Network Fundamentals

Exam Information

Exam number
888

Items
67

Points
67

Prerequisites
Computer Maintenance & Repair or Teacher Approval

Recommended course length
One semester or one year

National Career Cluster
Information Technology

Performance standards
Included (Optional)

Certificate available
Yes

Description

The Network Fundamentals industry certification exam assesses the knowledge and skills required to implement a defined network architecture with basic network security. Learners demonstrate their ability to configure, maintain, and troubleshoot network devices using appropriate network tools. They also show an understanding of the features and purpose of network technologies, make basic solution recommendations, analyze network traffic, and are familiar with common protocols and media types.

Exam Blueprint

Standard	Percentage of exam
1. Networking concepts	25%
2. Network installation & configuration	19%
3. Network media & topologies	24%
4. Network management	16%
5. Network security	15%

Standard 1

Networking Concepts

Objective 1 Compare the layers of the OSI and TCP/IP models.

1. OSI model:
    a. Physical
    b. Data Link
    c. Network
    d. Transport
    e. Session
    f. Presentation
    g. Application
2. TCP/IP model:
    a. Network Interface Layer
    b. Internet Layer
    c. Transport Layer
    d. Application Layer

Objective 2 Classify how application, devices, and protocols relate to the OSI model layers.

1. Mac address
2. IP address
3. Frame
4. Packets
5. Switch
6. Router
7. Multilayer switch
8. Hub
9. Encryption devices
10. Cable
11. NIC
12. Bridge

Objective 3 Explain the purpose and properties of IP addressing.

1. Classes of addresses
    a. A, B, C and D
    b. Public vs. Private
2. Classless (CIDR)
3. IPv4 vs. IPv6 (formatting)
4. MAC address format
5. Multicast vs. unicast vs. broadcast
6. APIPA

Objective 4 Explain the purpose and properties of routing and switching.

1. RIP

2. Static
3. Routing metrics (Hop counts, bandwidth, Latency)
4. Next hop
5. Broadcast domain vs. collision domain

Objective 5 Identify common TCP and UDP default ports.

1. SMTP – 25
2. HTTP – 80
3. HTTPS – 443
4. FTP – 20,21
5. TELNET – 23
6. IMAP – 143
7. RDP – 3389
8. SSH – 22
9. DNS – 53
10. DHCP 67, 68

Objective 6 Explain the function of common networking protocols.

1. TCP
2. FTP
3. UDP
4. TCP/IP Suite
5. DHCP
6. TFTP
7. DNS
8. HTTPS
9. HTTP
10. ARP
11. SSH
12. POP3
13. NTP
14. IMAP4
15. Telnet
16. SMTP
17. SNMP2/3
18. ICMP

Objective 7 Summarize DNS concepts and its components

1. DNS Servers
2. New 1.8 TroubleShooting Methodology

Standard 1 Performance Evaluation included below (Optional)

Standard 2

Network Installation and Configuration

Objective 1 Given a scenario, install and configure routers and switches.

1. Routing tables
2. NAT
3. PAT
4. Interface configurations (Full duplex, Half duplex, Port speeds, IP addressing, MAC filtering)
5. PoE

Objective 2 Given a scenario, install and configure a wireless network

1. WAP placement
2. Channels
3. Wireless standards
4. SSID (enable/disable)
5. Compatibility (802.I I a/b/g/n)

Objective 3 Explain the purpose and properties of DHCP.

1. Static vs. dynamic IP addressing
2. Reservations
3. Scopes
4. Leases

Objective 4 Given a scenario, troubleshoot common wireless problems.

1. Interference
2. Signal strength
3. Configurations
4. Incompatibilities
5. Incorrect channel
6. Latency
7. Encryption type
8. Bounce
9. SSID mismatch
10. Incorrect switch placement

Objective 5 Given a scenario, troubleshoot common router, switch and general network problems.

1. Switching loop
2. Bad cables/improper cable types
3. Port configuration
4. VLAN assignment
5. Mismatched MTU/MUT black hole
6. Power failure
7. Bad/missing routes

8. Bad modules (SFPs, GBICs)
9. Wrong subnet mask
10. Wrong gateway
11. Duplicate IP address
12. Wrong DNS

Objective 6 Given a set of requirements, plan and implement a basic SOHO network.

