

VERSION

24

PROFESSIONAL

SR. CODE

EAPL/PROF/PRTC18

COURSE CODE

EAPCH

SUB CATEGORY

CYBER SECURITY AND
NETWORKING



TOTAL DURATION

90
HOURS



THEORY TAKEN

20
HOURS



PRACTICAL TAKEN

70
HOURS

COMPTIA
HARDWARE A+
COURSE &
COMPTIA
NETWORK+
(N10-008)
**ELYSIUM
ACADEMY
COMPTIA-
HARDWARE A+
COURSE
& COMPTIA
NETWORK+
(N10-008)**

COURSE DESCRIPTION



CompTIA A+ 220-1102 covers Install, configure, and maintain computer equipment, mobile devices, and software for end users. Understand networking basics and apply basic cybersecurity methods to mitigate threats. Apply troubleshooting skills and provide customer support using appropriate communication skills. Properly and safely diagnose, resolve, and document common hardware and software issues.

COURSE GOALS



CompTIA A+ 220-1102 understands the basics of scripting, cloud technologies, virtualization, and multi-OS deployments in corporate environments. Industry standards and best practices for documentation, change management, disaster prevention and recovery, procedures and policies.

FUTURE SCOPE



Your potential is unrestricted with CompTIA A+ Certification. Because the certification does not emphasize vendor-specific software and hardware, you may concentrate on building your technical foundation and becoming familiar with the technical vocabulary you will need for your chosen career path. You have unfettered access to high-demand careers, such as cybersecurity and computer networking, with the CompTIA A+ certification. It addresses operating system installation and configuration, enhanced security, software troubleshooting, and operational processes

MOBILE DEVICES

01

CHAPTER

01.INSTALL AND CONFIGURE LAPTOP HARDWARE

01.Hardware/device Replacement

- a.Battery
- b.Keyboard/keys
- c.Random-access memory (RAM)
- d.Hard disk drive (HDD)/solid state drive (SSD) migration
- e.HDD/SSD replacement
- f. Wireless cards

02.Physical Privacy and Security Components

- a.Biometrics
- b.Near-field scanner features

02.DISPLAY COMPONENTS OF MOBILE DEVICE TYPES

01.Liquid crystal display (LCD)

- a.In-plane switching (IPS)
- b.Twisted nematic (TN)
- c.Vertical alignment (VA)

02.Organic light-emitting diode (OLED)

- a.Mobile display components
- b.WiFi antenna connector/placement
- c.Camera/webcam
- d.Microphone
- e.Touch screen/digitizer
- f.Inverter


01
HRS


02
HRS

02

CHAPTER

CONFIGURE ACCESSORIES

01. Connection methods

- a. Universal Serial Bus (USB)/ USB-C/ microUSB/miniUSB
- b. Lightning
- c. Serial interfaces
- d. Near-field communication (NFC)
- e. Bluetooth
- f. Hotspot

02. Accessories

- a. Touch pens
- b. Headsets
- c. Speakers
- d. Webcam
- e. Docking station
- f. Port replicator
- g. Trackpad/drawing pad


30
MINS


01
HRS

03

CHAPTER

MOBILE-DEVICE NETWORK CONNECTIVITY

01. Wireless/cellular data network (enable/disable)

- a. 2G/3G/4G/5G
- b. Hotspot
- c. Global System for Mobile Communications (GSM) vs. code-division multiple access (CDMA)
- e. Preferred Roaming List (PRL) updates


30
MINS


01
HOUR

O2. Bluetooth

- a. Global Positioning System (GPS) services
- b. Cellular location services

O3. Mobile device management (MDM)/mobile application management (MAM)

- a. Corporate email configuration
- b. Two-factor authentication
- c. Corporate applications

O4. Mobile device synchronization

- a. Account setup
 - Microsoft 365
 - Google Workspace
 - iCloud
- b. Data to synchronize
 - Mail
 - Photos
 - Calendar
 - Contacts
 - Recognizing data caps

NETWORKING

04

CHAPTER

TRANSMISSION CONTROL PROTOCOL (TCP) AND USER DATAGRAM PROTOCOL (UDP)


