

VERSION

2
4

SR. CODE

EAPL/CRASH/CRTC22

COURSE CODE

EACCN

SUB CATEGORY

NETWORKING & SECURITY



TOTAL DURATION
45
HOURS



THEORY TAKEN
10
HOURS



PRACTICAL TAKEN
35
HOURS

ELYSIUM
ACADEMY
COMPTIA
NETWORK +
(N10-008)

**ELYSIUM
ACADEMY
COMPTIA
NETWORK +
(N10-008)**

ELYSIUM
ACADEMY
COMPTIA
NETWORK +
(N10-008)

COURSE DESCRIPTION



Network designs, network media and topologies, network devices, security, TCP/IP, and configuration are just a few of the subjects covered in the CompTIA Network+ (N10-008) course. Additionally, it covers IPv6, Ethernet, Wireless, SONET/SDH, and WiMAX networking technologies. Learn how to build and configure basic networks and gain an understanding of how to install and support fundamental network technologies.

COURSE GOALS



Those people who want to work as an IT technician or network administrator, CompTIA Network+ (N10-008) is the best course to take. It is also appropriate for people looking to develop the skills necessary to work in network security, oversee cloud-based networks, or become a network technician.

FUTURE SCOPE



A certified IT professional with CompTIA Network+ has the following knowledge and abilities: Create and put into use useful networks. Configure, oversee, and maintain key network hardware. To segregate network traffic and build resilient networks, use hardware like switches and routers.

01

CHAPTER

1. INTRODUCTION PL/SQL

1. Getting started with PL/SQL

- a. What is Oracle PLSQL?
- b. Why Oracle PLSQL?
- c. What can PLSQL do?
- d. How PLSQL works
- e. Advantages of using PLSQL
- f. Websites that uses PLSQL

2. PL/SQL Software Requirements

- a. Downloading Oracle Database
- b. Install the Oracle Database
- c. Unlock The HR Schema
- d. Download and Configure Oracle SQL Developer Software
- e. HR Schema Create Code

3. PLSQL Architecture

a. PLSQL Blocks

- Declare Section
- Begin Section
- Exception Section
- End Section
- Anonymous Blocks
- Named Blocks

b. PLSQL Engine

c. Database Server



01
HRS



02
HRS

O2. Network Types and Characteristics

- a. Peer – To – Peer
- b. Client – Server
- c. Local Area Network (LAN)
- d. Metropolitan Area Network (MAN)
- e. Wide Area Network (WAN)
- f. Wireless Local Area Network (WLAN)
- g. Personal Area Network (PAN)
- h. Campus Area Network (CAN)
- i. Storage Area Network (SAN)
- j. Software – Defined Wide Area Network (SDWAN)
- k. Multiprotocol Label Switching (MPLS)
- l. Multipoint Generic routing Encapsulation (MGRE)

O3. Service – Related Entry Point

- a. V- Switch
- b. Virtual Network Interface Card (VNIC)
- c. Network Function Virtualization (NFV)
- d. Hypervisor

O4. Provider Links

- a. Satellite
- b. Digital Subscriber Line (DSL)
- c. Cable
- d. Leased Line
- e. Metro – Optical

03

CHAPTER

NETWORK TOPOLOGIES AND NETWORK TYPES



01
HRS



01
HRS

O1. Copper

a. Twisted Pair

- CAT 5
- CAT 5e
- CAT 6
- CAT 6a
- CAT 7
- CAT 8

b. Coaxial / RG – 6

c. Twin Axial

d. Termination Standards

- TIA / EIA – 567A
- TIA / EIA – 568 B

O2. Fiber

a. Single – Mode

b. Multimode

O3. Connector Types

a. Local Connector (LC), Straight Tip (ST), Subscriber Connector(SC), Mechanical Transfer (MT), Registered Jack (RJ)

- Angled Physical Contact (APC)
- Ultra – Physical Contact (UPC)

