AVTECH

COURSE SYLLABUS

Cisco Certified Network Professionals

CCNP **BCMSN** (Exam 642-812)

CISCO

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 BCMSN Exam 642-812** 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 BCMSN 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

1. Introduction to Building Cisco Multilayer Switched Networks

1.1. Understand key definitions and the pertains to build Cisco multilayer switched networks (BCMSN), such as the regulatory standards driving enterprise architectures (HIPAA,SEC, Sarbanes-Oxley), hardware-and software-switching terminology (ASIC, QoS marketing, ACL processing or IP rewriting, IOS, MLS, NAT))

1.2. Describes the main model for designing multilayer switched networks-the Enterprise Composite Network Model: Cisco Service-Oriented Network Architecture (SONA), Cisco Intelligent Information Network (IIN), Cisco AVVID Framework, the Enterprise Models: Cisco Enterprise Campus Architecture (Campus Infrastructure, Network Management, and Edge Distribution modules), Cisco Enterprise Data Center Architecture, Cisco Enterprise Branch Architecture, Cisco Enterprise Teleworker Architecture, Cisco Enterprise WAN Architecture, the major functional areas of Enterprise Composite Network Model (Enterprise Campus---Building Access, Building Distribution, Campus Backbone, Data Center, and Enterprise Distribution. Enterprise

Edge—E-Commerce, Internet Connectivity. Remote Access And VPN---Dial-in access concentrators, VPN concentrators, Firewalls and intrusion detection systems (IDS), Layer 2 switched. WAN. Service Provider Edge---ISP, Public Switched Telephone Network (PSTN), Frame Relay, ATM, and PPP. Data Center---Server Fabrics, Storage Area Networks/Fabrics, and Data Center Interconnects, Access Networks)

1.3. A brief review of each Catalyst switch; Understanding Layer 2,3,4 and 7 Switching Terminology in-depth: comparing the varying degree of performance, scalability, availability, and the cost of Enterprise Composite Network Model functional areas: such as Catalyst 6500 Family of Switches, Catalyst 4500 and 4900 Families of Switches, Catalyst 3560 Family of Switches, and Catalyst 2960 Family of Switches

2. The Roles of Switches in Designing Cisco Multilayer Switched Networks

2.1. Recognizing the roles of Switches in designing Cisco Switched Networks: Data Link Technologies ---(10-mbps Ethernet, Fast Ethernet, Gigabit Ethernet), Fast Ethernet and Gigabit Ethernet Auto-Negotiation, 10-Gigabit Ethernet, Gigabit Interface Converters, Cisco Long-Reach Ethernet, and describes how to build different network topologies based on the selecting model

2.2. Selecting the speed of Data Link Technologies for the purpose to Designing Cisco Multilayer Switched Networks using the Cisco Catalyst Switches: Reviewing the Campus Infrastructure Module of the Enterprise Composite Network Model, Selecting Layer 2 or Layer 3 Switches, Small Campus Network Design, Medium-Sized Campus Network Design, Large Campus Network Design, Data Center, Enterprise Edge; using specific Catalyst switches, features, and data-link technologies to apply the topologies based on the model selected

3. Initial Configuration and Troubleshooting of Cisco Multilayer Switches

3.1. Comparing Cisco CatOS and Cisco IOS, such as platform matrix, the features of system differences. Building different network topologies based on Enterprise Composite Network Model and applying the basic configuration parameters for any Catalyst switch, Preparing the initial installations of Catalyst switches with the understanding of the basic CLI configuration parameters---switch name, management IP configuration, telnet and SSH, DNS, system logging, SNMP, clock and NTP Settings

3.2. Managing Catalyst Switch Configurations, understanding the Cisco IOS File System (IFS) and Software Images on Catalyst Switches; knowing how to determining the IFS Size and contents, Cisco IOS Image Naming (Cisco CatOS Image Name to Supervisor Engine Mapping). Learning the steps of upgrading Software Versions on Catalyst Switches and Converting Cisco CatOS to Cisco Native IOS

