Server---Describes possible options available for connection monitoring with Easy VPN Server. The use of `show crypto isakmpsa` commands to monitor both the web interface and the CLI, and the use of `show crypto ipsec sa` command to monitor and/or to troubleshooting VPN connections
- 16.5. Troubleshooting the Easy VPN Server---Describes the basic process and options available in troubleshooting Easy VPN Server. The use of `debug crypto isakmp` command

17.0 Implementing the Cisco VPN Client

- 17.1. Cisco VPN Client Installation and Configuration Overview---Describes the purpose of the Cisco VPN Client (Specify a connection name/Primary VPN server address/Group or Group Mutual Group Authentication/transparent tunneling along with TCP-or UDP-based transport, Configuration of additional VPN servers, and Allow configuration of dialup parameters). Provides an overview of the installation and configuration process
- 17.2. Cisco VPN Client Installation---Describes the process of installing the Cisco VPN Client on a client PC. Review the configuration options available before installation, such as Parameter, Location, Purpose and Description
- 17.3. Cisco VPN Client Configuration---Describes the necessary configuration steps for the Cisco VPN Client. The Connection Entry Options Parameters are Connection Entry, Host, Authentication, Transport, Backup Server and Dial-Up

Part IV: Device Hardening

18.0 Cisco Device Hardening

- 18.1. Router Vulnerability---Identifies router services and interfaces that are vulnerable to network attack; the categories are Unnecessary Services and Interfaces, Common Management Services, Path Integrity Mechanisms, Probes and Scans, Terminal Access Security, and Gratuitous and Proxy ARP. Describes the unnecessary services and interfaces that should be disabled, the path integrity mechanisms that should be verified, the service that permit probes and scans that should be disabled, the AutoSecure secures the router functions, the Management plane services and functions secured by AutoSecure, Forwarding plane service and functions secured by AutoSecure, the privileged mode command used to invoke the Auto/Secure process, what the ADM security audit does, and the features of the ADM One-Step Lockdown process

- 18.2. Using Auto Secure to Secure a Router---Explains how to automate the process of locking down a Cisco router with the auto secure command. Describes the router functions are performed with AutoSecure; including Management plane services and functions, Forwarding plane services and functions, Firewall services and functions, Logging functions, NTP, SSH access, and TCP intercept services
- 18.3. Using SDM to Secure a Router---Explains how to use the SDM web-based utility to configure, monitor, and secure a Cisco router as well as how use One-Step Lockdown mode the Security Audit Wizard. Describes AutoSecure Default Configuration and SDM One-Step Lockdown Default Configuration.

19.0 Securing Administrative Access

- 19.1. Describes the basic three ways to configure a Cisco IOS router---CLI, Web interface and SNMP;,, the best practices for passwords that should be enforces for all network devices are Minimum length, Mix of characters, Do not use dictionary words, and Change passwords frequently. Describes a number of access points into a router that should be protect by password, the Cisco IOS log failed login attempts commend, the configuration of Setup mode to permits the configuration of the enable secret, enable, and vty password.
- 19.2. The topics needed to master for the CCNP ISCW exam (I): Router Access-Examines the various physical and logical ways to access a Cisco router, Password Considerations--Describes the best way to construct passwords for network devices, Set Login Limitations---Describes how to limit the number of failed login attempts into the router, Setup Mode---Covers the script that performs basic router configuration, including passwords, CLI Passwords---Describes all password options that can be configured in the CLI
- 19.3. The topics needed to master for the CCNP ISCW exam (II): Additional Line Protections---Covers other IOS features to further protect the console, aux, and vty lines, Password Length Restrictions---Describes how longer passwords are more difficult to guess or break, Password Encryption---Describes how password encryption prevents password compromise if the configuration is compromised
- 19.4. The topics needed to master for the CCNP ISCW exam (III): Create Banners---Describes how to create banners which are used to warn others that the network is for authorized use only, Provide Individual Logins---Explains how each administrator can have an individual login to the router rather than a shared password, Create Multiple Privilege Levels---Describes the various customized privilege levels that can be created to limit access to CLI commands. Role-Basic CLI-Explains how role-based CLI overcomes some of the shortcomings of privilege levels, Prevent Physical Router Compromise---Covers how physical security is sometimes forgotten

20.0 Using AAA to Scale Access Control

- 20.1. Describes the basic functions of AAA and its three components: Authentication, Authorization, and Accounting, two AAA Access Modes (character and packet) with its associated interfaces (Aux, Console, TTY, vty, PPP, ARAP, and NASI). Covers how AAA can depending on the interface used, understanding the TACACS+ and RADIUS

Protocols---Explores the use of TCP for TACACS+ and UDP for RADIUS comparing and contrasting the two systems