01
HRS


02
HRS

01. Ports and protocols

- a.20/21 – File Transfer Protocol (FTP)
- b.22 – Secure Shell (SSH)
- c.23 – Telnet
- d.25 – Simple Mail Transfer Protocol (SMTP)
- e.53 – Domain Name System (DNS)
- f.67/68 – Dynamic Host Configuration Protocol (DHCP)
- g.80 – Hypertext Transfer Protocol (HTTP)
- h.110 – Post Office Protocol 3 (POP3)
- i.137/139 – Network Basic Input/ Output System (NetBIOS)/ NetBIOS over TCP/IP (NetBT)
- j.143 – Internet Mail Access Protocol (IMAP)
- k.161/162 – Simple Network Management Protocol (SNMP)
- l. 389 – Lightweight Directory Access Protocol (LDAP)
- m.443 – Hypertext Transfer Protocol Secure (HTTPS)
- n.445 – Server Message Block (SMB)/Common Internet File System (CIFS)
- o.3389 – Remote Desktop Protocol (RDP)

O2.TCP vs. UDP

a.Connectionless

- DHCP
- Trivial File Transfer Protocol (TFTP)

b.Connection-oriented

- HTTPS
- SSH

05

CHAPTER

COMMON NETWORKING HARDWARE

a.Routers

b.Switches

- Managed
- Unmanaged

c.Access points

d.Patch panel

e.Firewall

f.Power over Ethernet (PoE)

- Injectors
- Switch
- PoE standards

g.Hub

h.Cable modem

i.Digital subscriber line (DSL)

j.Optical network terminal (ONT)

k.Network interface card (NIC)

l.Software-defined networking (SDN)



06

CHAPTER

01.CONTRAST PROTOCOLS FOR WIRELESS NETWORKING

a.Frequencies

- 2.4GHz
- 5GHz

b.Channels

- Regulations
- 2.4GHz vs. 5GHz

c.Bluetooth

d.802.11

- a
- b
- g
- n
- ac (WiFi 5)
- ax (WiFi 6)

e.Long-range fixed wireless

- Licensed
- Unlicensed
- Power
- Regulatory requirements for wireless power

f.NFC

g.Radio-frequency identification (RFID)



02.NETWORKED HOSTS

01. Server Roles

- a.DNS
- b.DHCP
- c.Fileshare
- d.Print servers
- e.Mail servers
- f.Syslog
- g.Web servers
- h.Authentication, authorization,
and accounting (AAA)

02.Internet Appliances

- a.Spam gateways
- b.Unified threat management (UTM)
- c.Load balancers
- d.Proxy servers

03.Legacy/Embedded Systems

- a.Supervisory control and data
acquisition (SCADA)

04.Internet of Things (IoT) Devices

07

CHAPTER

01.INSTALL AND CONFIGURE (SOHO)



30
MINS

01. Internet Protocol (IP) Addressing

a.IPv4

- Private addresses
- Public addresses

b.IPv6

c.Automatic Private IP Addressing (APIPA)

d.Static

e.Dynamic

f.Gateway



1.5
HOURS

02.COMMON NETWORK CONFIGURATION

01.DNS

a.Address

- A
- AAAA

b.Mail exchanger (MX)

c.Text (TXT)

- Spam management

(i) DomainKeys Identified Mail (DKIM)

(ii) Sender Policy Framework (SPF)

(iii) Domain-based Message Authentication, Reporting, and Conformance (DMARC)

08

CHAPTER

INTERNET CONNECTION AND NETWORK TYPES

O1. Internet Connection Types

- a.Satellite
- b.Fiber
- c.Cable
- d.DSL
- e.Cellular
- f.Wireless Internet service provider (WISP)

O2.Network types

- a.Local area network (LAN)
- b.Wide area network (WAN)
- c.Personal area network (PAN)
- d.Metropolitan area network (MAN)
- e.Storage area network (SAN)
- f.Wireless local area network (WLAN)


30
Mins


30
Mins

09

CHAPTER

NETWORKING TOOLS

- a.Crimper
- b.Cable stripper
- c.WiFi analyzer
- d.Toner probe
- e.Punchdown tool
- f.Cable tester
- g.Loopback plug
- h.Network tap