3.3. Understanding the Basic Troubleshooting Practices: The use of **show** and **debug** Commands, configurations and commands useful when troubleshooting, the impact of debug commands and recommended use, the steps of what to do when you are unable to connect to a Cisco Catalyst switch via the console port and/or to establish IP connectivity to or from the switch using Telnet or SSH

4. Implementing and Configuring VLANs

4.1. Implementing VLANs in Multilayer Switched Networks: Understanding the Role and Benefits of VLANs in the Multilayer Switched Network Design, such as severity, load balancing multiple paths, isolation of failure domains, the benefits of End-to End and local VLANS in a Campus Networks, mapping VLANs to a Hierarchical Network, Static and Dynamic VLANs, VLAN Ranges, the steps of VLAN Configuring modes in Cisco IOS (Global configuration mode, VLAN database configuration mode) and Cisco CatOS, verifying the VLAN Configuration and troubleshooting VLANS; such a slow throughput and communication issues

4.2. Understanding the consists of pVLAN (Private VLAN): A primary VLAN and a secondary VLAN (Community VLANs and Isolated VLANs), the steps of configuring pVLANs in Cisco IOS and in Cisco/CatOS

4.3. Implementing Trunking in Multilayer Switched Networks, the use of trunking protocols (Inter-Switch Link (ISL) and IEEE 802.1Q) in Native VLAN, understanding of DTP, VLAN Ranges and Mapping, Service provider-Managed VLAN Services, Cisco Trunking modes and methods , configuring ISL and 802.1Q trunking in Cisco IOS, Configuring VLAN Trunking in Cisco CatOS, verifying Trunking configurations and troubleshooting trunking

4.4. Applying VLAN Trunking Protocol in the manner of VLAN configuration steps; VTP Pruning, VTP Versions, VTP Authentication, the steps of configuring VTP in Cisco IOS and in Cisco CatOD, verifying the VTP configuration and troubleshooting VTP

5. Understanding and Configuring the 802.1D, 802.1s, and 802.1w Spanning Tree Protocols

5.1. Overview of the Spanning Tree protocol and Identifying Bridging Loops (the preventing of Bridging loops and building Loop-Free Networks, Adding Resiliency to Spanning Tree using advanced features and troubleshooting STP issues

5.2. Understanding the terms root bridge, root ports, and designated ports, and how STP (IEEE 802.1D) uses them to establish a loop-free path through the network: Bridge Identifier, Spanning-Tree Path Cost, Bridge Protocol Data Units (BPTU—Configuration BPDU and Topology Change Notification (TCN) BPDU), Spanning-Tree Port States (Blocking, Listening, Learning, Forwarding, and Disabled) and BPDU Timers (Hello time, Forward delay and Max age)

5.3. Understanding how STP initially converges on a logically loop-free network topology by performing the following steps: Selects one root bridge, selects the root port on all nonroot bridges, and selects the designated port on each segment)

5.4. Introducing of Per VLAN Spanning Tree Plus (Mac Address Allocation and Reduction), STP and IEEE 802.1q Trunks, configuring the basic parameters of PVST (Configuring the root bridge and port cost), verifying the STP configuration, Rapid Spanning Tree Protocol (IEEE 802.1w---RSTP): RSTP Port States, RSTP Port Roles, RSTP BPDU format and BPDU handling, Rapid Transition to Forwarding, RSTP topology change mechanism, compatibility with 802.1D

5.5. Understanding of Multiple Spanning Tree (MST); the extend of IEEE 802.1w RST algorithm to multiple spanning trees: PVST+ case, 802.1Q case, MST cast, MST Regions, IST Instances, MST Instances. Configuring basic parameters of MST with command **spanning-tree mode mst** to configure regions and instances with additional configuration commands.

6. **Adding Resiliency to Spanning Tree Using Advanced Features and Troubleshooting STP Issues**

6.1. The features of Enhancements to 802.1D Spanning Tree Protocol, including PortFast, UplinkFast, and BackboneFast, Improving Spanning-Tree Resiliency with BPDU Guard, BPDU filtering, and Root guard, Preventing Forwarding Loops and Black Holes; Cisco Catalyst switches support two important features to address such conditions---Aggressive mode UDLD and Loop Guard, the comparison between Aggressive mode UDLD and Loop Guard.