- 20.2. Configuring AAA Using the CLI---Explores how to configure AAA using the CLI. A simple five-step process is used to enable you to quickly configure AAA, Configuring AAA Using SDM---Describes how the SDM provides a graphical interface alternative to the CLI and how to configure AAA using SDM using both the basic and advanced modes of SDM. Explains how to use CLI commands including `aaa new model`, `radius-server host`, `tacacs-server host`, `radius-server key`, `tacacs=server key`, `aaa authentication`, `aaa authorization`, and `aaa accounting`
- 20.3. Using Debugging for AAA---Describes the debugging tools provided within the CLI to allow the administrator to quickly troubleshoot issues related to AAA, the use of AAA debug commands including `debug aaa authentication`, `debug aaa authorization`, `debug accounting`, `debug radius`, and `debug tacacs`

21.0 Understanding Cisco IOS Threat Defense Features (Firewall Technology)

- 21.1. Examines the concepts of a Layers Device Structure. A Layered security device provides security on many different IOS layers, explain how Cisco Firewall uses DMZs to isolate services from the internal network
- 21.2. Explores the three basic forms of firewall technology: Application Layer Gateway (ALG), stateful filtering, and stateless filtering. The technologies of Packet filtering (Uses IP addresses and/or port numbers with an ACL), ALG works like a proxy server, Stateful Packet Filtering uses ACS; also knows the connection state to determine access
- 21.3. Covers the most common three features of the Cisco IOS Firewall Feature Set---Cisco IOS Firewall, Authentication Proxy (Provides AAA authentication), and Intrusion Prevention System (IPS); which is a powerful tool that provides many security options (Drop the packet, Block the IP address, Terminate the TCP session, and Send an alarm)
- 21.4. Describes how the Cisco IOS Firewall accomplishes packet filtering by using several differing features including Permits or denies specified TCP and UDP traffic, maintains a state table, modifies ACLs dynamically, protects against DDoS attacks, and inspects packets passing through the interface. Covers Cisco IOS Firewall packet Inspection and Proxy Firewalls---Covers how the capabilities of the Cisco IOS Firewall Feature set combine to provide the best possible protection for the network, how the protocol (TCP,UDP, Applications, and Connectionless services) handled by a stateful packet filter

22.0 Implementing Cisco IOS Firewalls

- 22.1. Describe the five steps to Configuring a Cisco IOS Firewall using the CLI---Choose an interface and Packet Direction to Inspect, Configure an IP ACL for the Interface, Define the Inspection Rules, Apply the Inspection Rules and the ACK to the Interface, Verify the Configuration, use of the `ip inspect name/show ip inspect/debug inspect` command options and its parameters, and describe a simple IP inspection rule
- 22.2. Explains how replacing the CLI with a graphical interface, the Basic Firewall Wizard, makes configurations quick, accurate, and intuitive---Configuring a Basic Firewall or an

Advanced Firewall using SDM and its features: Configure un-trusted network, multiple un-trusted networks, trusted network, and multiple trusted networks.

- 22.3. Describes how adding a DMZ or configuring multiple un-trusted networks through the advanced Firewall Wizard combines ease of use with multiple options to provide for all the configuration needs; such as Configuring DMZ, Configure protocol-specific alerts and protocol-specific logging, Graphic interface, and Monitoring capabilities

23.0 Implementing Cisco IDS and IPS

- 23.1. Describes the functions and operations of intrusion detection systems (IDS) and intrusion prevention systems (IPS); the use of IPS to detect viruses, worms, malicious applications (Trojan horse), and vulnerability exploits, the difference between IDS and IPS Categories of IDS and IPS and how they use together to provide tighter network security
- 23.2. Describes two ways to categorize an IPS or IPS: Scope and Approach to identify malicious traffic. The two IDS and IPS scopes (Network and Host), and three different identity approach mechanisms to categorize IDS and IPS systems with the approach they take to identify malicious traffic (Signature-based, Policy-based and Anomaly-based)
- 23.3. Describes the four types of IDS and IPS signatures---Exploit, Connection, String, and DoS. Describes what happens (the reaction) when a signature is matched including send an alarm to a syslog or centralized management server, Drop the packet, Reset the connection, Block network traffic from the source IP address for a specified amount of time, and Block network traffic on the connection for a specified amount of time
- 23.4. Describes how to configure and verify Cisco IOS IPS using the CLI, the four steps of Cisco IPS configuration commands need to establish A BASIC Cisco IPS NIPS setup: Specify the location of the SDF, Configure the failure parameter, Create an IPS rule, and Apply the IPS rule to an interface. The use of Cisco IOS IPS Configuration commands, such as `ips sdf builtin`, `ip ips fail closed`, `no ip ips fail closed`, `ip ips name testips list 123`, `ip ips tesips in`, `copy flash:attack-drop.sdf ips-sdf`, `copy ips-sdf flash:newsignatures.sdf`, `ip ips sdf location`, and `flash:newsignatures.sdf`
- 23.5. Describes the Cisco IPS takes that are completed with SDM; SDM offers the IPS Wizard to create and edit IPS rules. Explains how to use the Create IPS tab to select the interface, select the traffic direction to inspect, and specify the SDF. Also covers how to function the screens within the Create IPS including Select Interfaces window, SDF Locations window, Add a Signature Location dialog box, IPS Summary window, IPS Policies, Global Settings, SDEE Messages, and Signatures

