

**NEW ZEALAND INSTITUTES OF TECHNOLOGY AND POLYTECHNIC
QUALIFICATIONS IN INFORMATION & COMMUNICATIONS TECHNOLOGY**

PRESCRIPTION: NW620 NETWORKING PRACTICE

AIM OF MODULE:	To provide students with an understanding of Wide Area Networks (WANs) and the selection, configuration and troubleshooting of networking equipment to interface with WANs and provide enterprise level networking services
CREDITS:	14
KNOWLEDGE ASSUMED FROM:	NW500, NW600 and NW610 (CCNA Exploration 1, 2 and 3)
STUDENT LEARNING HOURS:	140
CONTENT REVISED:	2010
PRESCRIPTION EXPIRY DATE:	November 2013
NOTE:	The content of this module is based on Cisco Networking Academy CCNA - Exploration 4 V4.0 course content and is cognisant of the Plan for Academy Student Success (PASS)

Level and Assessment Schedule

TOPICS	Highest Skill Level				Suggested Assessment Percentage
	R	C	A	P	
1. IP Addressing Services				*	15
2. WAN Technologies and Troubleshooting			*		20
3. Point-to-point Protocol (PPP)				*	10
4. Access Control Lists (ACLs)				*	10
5. Frame Relay				*	15
6. Network Security			*		10
7. Case Study – WAN Technologies				*	20
					<hr/> <hr/> 100 <hr/> <hr/>

LEARNING OUTCOMES

The student will:

- P 1. Describe, verify, configure and troubleshoot; NAT, PAT and DHCP and investigate the IPv6 addressing scheme
- A 2. Describe various WAN technologies including packet and circuit switching, cable modems, Digital Subscriber Line (DSL), broadband wireless Virtual Private Networks (VPNs) and Teleworker Services. Also investigate troubleshooting guidelines and tools
- P 3. Describe Point-to-Point links and the PPP protocol and configure, verify and troubleshoot PPP
- P 4. Describe, verify, configure access control Lists (ACLs)
- P 5. Describe, verify, configure and troubleshoot Frame Relay
- A 6. Describe various security threats, methods and configure router security using the Command Line interface (CLI) and Security Device Manager (SDM)
- P 7. Complete a case study on WAN Technologies, as prescribed by Cisco

CONTENT

1. IP addressing Services

- A description and configuration of Network Address Translation (NAT) and Dynamic Host configuration Protocol (DHCP) will include:
 - A description of NAT and PAT features, advantages and drawbacks
 - A description of private and public addressing
 - Configuring Static, Dynamic, Overload NAT and port forwarding
 - Scaling networks with NAT
 - A description of DHCP operation, relationship to BOOTP
 - A description of DHCP relay
 - Configuring DHCP using the CLI and Cisco SDM
 - Verify and troubleshoot NAT and DHCP configurations
- Investigation of the IPv6 addressing scheme involves:
 - Describing the reasons for using IPv6
 - IPV6 addressing scheme
 - Transition strategies from IPv4
 - Dual Stacking
 - IPv6 Tunnelling
 - NAT protocol translation
 - Routing Considerations
 - RIP and IPv6
 - Name resolution
 - Enabling IPv6 on Cisco routers

2. WAN Technologies

- A description of the various WAN technologies includes:
 - WAN layer 1 concepts and standards
 - WAN layer 2 protocols, frame formats and encapsulation
 - WAN link connection options overview:
 - Private options:
 - Leased lines
 - Circuit switched
 - Analog dialup and ISDN
 - Packet switching
 - X.25, Frame relay and Asynchronous Transfer Mode (ATM)
 - Public options (Teleworker and broadband services):
 - DSL
 - Cable modem
 - Broadband wireless
 - Municipal WiFi
 - WiMAX
 - Satellite internet
 - Virtual Private Networks (VPNs)
 - Types: site-to-site and remote access
 - Characteristics and benefits
 - VPN tunnelling
 - Data Integrity
 - IPSec security protocols
 - Metro Ethernet – and benefits
 - WAN design
 - Traffic, topology and bandwidth considerations
 - Topology considerations
 - Implementation issues
 - Business requirements for Teleworker Services
 - Range of services
 - Internet Service Provider (ISP) case study
 - An investigation of Troubleshooting guidelines and tools include:
 - The documentation process
 - Steps for establishing a network baseline
 - General trouble shooting approaches, procedures and methods
 - Details of troubleshooting at layer 1,2,3,4 and 7 of the OSI model
 - Gathering symptoms and questioning end users
 - Troubleshooting Tools