6.2. Troubleshooting STP involves identify the potential STP problems (Duplex mismatch, unidirectional link failure, frame corruption, resource errors, PortFast configuration error, Inappropriate STP diameter parameter running) and preventing such loops, including the troubleshooting methodology for STP problems, Know the Network, identify a bridging loop, restore connectivity, check Port status, look for resource errors, and disable unneeded features

7. **Enhancing network stability, functionality, reliability, and performance using advanced features**

7.1. Understanding the features of minimizing network traffic packet loss and the services for adding functionality to the switches to support specific network devices or applications, the use of Layer2 and Layer3 features to effectively administer the network with improved reliability ad stability

7.2. The understanding of EtherChannel (PAgP Modes, LACP Modes), EtherChannel Guidelines, EtherChannel Configuration Example, EtherChannel Load Balancing0, CDP(Voice VLAN and CDP and security issues). The use of command to enable or disable Multiple Default Gateway (MDG) feature, MAC Address Notification, Layer 3 Protocol Filtering (IP, IPX, AppleTalk, DECnet, and Banyan VINES, other protocols), DHCP for Management IP Configuration, Debounce Timer Feature, Broadcast and Multicast Suppression, Baby Giants and Jumbo Frames, Error-Disable Feature, IEEE 802.3 Flow Control, UDLD and Aggressive Mode UDLD

8. **Understanding and configuring Inter-VLAN routing**

8.1. Knowing the architecture of multilayer switching from a Catalyst switch perspective (IP Address), introduction to Inter-VLAN routing (the commands (such as **ping, show running-config, show ip route, show ip protocol**) use of connecting VLANs with Multilayer Catalyst Switches, router on a Stick (External Router), verifying the Inter-VLAN routing configuration

8.2. Understanding the role of I Cisco IOS IP broadcast Forwarding when using VLANs to centrally locate DHCP or other servers (such as forward NetBIOS over IP broadcasts for Microsoft Windows clients that are not using WINS servers) where clients rely on broadcasts to locate or communicate with the services running on the servers by its features to provide DHCP relay agent and UDP broadcast forwarding

9. **Understanding and Configuring Multilayer Switching**

   9.1. Understanding Traditional MLS and learning the configuration of Cisco Express Forwarding (CEF)-based MLS (Centralized and Distributed Switching, Address Resolution Protocol Throttling, Switching Table Architectures (CAM, TCAM, CEF-Based MLS Operation and use of TCAM), and CEF-Based MLS Load Sharin

   9.2. The Configuration and commands use of CEF-Based MLS Configuration, Verification, (show interface), viewing Layer 3 Engine CEF Table (**show ip cef, show ip cef detail**) , viewing the Layer 3 Engine Adjacency Table (**show adjacency, show adjacency detail**), Debugging CEF on the Lay3 Engine (**debug ip cef, drops, receive, evens, prefix-ipc, table, ipc, interface-ipc**) and CEF-Based MLS Troubleshooting Methodology

10. **Understanding and Implementing Quality of Service (QoS) in Cisco Multilayer Switched Networks**

    10.1. Introducing the need of QoS, including the following properties: Ethernet speed mismatch, many=to-one switching fabrics, aggregation, anomalous behavior, security, delay (or latency), delay variation (or jigger), and packet loss

    10.2. Learning the two QoS Service Models (architectures) used in IP networks when designing a QoS solution : IntServ and DiffServ models, the three basic levels of service for QoS: Best-effort service, integrated services, and differentiated services, assured Forwarding and expedited forwarding, the factors (application support, technology upgrade speed and path, and cost) depended on to choose the type of service to use in a multilayer switched network)

    10.3. Catalyst QoS Fundamentals; the Queing Components include classification, marking, traffic conditioning' policing (rate, burst, conforming action, exceed action, violate action) , individual policers, aggregate poplicers, and Microflow policing) and shaping, congestion management (FIFO Queuing, Weighted Round Robin Queuing, Shapped Round Robin (SRR), Prior Queuing, Custom Queuing, and other Congestion-Management Features and Components), and congestion avoidance (Tail drop, weighted random early detection)