- a. RJ 11
- b. RJ 45
- c. F – Type Connector
- d. Transceiver Type
 - Small Form – Factor Pluggable (SFP)
 - Enhanced Form – Factor Pluggable (SFP +)
 - Quad Small Form Factor Pluggable (QSFP)
 - Enhanced Quad Small Form Factor Pluggable (QSFP +)

O4. Cable Management

- a. Patch Panel / Patch Bay
- b. Fiber Distribution Panel
- c. Punch Down Block
 - 66
 - 110
 - Krone
 - BIX

O5. Ethernet Standards

- a. Copper
 - 10 BASE – T
 - 100 BASE – TX
 - 1000 BASE – T
 - 10 G BASE – T
 - 40 G BASE – T

b. Fiber

- 100 BASE – FX
- 100 BASE – SX
- 1000 BASE – SX
- 1000 BASE – LX
- 10 G BASE – SR
- 10 G BASE – LR
- Coarse Wavelength Division Multiplexing (CWDM)
- Dense Wavelength Division Multiplexing (DWDM)
- Bidirectional Wavelength Division Multiplexing (WDM)

04

CHAPTER

CONFIGURE A SUBNET AND USE APPROPRIATE IP ADDRESSING SCHEMES

O1• Public Vs. Private

- a. TFC1918
- b. Network Address Translation (NAT)
- c. Port Address Translation (PAT)

O2• IPV4 Vs. IPV6

- a. Automatic Private IP Addressing (APIPA)
- b. Extended Unique Identifier (EUI – 64)



- c. Multicast
- d. Unicast
- e. Anycast
- f. Broadcast
- g. Link Local
- h. Loop Back
- i. Default Gateway

O3· IPv4 Sub Netting

- a. Classless (Variable – Length Subnet Mask)
- b. Classful
 - –A
 - –B
 - –C
 - –D
 - –E
 - Classless Inter – Domain Routing (CIDR) Notation

O4· Ipv6 Concepts

- a. Tunneling
- b. Dual Stack
- c. Shorthand Notation
- d. Router Advertisement
- e. Stateless Address Auto Configure (SLAAC)

O5. Virtual IP(VIP)

O6. Sub – Interfaces

O7. Explain Common Ports and Protocols, their application, and Encrypted Alternatives

a. Ports and Protocols

b. Internet Control Message Protocol (ICMP)

c. TCP

d. UDP

e. Generic Routing Encapsulation (GRE)

f. Internet Protocol Security (IPSec)

g. Authentication Header (AH) /

Encapsulation Security Payload (ESP)

h. Connection Less Vs. Connection – Oriented

05

CHAPTER

USE AND PURPOSE OF NETWORK SERVICES

O1. DHCP

a. Scope

b. Exclusion Ranges

c. Reservation

d. Dynamic Assignment

e. Static Assignment

f. Lease Time

g. Scope Options



h. Available Leases

i. DHCP Relay

j. IP Helper / UDP Forwarding

O2. DNS

a. Record Types

- Address (A Vs. AAAA)
- Canonical Name (CNAME)
- Mail Exchange (MX)
- Start of Authority (SOA)
- Pointer (PTR)
- Text (TXT)
- Service (SRV)
- Name Server (NS)

b. Global Hierarchy

- Root DNS Server

c. Internal Vs. External

d. Zone Transfers

e. Authoritative Name Servers

f. Time to Live (TTL)

g. DNS Caching

h. Reverse DNS / Reverse Lookup /
Forward Lookup

i. Recursive Lookup / Iterative Lookup

O3. NTP

- a. Stratum
- b. Clients
- c. Servers

06

CHAPTER

BASIC CORPORATE AND DATACENTER NETWORK

O1. Three-tiered

- a. Core
- b. Distribution/aggregation layer
- c. Access/edge

O2. Software-defined networking

- a. Application layer
- b. Control layer
- c. Infrastructure layer
- d. Management plane