30
Mins


01
HOUR

HARDWARE

10

CHAPTER

CABLE TYPES AND THEIR CONNECTORS

O1. Network Cables

a. Copper

- Cat 5
- Cat 5e
- Cat 6
- Cat 6a
- Coaxial
- Shielded twisted pair

(i) Direct burial

- Unshielded twisted pair

b. Plenum

c. Optical

- Fiber

d. T568A/T568B

O2. Peripheral cables

a. USB 2.0

b. USB 3.0

c. Serial

d. Thunderbolt

O3. Video cables

a. High-Definition Multimedia Interface (HDMI)

b. DisplayPort

c. Digital Visual Interface (DVI)

d. Video Graphics Array (VGA)



O4.Hard drive cables

- a.Serial Advanced Technology Attachment (SATA)
- b.Small Computer System Interface (SCSI)
- c.External SATA (eSATA)
- d.Integrated Drive Electronics (IDE)

O5.Adapters

O6.Connector types

- a.RJ11
- b.RJ45
- c.F type
- d.Straight tip (ST)
- e.Subscriber connector (SC)
- f.Lucent connector (LC)
- g.Punchdown block
- h.microUSB
- i.miniUSB
- j.USB-C
- k.Molex
- l.Lightning port
- m.DB9

11 CHAPTER

INSTALL THE APPROPRIATE RAM

O1.RAM types

- a.Virtual RAM
- b.Small outline dual inline memory module (SODIMM)
- c.Double Data Rate 3 (DDR3)
- d.Double Data Rate 4 (DDR4)
- e.Double Data Rate 5 (DDR5)
- f.Error correction code (ECC) RAM

O2.Single-channel

O3.Dual-channel

O4.Triple-channel

O5.Quad-channel



12 CHAPTER

INSTALL STORAGE DEVICES

O1.Hard Drives

- a.Speeds
 - 5,400rpm
 - 7,200rpm
 - 10,000rpm
 - 15,000rpm
- b.Form factor
 - 2.5
 - 3.5



O2.SSDs

a.Communications interfaces

- Non-volatile Memory Express (NVMe)
- SATA
- Peripheral Component Interconnect Express (PCIe)

b.Form factors

- M.2
- mSATA

O3.Drive configurations

a.Redundant Array of Independent (or Inexpensive) Disks (RAID) 0, 1, 5, 10

O4.Removable storage

a.Flash drives

b.Memory cards

c.Optical drives

13

CHAPTER

CONFIGURE MOTHERBOARDS, CENTRAL PROCESSING UNITS (CPUS)

O1.Motherboard form factor

- a.Advanced Technology eXtended (ATX)
- b.Information Technology eXtended (ITX)

O2.Motherboard connector types

- a.Peripheral Component Interconnect (PCI)
- b.PCI Express (PCIe)



c.Power connectors

d.SATA

e.eSATA

f.Headers

g.M.2

O3.Motherboard Compatibility

a.CPU sockets

· Advanced Micro Devices, Inc. (AMD)

· Intel

b.Server

c.Multisocket

d.Desktop

e.Mobile

O4.Basic Input/Output System (BIOS)/Unified Extensible Firmware Interface (UEFI) settings

a.Boot options

b.USB permissions

c.Trusted Platform Module (TPM) security features

d.Fan considerations

e.Secure Boot

f.Boot password

O5.Encryption

a.TPM

b.Hardware security module (HSM)

O6.CPU architecture

- a.x64/x86
- b.Advanced RISC Machine (ARM)
- c.Single-core
- d.Multicore
- e.Multithreading
- f.Virtualization support

O7.Expansion cards

- a.Sound card
- b.Video card
- c.Capture card
- d.NIC

O8.Cooling

- a.Fans
- b.Heat sink
- c.Thermal paste/pads
- d.Liquid

14

CHAPTER

POWER SUPPLY

- a.Input 110-120 VAC vs. 220-240 VAC
- b.Output 3.3V vs. 5V vs. 12V
- c.20-pin to 24-pin motherboard adapter
- d.Redundant power supply
- e.Modular power supply
- f.Wattage rating