    10.4. Using both Layer 2 and Layer 3 features (QoS)to deploy Multicast in the Multilayer Switched Network: QoS in the building access submodule, QoS in the building distribution submodule, and QoS in the campus backbone, use Cisco AutoQoS enables customers to deploy QoS features for converged IP telephony and data network; AutoQoS helps in all five major aspects of successful QoS Deployments (Application classification, policy generation, configuration, monitoring and reporting, and consistency)

11. **Deploying Multicast in the Multilayer Switched Network**

    11.1. Introduction to Multicast; the different effect on network bandwidth: Unicast, Broadcast, and Multicast. The fundamentals (the structure and the range) of IP multicast: Multicast IP address structure, (Reversed Link local addresses, global scoped addresses, source-specific multicast addresses, GLOP addresses, and limited-scope addresses), Multicast MAC address structure, Reverse path forwarding, and Multicast forwarding tree (source trees, shared trees, comparing source trees and shared trees)

11.2. IP Multicast Protocols: protocol independent multicast (PIM) and Internet Group Management Protocol (IGMP), the four models of PIM (dense, sparse, sparse-dense, and bidirectional) automating distribution of RP, Auto-RP, bootstrap router, comparison and compatibility of PIM version 1 and version 2, the current version of IGMP (IGMPv1, IGMPv2, IGMPv3, IGMPv3 lite)

11.3. Multicast Hardware-Based Switching Methods (Multicast multilayer switching (MMLS), CEF-based MMLS, multicast forwarding information base (MFIB) subsystem), Layer 2 Multicast Protocols: the two methods to control multicast at layer 2 on multilayer switches (IGMP snooping, Cisco Group Management Protocol (CGMP))

11.4. IP Multicast in the Multilayer Switched Network, the steps to configure Multicast, monitoring and verifying IP Multicast traffic with commands (**ping, show ip mroute, show ip pim interface, show ip pim interface, show ip mroute, show ip mroute summary, show ip mroute active, show ip mroute count, show ip pim interface count**, and etc.)

12. Design Network Resiliency, Redundancy, and High Availability in Multilayer Switched Networks

12.1. Understanding the basics of Virtual Router Redundancy Protocol (VRRP), Hot Standby Routing Protocol (HSRP), Cisco IOS Software Modularity, and Supervisor Engine redundancy, the Network Components to Achieve High Availability in Multilayer Switches (reliable, fault-tolerant network device, device and link redundancy, resilient network technologies, optimized network design, best practices, and change control)

12.2. Implementing (Configuring and verifying) Redundant Supervisor Engines in Catalyst Switches with the features and protocols: Route Processor Redundancy (RPR) or Route Processor Redundancy Plus (RPR+), Stateful Switchover (SSO), Stateful Switchover (SSO), NSF with SSO (improved network availability and overall network stability)

12.3. Router Redundancy using Single Router Mode on the Catalyst 6500 Series of Switches: the events occur to failover as SRM failure scenario with a catalyst 6500 Supervisor Engine II and MSFC2 and SRM failure scenario with Supervisor Engine IA, and SRM configuration

12.4. Understanding Cisco Software Modularity and In-Service Software Upgrade (ISSU), Implementing Redundant Supervisor Uplink Modules in Catalyst Switches, Implementing Redundant Power Supplies, Implementing Default Gateway Router Redundancy in Multilayer Switched Networks (proxy ARP, routing protocol, ICMP router discovery protocol (IRDP), static default Gateway configuration, hot standby routing protocol, virtual router redundancy protocol, VRRP scenarios, and Gateway load balancing protocol), Cisco IOS Server Load Balancing: Cisco IOS SLB Modes of Operation, configuring the Server Farm in a Data Center with Real Servers , and configuring Virtual Servers

13. Best Practices for Deploying Cisco IP Telephony Using Cisco Catalyst Switches

13.1. The reason to include VoIP when building a converged network, introduction the four primary IP Telephony Components: Infrastructure, IP phones, Cisco CallManager, and voice applications, Network Design recommendations for IP Telephony (QoS, voice (auxiliary) VLANS, network bandwidth provisioning, power considerations, network management, IP telephony high availability, and security)