O3. Spine and leaf

- a. Software-defined network
- b. Top-of-rack switching
- c. Backbone

O4. Traffic flows

- a. North-South
- b. East-West



O5· Branch office vs. on-premises datacenter vs. colocation

O6. Storage area networks

- a. Connection types
- b. Fibre Channel over Ethernet (FCoE)
- c. Fibre Channel
- d. Internet Small Computer Systems Interface (iSCSI)

07

CHAPTER

CLOUD CONCEPTS AND CONNECTIVITY

O1· Deployment models

- a. Public
- b. Private
- c. Hybrid
- d. Community

O2· Service models

- a. Software as a service (SaaS)
- b. Infrastructure as a service (IaaS)
- c. Platform as a service (PaaS)
- d. Desktop as a service (DaaS)

O3· Infrastructure as code

- a. Automation/orchestration

O4· Connectivity options



- a. Virtual private network (VPN)
- b. Private-direct connection to cloud provider

O5. Multitenancy

O6. Elasticity

O7. Scalability

O8. Security implications

08

CHAPTER

CONTRAST VARIOUS DEVICES, APPROPRIATE PLACEMENT ON THE NETWORK

O1. Networking devices

- a. Layer 2 switch
- b. Layer 3 capable switch
- c. Router
- d. Hub
- e. Access point
- f. Bridge
- g. Wireless LAN controller
- h. Load balancer
- i. Proxy server
- j. Cable modem
- k. DSL modem
- l. Repeater
- m. Voice gateway



09

CHAPTER

ROUTING TECHNOLOGIES AND BANDWIDTH MANAGEMENT

O1. Routing

- a. Dynamic routing
- b. Protocols [Routing Internet Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP)]
- c. Link state vs. distance vector vs. hybrid
- d. Static routing
- e. Default route
- f. Administrative distance
- g. Exterior vs. interior
- h. Time to live

O2. Bandwidth management

- a. Traffic shaping
- b. Quality of service (QoS)



09

CHAPTER

ROUTING TECHNOLOGIES AND BANDWIDTH MANAGEMENT

O1· Routing

- a. Dynamic routing
- b. Protocols [Routing Internet Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP)]
- c. Link state vs. distance vector vs. hybrid
- d. Static routing
- e. Default route
- f. Administrative distance
- g. Exterior vs. interior
- h. Time to live

O2· Bandwidth management

- a. Traffic shaping
- b. Quality of service (QoS)


01
HRS


01
HRS

TU
HOURS

TU
HOURS

UU
HOURS

10

CHAPTER

INSTALL AND CONFIGURE WIRELESS STANDARDS AND TECHNOLOGIES



01
HRS



1.5
HRS

O1. 802.11 standards

- a. a
- b. b
- c. g
- d. n (WiFi 4)
- e. ac (WiFi 5)
- f. ax (WiFi 6)

O2. Frequencies and range

- a. 2.4GHz
- b. 5GHz

O3. Channels

- a. Regulatory impacts

O4. Channel bonding

O5. Service set identifier (SSID)

- a. Basic service set
- b. Extended service set
- c. Independent basic service set (Ad-hoc)
- d. Roaming

O6. Antenna types

- a. Omni
- b. Directional

O7• Encryption standards

- a. WiFi Protected Access (WPA)/
WPA2 Personal [Advanced
Encryption Standard (AES)/
Temporal Key Integrity Protocol (TKIP)]
- b. WPA/WPA2 Enterprise (AES/TKIP)

O8• Cellular technologies

- a. Code-division multiple access (CDMA)
- b. Global System for Mobile
Communications (GSM)
- c. Long-Term Evolution (LTE)
- d. 3G, 4G, 5G

O9• Multiple input, multiple output (MIMO) and multi-user MIMO (MU-MIMO)

11

CHAPTER

STATISTICS AND SENSORS TO ENSURE NETWORK AVAILABILITY

O1• Performance metrics/sensors

- a. Device/chassis
- b. Temperature
- c. Central processing
unit (CPU) usage
- d. Memory



- e. Network metrics
- f. Bandwidth
- g. Latency
- h. Jitter

O2. SNMP

- a. Traps
- b. Object identifiers (OIDs)
- c. Management information bases (MIBs)