1. List of requirements
2. Cable length
3. Device types/requirements
4. Environment limitations
5. Equipment limitations
6. Compatibility requirements

Objective 7 IP Configuration

1. IP Configuration
2. Subnetting
3. Classless Subnetting

Standard 3

Network Media and Topologies

Objective 1 Categorize standard media types and associated properties.

1. Fiber
   a. Multimode
   b. Singlemode
2. Copper
   a. UTP
   b. STP
   c. CAT3
   d. CAT5
   e. CAT5e
   f. CAT6
   g. CAT6a
   h. Crossover
   i. TI Crossover
   j. Straight-through
3. Plenum vs. non-plenum
4. Distance limitations and speed limitations
5. Broadband over powerline

Objective 2 Categorize standard connector types based on network media.

1. Fiber
    a. ST SC LC
    b. MTRJ
2. Copper
    a. RJ-45 RJ-11 BNC
    b. F-connector
    c. DB-9 (RS-232)
    d. Patch panel
    e. 110 block (T568A, T568B)

Objective 3 Compare and contrast different wireless standards.

1. 802.11 a/b/g/n standards
    a. Distance
    b. Speed
    c. Latency
    d. Frequency
    e. Channels
    f. MIMO
    g. Channel bonding

Objective 4 Categorize WAN technology types and properties.

1. Types:
    a. T1/E1
    b. T3/E3
    c. DS3
    d. OCx
    e. SONET
    f. SDH
    g. DWDM
    h. Satellite
    i. ISDN
    j. Cable
    k. DSL
    l. Cellular
    m. WiMAX
    n. LTE
    o. HSPA+
    p. Fiber
    q. Dialup
    r. PON
    s. Frame relay
    t. ATMs
2. Properties:
    a. Circuit switch
    b. Packet switch

    c. Speed
    d. Transmission media
    e. Distance

Objective 5 Describe different network topologies.

1. MPLS
2. Point-to-point
3. Point-to-multipoint
4. Ring
5. Star
6. Mesh
7. Bus
8. Peer-to-peer
9. Client-server
10. Hybrid

Objective 6 Cable problems:

1. Bad connectors
2. Bad wiring
3. Open, short
4. Split cables
5. DB loss
6. TXRX reversed
7. Cable placement
8. EMI/Interference
9. Distance

Objective 7 Compare and contrast different LAN technologies.

1. Type
    a. Ethernet
    b. 10BaseT
    c. 100BaseT
    d. 1000BaseT
    e. 100BaseTX
    f. 100BaseFX
    g. 1000BaseX
    h. 10GBaseSR
    i. 10GBaseLR
    j. 10GBaseER
    k. 10GBaseSW
    l. 10GBaseLW
    m. 10GBaseEW
    n. 10GBaseT
2. Properties

    a. CSMA/CD
    b. CSMA/CA
    c. Broadcast
    d. Collision
    e. Bonding
    f. Speed
    g. Distance

Objective 8 Identify components of wiring distribution.

1. IDF
2. MDF
3. Demarc
4. Demarc extension
5. Smart jack
6. CSU/DSU

Standard 3 Performance Evaluation included below (Optional)

Standard 4

Network Management

Objective 1 Explain the purpose and features of various network appliances.

1. Load balancer
2. Proxy server
3. Content filter
4. VPN concentrator

Objective 2 Given a scenario, use appropriate hardware tools to troubleshoot connectivity issues.

1. Cable tester
2. Cable certifier
3. Crimper
4. Butt set
5. Toner probe
6. Punch down tool
7. Protocol analyzer
8. Loop back plug
9. TDR
10. OTDR
11. Multimeter
12. Environmental monitor

Objective 3 Given a scenario, use appropriate software tools to troubleshoot connectivity issues.

1. Protocol analyzer
2. Throughput testers
3. Connectivity software
4. Ping
5. Tracert/traceroute
6. Dig
7. Ipconfig/ifconfig
8. Nslookup
9. Arp
10. Nbtstat
11. Netstat
12. Route

Objective 4 Given a scenario, use the appropriate network monitoring resource to analyze traffic.

1. SNMP
2. SNMPv2
3. SNMPv3
4. Syslog
5. System logs
6. History logs
7. General logs
8. Traffic analysis
9. Network sniffer

Objective 5 Describe the purpose of configuration management documentation.