Prerequisite

Valid CCNA certification

Contact Hours

_____ Contact Hours (Lecture ____ Hours / Lab ____ Hours)

Semester Credit Hours

_____ Semester credit hours

Text / Lab Books

CCNP ISCW Official Exam Certification Guide

- ü Master all **642-825 exam topics** with the official study guide
- ü Access your knowledge with **chapter-opening quizzes**
- ü Review key concepts with **foundation summaries**
- ü Practice with **hundreds of exam questions** on the CD-ROM

Author: Brian Morgan, CCIE® No. 4865, Neil Lovering, CCIE No. 1772

www.ciscopress.com

ISBN-13: 978-1-58720-150-9

ISBN-10: 1-58720-150-X

To gain 45-day Safari Enabled access to this book:

- Go to <http://www.ciscopress.com/safarienabled>
- Complete the brief registration form
- Enter the coupon code 3ZR2-AU1P-9FRQ-NAPZ-ZZVJ

Teaching Strategies

A variety of teaching strategies may be utilized in this course, including but not limited to, lecture, discussion, written classroom exercises, written lab exercises, performance based lab exercises, demonstrations, quizzes and examinations. Some quizzes may be entirely or contain lab based components. A mid-course and end course examination will be given.

CCNP Exams & Recommended Training

Required Exam(s)	Recommended Training
642-901 BSCI	Building Scalable Cisco Internetworks (BSCI)
642-812 BCMSN	Building Cisco Multilayer Switched Network (BCMSN)
642-825 ISCW	Implementing Secure Converged Wide Area Networks (ISCW)
642-845 ONT	Optimizing Converged Cisco Networks (ONT)
OR	

642-892 Composite	Building Scalable Cisco Internetworks (BSCI) Building Cisco Multilayer Switched Network (BCMSN)
642-825 ISCW	Implementing Secure Converged Wide Area Networks (ISCW)
642-845 ONT	Optimizing Converged Cisco Networks (ONT)

Method of Evaluating Students

Grade Distribution

Class Attendance	10
Mid Term	30
Finals	50
Special Projects Makeup projects	10
Total	100%

Grading Policy

At the end of each course, each student is assigned a final grade as follows:

Point Range	Interpretation	Grade	Quality Points
90 – 100	Excellent	A	4.0
80 – 89	Very Good	B	3.0 – 3.9
70 – 79	Average	C	2.0 – 2.9
60 – 69	Poor	D	1.0 – 1.9
Below 60	Failure	F	0
N/A	Withdrawal	W	0
N/A	Pass	P	0
N/A	Incomplete	I	0

A student earning a grade of D or above is considered to have passed the course and is eligible to pursue further studies. A student receiving a grade of F has failed the course. A failed course must be repeated and passed to meet Avtech Institute's graduation requirements, in addition to an overall program GPA of 2.0.

Requirements for Successful Completion of the Course

At a minimum, students must achieve the following:

- A passing grade of **D** or above
- Completion of all required examinations

- Submission of all required lab exercises and projects and;
- Adherence to the school attendance policy.

Equipment Needed

Industry standard desktop computer for lab exercises.

Equipment Breakdown Lab room

Videos and Projector

Library Assignments

To be determined by the instructor.

Portfolio Assignment

Student program outcome portfolios are required to demonstrate student competencies. In conjunction with your course structure, please select a project/paper that best demonstrates what you have learned in this course and add it to your program portfolio.

Course Policies

Disruptive Behavior

Disruptive behavior is an activity that interferes with learning and teaching. Inappropriate talking during class, surfing inappropriate website, tardiness, cheating, alcohol or drug use, use of cell phone, playing loud music during class, etc. all disrupt the learning process.

Copyright Infringement

Specific exemptions to copyright infringement are made for student use in the context of learning activities. Graphic design students often download images from the Internet, or scan images from publications. As long as this work is for educational purpose, and subject to faculty permission, this is not a problem.

Plagiarism

Faculty cannot tolerate the *misrepresentation of work as the student's own*. This often involves the use by one student or another student's design, whether voluntarily or involuntarily. In the event that plagiarism is evident and documented, all students involved in the conscious decision to misrepresent work must receive an F as the grade for the project. A second occurrence may result in suspension for the rest of the quarter, and return to the school only after a review by the Academic Standards Committee.

Attendance

Attendance and Lateness

In education and the workplace, regular attendance is necessary if individuals are to excel. There is a direct correlation between attendance and academic success. Attendance is mandatory. All students must arrive on time and prepared to learn at each class session. At the faculty member's discretion, students may be marked absent if they arrive more than 15 minutes late to any class.

More than five absences in a class that meets twice per week or more than two absences in a class that meets once per week may result in a failure.

Make-Up Work

Late Projects and Homework

All projects and homework must be handed in on time. Homework should be emailed to your instructor if you are going to miss a class. Work that is submitted one week late will result in the loss of one full grade; and work that is submitted two weeks late will result in the loss of two full grades; more than two weeks late you will receive a failing grade on the project.