O3. Network device logs

- a. Log reviews
- b. Traffic logs
- c. Audit logs
- d. Syslog
- e. Logging levels/severity levels

O4. Interface statistics/status

- a. Link state (up/down)
- b. Speed/duplex
- c. Send/receive traffic
- d. Cyclic redundancy checks (CRCs)
- e. Protocol packet and byte counts

O5. Interface errors or alerts

- a. CRC errors
- b. Giants
- c. Runts
- d. Encapsulation errors

O6· Environmental factors and sensors

- a. Temperature
- b. Humidity
- c. Electrical
- d. Flooding

O7· Baselines

O8· NetFlow data

O9· Uptime/downtime

12

CHAPTER

PURPOSE OF ORGANIZATIONAL DOCUMENTS AND POLICIES

O1· Plans and procedures

- a. Change management
- b. Incident response plan
- c. Disaster recovery plan
- d. Business continuity plan
- e. System life cycle
- f. Standard operating procedures

O2· Hardening and security policies

- a. Password policy
- b. Acceptable use policy
- c. Bring your own device (BYOD) policy



- d. Remote access policy
- e. Onboarding and offboarding policy
- f. Security policy
- g. Data loss prevention

O3· Common documentation

- a. Physical network diagram
- b. Floor plan
- c. Rack diagram
- d. Intermediate distribution frame (IDF)/main distribution frame (MDF) documentation
- e. Logical network diagram
- f. Wiring diagram
- g. Site survey report
- h. Audit and assessment report
- i. Baseline configurations

O4· Common agreements

- a. Non-disclosure agreement (NDA)
- b. Service-level agreement (SLA)
- c. Memorandum of understanding (MOU)

13

CHAPTER

HIGH AVAILABILITY AND DISASTER RECOVERY CONCEPTS

- O1. Load balancing
- O2. Multipathing
- O3. Network interface card (NIC) teaming
- O4. Redundant hardware/clusters
 - a. Switches
 - b. Routers
 - c. Firewalls
- O5. Facilities and infrastructure support
 - a. Uninterruptible power supply (UPS)
 - b. Power distribution units (PDUs)
 - c. Generator
 - d. HVAC
 - e. Fire suppression
- O6. Redundancy and high availability (HA) concepts
 - a. Cold site
 - b. Warm site
 - c. Hot site
 - d. Cloud site
 - e. Active-active vs. active-passive
 - f. Multiple Internet service providers (ISPs)/diverse paths


01
HRS


1.5
HRS

- g. Virtual Router Redundancy Protocol (VRRP)/First Hop Redundancy Protocol (FHRP)
- h. Mean time to repair (MTTR)
- i. Mean time between failure (MTBF)
- j. Recovery time objective (RTO)
- k. Recovery point objective (RPO)

O7. Network device backup/restore

- a. State
- b. Configuration

14

CHAPTER

COMMON SECURITY CONCEPTS

- O1. Confidentiality, integrity, availability (CIA)**
- O2. Threats**
 - a. Internal
 - b. External
- O3. Vulnerabilities**
 - a. Common vulnerabilities and exposures (CVE)
 - b. Zero-day
- O4. Exploits**
- O5. Least privilege**
- O6. Role-based access**


01
HRS


1.5
HRS

O7. Zero Trust

O8. Defense in depth

- a. Network segmentation enforcement
- b. Perimeter network [previously known as demilitarized zone (DMZ)]
- c. Separation of duties
- d. Network access control
- e. Honeypot

O9. Authentication methods

- a. Multifactor
- b. Terminal Access Controller Access-Control System Plus (TACACS+)
- c. Single sign-on (SSO)
- d. Remote Authentication Dial-in User Service (RADIUS)
- e. LDAP
- f. Kerberos
- g. Local authentication
- h. 802.1X
- i. Extensible Authentication Protocol (EAP)

10. Risk Management

- a. Security risk assessments
- b. Threat assessment
- c. Vulnerability assessment
- d. Penetration testing