30
Mins


01
HRS

15

CHAPTER

PRINTERS AND SETTINGS

O1. Properly unboxing a device – setup location considerations

O2. Use appropriate drivers for a given OS

a. Printer Control Language (PCL) vs. PostScript

O3. Device connectivity

a. USB

b. Ethernet

c. Wireless

O4. Public/shared devices

a. Printer share

b. Print server

O5. Configuration settings

a. Duplex

b. Orientation

c. Tray settings

d. Quality

O6. Security

a. User authentication

b. Badging

c. Audit logs

d. Secured prints

O7. Network scan services

a. Email

b. SMB

c. Cloud services

O8. ADF/flatbed scanner



30
Mins



01
HRS

16

CHAPTER

INSTALL AND REPLACE PRINTER CONSUMABLES


01
HRS


1.5
HRS

O1. Laser

- a. Imaging drum, fuser assembly, transfer belt, transfer roller, pickup rollers, separation pads, duplexing assembly
- b. Imaging process: processing, charging, exposing, developing, transferring, fusing, and cleaning
- c. Maintenance: Replace toner, apply maintenance kit, calibrate, clean

O2. Inkjet

- a. Ink cartridge, print head, roller, feeder, duplexing assembly, carriage belt
- b. Calibration
- c. Maintenance: Clean heads, replace cartridges, calibrate, clear jams

O3. Thermal

- a. Feed assembly, heating element
- b. Special thermal paper
- c. Maintenance: Replace paper, clean heating element, remove debris
- d. Heat sensitivity of paper

O4. Impact

- a. Print head, ribbon, tractor feed
- b. Impact paper
- c. Maintenance: Replace ribbon, replace print head, replace paper

O5.3-D printer

- a.Filament
- b.Resin
- c.Print bed

VIRTUALIZATION AND CLOUD COMPUTING

17

CHAPTER

CLOUD-COMPUTING CONCEPTS

O1.Common cloud models

- a.Private cloud
- b.Public cloud
- c.Hybrid cloud
- d.Community cloud
- e.Infrastructure as a service (IaaS)
- f.Software as a service (SaaS)
- g.Platform as a service (PaaS)

O2.Cloud characteristics

- a.Shared resources
- b.Metered utilization
- c.Rapid elasticity
- d.High availability
- e.File synchronization

O3.Desktop virtualization

- a.Virtual desktop infrastructure (VDI) on premises
- b.VDI in the cloud



01
HRS



00
HRS

18

CHAPTER

CLIENT-SIDE VIRTUALIZATION

O1. Purpose of virtual machines

- a. Sandbox
- b. Test development
- c. Application virtualization
 - Legacy software/OS
 - Cross-platform virtualization

O2. Resource requirements

O3. Security requirements



30
Mins



30
Mins

HARDWARE AND NETWORK TROUBLESHOOTING

19

CHAPTER

PRACTICE METHODOLOGY TO RESOLVE PROBLEMS

O1. Always consider corporate policies, procedures and impacts before implementing changes

- a. Identify the problem
 - Gather information from the user, identify user changes, and, if applicable, perform backups before making changes
 - Inquire regarding environmental or infrastructure changes



30
Mins



1.5
HRS

O2. Establish a theory of probable cause

- a. If necessary, conduct external or internal research based on symptoms

O3. Test the theory to determine the cause

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

O4. Establish a plan of action to resolve the problem and implement the solution

- a. Refer to the vendor's instructions for guidance

O5. Verify full system functionality and, if applicable, implement preventive measures

O6. Document the findings, actions, and outcomes

20

CHAPTER

TROUBLESHOOT MOTHERBOARDS, RAM, CPU, AND POWER

01.Common symptoms

- a.Power-on self-test (POST) beeps
- b.Proprietary crash screens
(blue screen of death [BSOD]/
pinwheel)
- c.Black screen
- d.No power
- e.Sluggish performance
- f.Overheating
- g.Burning smell
- h.Intermittent shutdown
- i.Application crashes
- j.Grinding noise
- k.Capacitor swelling
- l.Inaccurate system date/time


01
HRS


02
HRS

21

CHAPTER

DIAGNOSE PROBLEMS WITH STORAGE DRIVES

01.Common symptoms

- Light-emitting diode (LED)
status indicators
- Grinding noises
- Clicking sounds
- Bootable device not found