13.2. Understanding the requirements for IP telephony in multilayer switched networks and voice (auxiliary) VLANs, the best practices for deploying IP Telephony in the enterprise composite network model; such as Layer 3 redundancy using Hot Standby Routing Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP), Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing Protocol (EIGRP) with adequately tuned timers, A-UDLD, QoS with adequately tuned timers

14. Securing the Multilayer Switched Network to minimize service loss and data theft

14.1. Introduction to Layer 2 Security and types of Layer 2 attacks: Learning both control plane (management) security and data plane (traffic) security, understanding the topics on how a rogue device gains unauthorized access, categories of Layer 2 attacks (Attacks on switch configuration/management, MAC layer attacks, Spoof attacks, VLAN attacks, STP attacks, and VTP attacks)

14.2. Catalyst Switch Configuration for Security in Multilayer Switched Networks: Configuring strong system passwords, restricting management access using access control lists, securing physical access to the console, securing access to *vty* lines, configuring system warning banners, disabling unneeded or unused services, trimming and minimizing use of CDP, Disabling the integrated HTTP daemon, configuring basic system logging, securing SNMP, limiting trunking connections and propagated VLANs, securing the Spanning-Tree topology

14.3. Configuring Dynamic Address Resolution Protocol Inspection (DAI) and AAA authorization, authentication, and accounting), Port Security (allowing traffic based on host MAC address, restricts traffic based on host MAC addresses, blocks unicast flood packets on configured ports, prevents MAC flooding attacks, and prevents MAC spoofing attacks), and configuring Network Access Security using IEEE 802.1x

14.4. Understanding Cisco Network Admission Control on Catalyst Switches, applying security using Access Control Lists (RACL, VACL. QoS access control lists, and PACL), the two methods (Order independent and Order dependent) of performing an ACL merge, security networks using Firewalls, security through Network Address Translation (NAT), DHCP Snooping (IP source guard and configuring IPSG), Dynamic ARP Inspection, understanding the role of pVLAN/QoS as a security feature, STP security mechanisms review

15. Having an overview of the Catalyst Switching Architectures

15.1. Catalyst 6500: types of Line cards on Catalyst 6500, Catalyst 6500 Supervisor Engine 32, Catalyst 6500 with Supervisor Engine II, Catalyst 6500 with Supervisor Engine 720, Catalyst 6500 Modules, Catalyst 6500 Service Modules, and Catalyst summary

15.2. Catalyst 4500: the features of Catalyst 4500, Catalyst 4500 fixed configuration models, Catalyst 4500 family of switches Supervisor Engines

15.3. Catalyst 3750: the features of Catalyst 3750, Catalyst 3750 models and the events happen when a port receives a frame, Catalyst 3750 family of switches

15.4. Catalyst 3560: the features of Catalyst 3560, Catalyst 3560 models and the events happen when a port receives a frame, Catalyst 3560 family of switches, the additional critical features of Catalyst 3560

15.5. Catalyst 2960: the features of Catalyst 2960, the events occurs for packet forwarding of Catalyst 2960, and the types of interfaces supported by Catalyst 2960

16. Designing, Building, and Connecting Cisco Multilayer Switched Networks Using Metro Solutions

16.1. Introduction to Cisco Metro Solutions, the design characteristics as high bandwidth in terms of 1 to 10 Gbps, high availability in terms of 10-ms failover, low latency, scalability, and modularity. The definitions for the acronyms and abbreviations used in generic metro solution hierarchy, such as EFM, OPT, L2 Ethernet VPNs, SONEY/SDH, WDM

16.2. Metro Ethernet: Metro Ethernet Connectivity and Transport (the criteria for determining the best available option for metro Ethernet connectivity, such as cost-effectiveness, service level, point-to-point versus multipoint, transparent, scalability, for example, transparent LAN Services (TLS) and Directed VLAN service (DVS)), Metro Ethernet over SONET, Metro Ethernet over Wavelength Division Multiplexing Optical Solutions (Metro Ethernet over DWDM, Metro Ethernet over CDWM), Optical Distance Challenges (Attenuation, Dispersion and Nonlinearitis)