- e. Posture assessment
- f. Business risk assessments
- g. Process assessment
- h. Vendor assessment

11. Security information and event management (SIEM)

15

CHAPTER

CONTRAST COMMON TYPES OF ATTACKS

01. Technology-based

- a. Denial-of-service (DoS)/ distributed denial-of-service (DDoS)
- b. Botnet/command and control
- c. On-path attack (previously known as man-in-the-middle attack)
- d. DNS poisoning
- e. VLAN hopping
- f. ARP spoofing
- g. Rogue DHCP
- h. Rogue access point (AP)
- i. Evil twin
- j. Ransomware
- k. Password attacks
- l. Brute-force
- m. Dictionary



01
HRS



01
HRS

- n. Dictionary
- o. MAC spoofing
- p. IP spoofing
- q. Deauthentication
- r. Malware

O2. Human and environmental

- a. Social engineering
- b. Phishing
- c. Tailgating
- d. Piggybacking
- e. Shoulder surfing

16

CHAPTER

NETWORK HARDENING TECHNIQUES

O1. Best practices

- a. Secure SNMP
- b. Router Advertisement (RA) Guard
- c. Port security
- d. Dynamic ARP inspection
- e. Control plane policing
- f. Private VLANs
- g. Disable unneeded switchports
- h. Disable unneeded network services
- i. Change default passwords
- j. Password complexity/length
- k. Enable DHCP snooping
- l. Change default VLAN



01
HRS



01
HRS

- m. Patch and firmware management
- n. Access control list
- o. Role-based access
- p. Firewall rules
- q. Explicit deny
- r. Implicit deny

O2. Wireless security

- a. MAC filtering
- b. Antenna placement
- c. Power levels
- d. Wireless client isolation
- e. Guest network isolation
- f. Preshared keys (PSKs)
- g. EAP
- h. Geofencing
- i. Captive portal

O3. IoT access considerations

02. REMOTE ACCESS METHODS AND SECURITY IMPLICATIONS

O1. Site-to-site VPN

O2. Client-to-site VPN

- a. Clientless VPN
- b. Split tunnel vs. full tunnel

O3. Remote desktop connection

O4. Remote desktop gateway

O5. SSH

- O6. Virtual network computing (VNC)
- O7. Virtual desktop
- O8. Authentication and authorization considerations
- O9. In-band vs. out-of-band management

17

CHAPTER

IMPORTANCE OF PHYSICAL SECURITY

O1. Detection methods

- a. Camera
- b. Motion detection
- c. Asset tags
- d. Tamper detection

O2. Prevention methods

- a. Employee training
- b. Access control hardware
- c. Badge readers
- d. Biometrics
- e. Locking racks
- f. Locking cabinets
- g. Access control vestibule
(previously known as a mantrap)
- h. Smart lockers

O3. Asset disposal

- a. Factory reset/wipe configuration
- b. Sanitize devices for disposal



18

CHAPTER

NETWORK TROUBLESHOOTING

O1· Identify the problem

- a. Gather information
- b. Question users
- c. Identify symptoms
- d. Determine if anything has changed
- e. Duplicate the problem, if possible
- f. Approach multiple problems individually

O2· Establish a theory of probable cause

- a. Question the obvious
- b. Consider multiple approaches
- c. Top-to-bottom/
bottom-to-top OSI model
- d. Divide and conquer

O3· Test the theory to determine the cause

- a. If the theory is confirmed, determine the next steps to resolve the problem
- b. If the theory is not confirmed, reestablish a new theory or escalate



- O4. Establish a plan of action to resolve the problem and identify potential effects
- O5. Implement the solution or escalate as necessary
- O6. Verify full system functionality and, if applicable, implement preventive measures
- O7. Document findings, actions, outcomes, and lessons learned