01
HRS


01
HRS

- e.Data loss/corruption
- f.RAID failure
- g.Self-monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) failure
- h.Extended read/write times
- i.Input/output operations per second (IOPS)
- j.Missing drives in OS

22

CHAPTER

TROUBLESHOOT VIDEO, PROJECTOR, AND DISPLAY ISSUES

01.Common symptoms

- a.Incorrect data source
- b.Physical cabling issues
- c.Burned-out bulb
- d.Fuzzy image
- e.Display burn-in
- f.Dead pixels
- g.Flashing screen
- h.Incorrect color display
- i.Audio issues
- j.Dim image
- k.Intermittent projector shutdown



01
HRS



1.5
HRS

23

CHAPTER

TROUBLESHOOT MOBILE DEVICES

01.Common symptoms

- a.Poor battery health
- b.Swollen battery
- c.Broken screen
- d.Improper charging
- e.Poor/no connectivity
- f.Liquid damage
- g.Overheating
- h.Digitizer issues
- i.Physically damaged ports
- j.Malware
- k.Cursor drift/touch calibration


30
Mins


01
HRS

24

CHAPTER

TROUBLESHOOT AND RESOLVE PRINTER ISSUES

01.Common symptoms

- a.Lines down the printed pages
- b.Garbled print
- c.Toner not fusing to paper
- d.Paper jams
- e.Faded print
- f.Incorrect paper size
- g.Paper not feeding
- h.Multipage misfeed


1.5
HRS


01
HRS

- i. Multiple prints pending in queue
- j. Speckling on printed pages
- k. Double/echo images on the print
- l. Incorrect color settings
- m. Grinding noise
- n. Finishing issues
 - Staple jams
 - Hole punch
- o. Incorrect page orientation

25

CHAPTER

TROUBLESHOOT PROBLEMS WITH WIRED AND WIRELESS NETWORKS

01. Common symptoms

- a. Intermittent wireless connectivity
- b. Slow network speeds
- c. Limited connectivity
- d. Jitter
- e. Poor Voice over Internet Protocol (VoIP) quality
- f. Port flapping
- g. High latency
- h. External interference



26

CHAPTER

NETWORK FUNDAMENTALS

- O1. What is NETWORK?
- O2. Concepts For Network +
 - a. Data Networking
 - B. Communication Process
- O3 OSI MODEL / TCP Model
- O4. Encapsulation Concepts
 - a. Data Encapsulation and Decapsulation within the OSI Model Context.
 - b. Ethernet Header
 - c. Internet Protocol (IP) Header
 - d. Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) Headers
 - e. TCP Flags
 - f. Payload
 - g. Maximum Transmission Unit(MTU)



27

CHAPTER

NETWORK TOPOLOGIES AND NETWORK TYPES

- O1. Types Of Topologies
 - a. Star / Hub – and – Spoke
 - b. Mesh
 - c. Bus
 - d. Ring
 - e. Hybrid



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

28

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)

29

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

30

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



01
HRS



01
HRS

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

31

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



01
HRS



01
HRS

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)

32

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

33

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



- n. Media converter
- o. Intrusion prevention system (IPS)/intrusion detection system (IDS) device
- p. Firewall
- q. VPN headend

O2. Networking devices

- a. Voice over Internet Protocol (VoIP) phone
- b. Printer
- c. Physical access control devices
- d. Cameras
- e. Heating, ventilation, and air conditioning (HVAC) sensors
- f. Internet of Things (IoT)
- g. Refrigerator
- h. Smart speakers
- i. Smart thermostats
- j. Smart doorbells
- k. Industrial control systems/ supervisory control and data acquisition (SCADA)

34

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)



35

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)

36

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



01
HRS



1.5
HRS

- 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

37

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)

38

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

39

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)

40

CHAPTER

CONTRAST COMMON TYPES OF ATTACKS

O1. 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



- 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

41

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

42

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



01
HRS



01
HRS

43

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

44

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

45

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



01
HRS



01
HRS

O3· Basic network platform commands

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

46

CHAPTER

01. TROUBLESHOOT COMMON WIRELESS CONNECTIVITY ISSUES



01
HRS



1.5
HRS

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

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