17. Using the performance and connectivity troubleshooting tools for Multilayer Switches

17.1. Techniques to Enhance performance, including user/application performance, capacity planning, and proactive fault management, the critical success tasks that need to be performed for performance management, such as gather a baseline for both network and application data, perform a what-if analysis on your network and applications, perform exception reporting for capacity issues, determine the network management overhead for all proposed or potential network management services, analyze the capacity information, periodically review capacity information, baseline, and exceptions for the network and applications, and maintain upgrade or tunning procedures that are set up to handle capacity issues on both a reactive and longer-term basis

17.2. Using SPAN to monitor the CPU Interface of Switches, monitoring performance with RSPAN, and monitoring performance with EPSPAN, monitoring performance using VACLs with EPSPAN, monitoring performance using VACLs with the Capture option, and troubleshooting using L2 Traceroute

17.3. Understanding the features of the Enhanced Remote SPAN (ERSPAN), the Embedded Event Manager (EEM), and the Network Analysis Module (NAM). Enhancing Troubleshooting and Recovery using Cisco IOS Embedded Event Manager, Performance: the Cisco three NAM versions, the RMON extensions for switched networks used for the NAM monitors and analyzes network traffic, Monitoring using the Network Analysis Module in the Catalyst 6500 Family of Switches,, the show commands used to verify the NAM configuration, troubleshooting common problems with the NAM

18. Knowing the components, topologies, usage and configurations of Wireless into the Campus Network

18.1. Comparison of WLANs to wired LANS: WLAN and Ethernet similarities, WLAN and Ethernet differences: Privacy concerns, environmental concerns, compression concerns, and mobility concerns

18.2. Wireless Network Implementations: Understanding of WLAN components (wires, RF fundamentals, and access point (AP) types---autonomous and light weight), building blocks, building of AP WLAN topologies, topology implementations, wireless theory and standards (RF basics, WLAN: RF math, antennas, regulatory agencies and standards). 802.11 operational standards (IEEE 802.11 standards in the 2.4-GHZ band, 802.11a standards in the 5-GHZ band, , comparing the 802.11 standards), implementing WLANS (802.11b/g channel reuse, 802.11a channel reuse, best practices, bridge path considerations, power implementation)

18.3. Cisco WLANs: Enterprise WLAN issues, overview of Cisco WLAN, comparing Autonomous and Lightweight APs, Wireless LAN management, comparing Core and advanced featuring roaming, split MAC, LWAPP AP association, mixing LWAPP with Autonomous APs), Cisco wireless clients (wireless client association, open authentication, pre-shared key authentication (WEP), introducing WLAN security, Cisco Client Cards, and Cisco compatible extensions

18.4. Configuring a Basic WLAN: Available interfaces (Management, AP-manager, virtual, serve-point, and dynamic) for WLAN configuration and configuring the controller, verifying controller configuration (the use of following commands: **show stats, show client show radius, show rogue ap, show rogue client**)

Prerequisite

Valid CCNA certification or equivalent level of knowledge, Microsoft Office Skills, introductory programming or multimedia courses, and introductory electronics.

Contact Hours

______ Contact Hours (Lecture ___ Hours / Lab ____ Hours)

Semester Credit Hours

__________ Semester credit hours

Text / Lab Books

Authorized Self-Study Guide

Building Cisco Multilayer Switched Networks (BCMSN)

Foundation learning for CCNP 642-812 BCMSN

Author: Richard Froom, CCIE® No. 5102
Balaji Sivasubramanian, Erun Frahim, CCIE No. 7549

www.ciscopress.com

ISBN-13: 978-1-58705-273-6

ISBN-10: 1-58705-273-3

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 PZLM-XSTJ-LMRT-GAJZ-SIYD

Teaching Strategies

The goal of taking the BCMSN course is to prepare and aid the students in passing the Building Cisco Multilayer Switched Networks certification. 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 lout 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 that five absences in a class that meets twice per week or more that 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.