3. Point-to-Point Protocol (PPP)

- A description of Point-to-Point links and the PPP includes:
 - An introduction to serial communication and time-division multiplexing
 - A description of the demarcation point, DTE-DCE devices and cable standards
 - Encapsulation of HDLC and PPP frames
 - Establishment phases of PPP using Link and Network Control Protocols (LCP and NCP)

- A description of the authentication protocols including:
 - Password Authentication Protocol (PAP)
 - Challenge Handshake Authentication Protocol (CHAP)
 - Configuring, verifying and troubleshooting PPP involves:
 - A description of the layered architecture
 - Configuring PPP authentication
 - Configuring PPP options
 - Verifying and troubleshooting the serial PPP encapsulation configuration
- 4. Access Control Lists (ACLs)**
- A description of ACLs includes:
 - A description of TCP ports and establishment
 - Packet Filtering Types
 - ACL operation:
 - Wildcard masking
 - Where to place
 - A description of ACL types:
 - Standard
 - Extended
 - Named
 - Dynamic
 - Reflexive
 - Configuring, verifying and troubleshooting ACLs involves:
 - Configuring Standard, Dynamic and Named ACLs
 - Applying the ACLs to interfaces
 - Verify and troubleshoot ACL operation
- 5. Frame Relay**
- A description of Frame Relay (FR) includes:
 - A description of FR devices, architecture and operation
 - FR encapsulation process
 - FR topologies: star, full and partial mesh
 - Virtual circuits and address mapping
 - Reach-ability issues and the frame relay sub-interface solution
 - FR costs
 - Over-subscription, bursting, access rate and port speed
 - LMI and stages of inverse ARP and LMI
 - Configuring and troubleshooting FR includes:
 - Configuring Frame Relay encapsulation, bandwidth and LMI types
 - Configuring a static FR map
 - Configuring FR sub-interfaces
 - Verify and troubleshoot the FR configuration
- 6. Network Security**
- A description of security methods includes:
 - Identifying security threats
 - Developing a security policy and details of an enterprise security policy
 - Host and server based security
 - Intrusion and detection based security

- Security appliances and applications
- The Network Security Wheel
- Securing routing protocols: RIPv2, OSPF and EIGRP authentication
- Cisco SDM interface, features, wizards and locking down the router
- Configuring router security involves:
 - Password encryption
 - Routing protocol and AAA authentication
 - Logging router activity
 - Disabling unused interfaces, interface services and global services
 - Locking down routers with Cisco Auto Secure
 - Manage the Cisco IOS and configuration files
 - Performing password recovery using ROM monitor mode
 - Installing Cisco SDM
 - Troubleshoot Cisco IOS configurations

7. Case Study

- The completion of a case study on WANs will require a group of students to:
 - Setup the physical layout of the network using the diagram and accompanying narrative
 - Correctly configure DHCP
 - Correctly configure NAT
 - Possibly configure PPP and Frame Relay
 - Create and apply Access Control Lists (ACLs) on the appropriate routers and interfaces
 - Verify that all configurations are operational and functioning according to the scenario guidelines
 - Provide detailed documentation in a prescribed form as listed in the deliverables sections

NOTES FOR TUTORS

A typical assessment strategy should include:

- practical skills tests
- laboratory exercises
- group activities
- progressive on-line tests (CISCO Web Portal)
- summative (final) on-line test (CISCO Web Portal)
- a final practical test
- kinaesthetic activities

Students are to maintain individual Engineering Journals

LEARNING RESOURCES

- CISCO Networking Academy Programme:
 - Cisco Press: Accessing the WAN, CCNA Exploration Companion Guide
 - Cisco Press: Accessing the WAN, CCNA Exploration Labs and Study Guide