19

CHAPTER

TROUBLESHOOT COMMON CABLE CONNECTIVITY

- O1. Specifications and limitations
 - a. Throughput
 - b. Speed
 - c. Distance
- O2. Cable considerations
 - a. Shielded and unshielded
 - b. Plenum and riser-rated
- O3. Cable application
 - a. Rollover cable/console cable
 - b. Crossover cable
 - c. Power over Ethernet



O4. Common issues

- a. Attenuation
- b. Interference
- c. Decibel (dB) loss
- d. Incorrect pinout
- e. Bad ports
- f. Open/short
- g. Light-emitting diode (LED) status indicators
- h. Incorrect transceivers
- i. Duplexing issues
- j. Transmit and receive (TX/RX) reversed
- k. Dirty optical cables

O5. Common tools

- a. Cable crimper
- b. Punchdown tool
- c. Tone generator
- d. Loopback adapter
- e. Optical time-domain reflectometer (OTDR)
- f. Multimeter
- g. Cable tester
- h. Wire map
- i. Tap
- j. Fusion splicers
- k. Spectrum analyzers
- l. Snips/cutters
- m. Cable stripper
- n. Fiber light meter

20

CHAPTER

NETWORK SOFTWARE TOOLS AND COMMANDS

O1· Software tools

- a. WiFi analyzer
- b. Protocol analyzer/packet capture
- c. Bandwidth speed tester
- d. Port scanner
- e. iperf
- f. NetFlow analyzers
- g. Trivial File Transfer Protocol (TFTP) server
- h. Terminal emulator
- i. IP scanner

O2· Command line tool

- a. ping
- b. ipconfig/ifconfig/ip
- c. nslookup/dig
- d. traceroute/tracert
- e. arp
- f. netstat
- g. hostname
- h. route
- i. telnet
- j. tcpdump
- k. nmap



O3· Basic network platform commands

- a. show interface
- b. show config
- c. show route

21

CHAPTER

01. TROUBLESHOOT COMMON WIRELESS CONNECTIVITY ISSUES

O1· Specifications and limitations

- a. Throughput
- b. Speed
- c. Distance
- d. Received signal strength indication (RSSI) signal strength
- e. Effective isotropic radiated power (EIRP)/power settings

O2· Considerations

- a. Antennas
- b. Placement
- c. Type
- d. Polarization
- e. Channel utilization
- f. AP association time
- g. Site survey



01
HRS



1.5
HRS

O3. Common issues

- a. Interference
- b. Channel overlap
- c. Antenna cable attenuation/signal loss
- d. RF attenuation/signal loss
- e. Wrong SSID
- f. Incorrect passphrase
- g. Encryption protocol mismatch
- h. Insufficient wireless coverage
- i. Captive portal issues
- j. Client disassociation issues

02. TROUBLESHOOT GENERAL NETWORKING ISSUES

O1. Considerations

- a. Device configuration review
- b. Routing tables
- c. Interface status
- d. VLAN assignment
- e. Network performance baselines

O2. Common issues

- a. Collisions
- b. Broadcast storm
- c. Duplicate MAC address
- d. Duplicate IP address
- e. Multicast flooding
- f. Asymmetrical routing

- g. Switching loops
- h. Routing loops
- i. Rogue DHCP server
- j. DHCP scope exhaustion
- k. IP setting issues
- l. Incorrect gateway
- m. Incorrect subnet mask
- n. Incorrect IP address
- o. Incorrect DNS
- p. Missing route
- q. Low optical link budget
- r. Certificate issues
- s. Hardware failure
- t. Host-based/network-based firewall settings
- u. Blocked services, ports, or addresses
- v. Incorrect VLAN
- w. DNS issues
- x. NTP issues
- y. BYOD challenges
- z. Licensed feature issues
- aa. Network performance issues

Placement Assistance

100%

135+ Professional Courses

Practical Sessions

90%

67+ Global Pacts

Corporate Placements

65%

170+ IT Companies Tie-Up

ELYSIUM
GROUP OF
COMPANIES

**ELYSIUM
ACADEMY**

**PRIVATE
LIMITED**

AUTHORIZED INTERNATIONAL

Partners