1. Wire schemes
2. Network maps
3. Documentation
4. Cable management
5. Asset management
6. Baselines
7. Change management

Objective 6 Explain different methods and rationales for network performance optimization.

1. Methods:
    a. QoS
    b. Traffic shaping
    c. Load balancing
    d. High availability
    e. Caching engines
    f. Fault tolerance
    g. CARP
2. Reasons:

    a. Latency sensitivity
    b. High bandwidth applications (VoIP, video applications, unified communications)
    c. Uptime

Standard 4 Performance Evaluation included below (Optional)

Standard 5

Network Security

Objective 1 Given a scenario, implement appropriate wireless security measures.

1. Encryption protocols:
    a. WEP
    b. WPA
    c. WPA2
    d. WPA Enterprise
2. MAC address filtering
3. Device placement
4. Signal strength

Objective 2 Explain the methods of network access security

1. ACL:
    a. MAC filtering
    b. IP filtering
    c. Port filtering
2. Tunneling and encryption:
    a. SSL VPN
    b. VPN
    c. L2TP
    d. PPTP
    e. IPSec
    f. ISAKMP
    g. TLS
    h. TLS 1.2
    i. Site-to-site and client-to-site
3. Remote access:
    a. RAS
    b. RDP
    c. PPoE
    d. PPP
    e. ICA
    f. SSH

Objective 3 Explain methods of user authentication.

1. PKI
2. Kerberos
3. AAA (RADIUS, TACACS+)
4. Network access control (802.1x, posture assessment)
5. CHAP
6. MS-CHAP
7. EAP
8. Two-factor authentication
9. Multi Factor authentication
10. Single sign-on
11. Secure passwords

Objective 4 Explain common threats, vulnerabilities, and mitigation techniques.

1. Wireless:
    a. War driving
    b. Warchalking
    c. WEP cracking
    d. WPA cracking
    e. Evil twin
    f. Rogue access point
2. Attacks:
    a. DoS
    b. DDoS
    c. Man in the middle
    d. Social engineering
    e. Virus
    f. Worms
    g. Buffer overflow
    h. Packet sniffing
    i. FTP bounce
    j. Smurf
3. Mitigation techniques
    a. Training and awareness
    b. Patch management
    c. Policies and procedures
    d. Incident response

Objective 5 Given a scenario, install and configure a basic firewall.

1. Types
    a. Software and hardware firewalls
    b. Port security
    c. Firewall rules
        i. Block/Allow
        ii. Implicit deny

        iii. ACL

    d. NAT/PAT
    e. DMZ

Objective 6 Categorize different types of network security appliances and methods.

1. IDS and IPS:
    a. Behavior based
    b. Signature based
    c. Network based
    d. Host based
2. Vulnerability scanners:
    a. NESSUS
    b. NMAP
3. Methods
    a. Honeypots
    b. Honeynets

Standard 5 Performance Evaluation included below (Optional)

Network Fundamentals

Performance assessments may be completed and evaluated at any time during the course. The following performance skills are to be used in connection with the associated standards and exam. To pass the performance standard the student must attain a performance standard average of 8 or higher on the rating scale. Students may be encouraged to repeat the objectives until they average 8 or higher.

Student's Name: ____

Class: ____

Performance standards rating scale

0	Limited skills	2	⟶	4	Moderate skills	6	⟶	8	High skills	10

Standard 1 – Networking Concepts

Score:

- Explain the differences between OSI and TCP/IP layers and models
- Identify TCP and UDP ports and their numbers
- Describe the relationship between network devices, applications and protocols and the OSI model
- Explain networking protocols and DNS components

Standard 3 – Networking Media and Topologies

Score:

- Identify the different network media types and connectors
- Identify wiring distribution components

Standard 4 – Networking Management

Score:

- Troubleshoot hardware connectivity problems
- Troubleshoot software connectivity problems

Standard 5 – Network Security

Score:

- Identify network access security methods
- Demonstrate how remote access works
- Explain the different user authentication methods
- Install a basic firewall

Performance standard average score:

Evaluator Name: ____

Evaluator Title: ____

Evaluator Signature: ____

Date: ____