Network Fundamentals (888)

Description

The knowledge and skills contained in these Network Fundamentals standards cover the necessary competencies for an entry-level Network professional. These include an understanding of the purpose of different networking equipment and tools, and the ability to install, configure, maintain, and troubleshoot standard network architecture, configurations, equipment, and protocols.

Total Test Questions:	77	Levels:	10-12	Units of Credit: .5 or 1.0
Prerequisites: Computer Maintenance and Repair (884)				

Standards, Objectives, and Indicators

STANDARD 1 — 38% of Exam Blueprint

- **Students will identify and understand key terms and concepts relating to network administration.**

Objective 1: Show competency in your understanding of the differences between OSI and TCP/IP layers and models

1. OSI
   - Explain Physical Layer
   - Explain Data link Layer
   - Explain Network Layer
   - Explain Transport Layer
   - Explain Session Layer
   - Explain Presentation Layer
   - Explain Application Layer
2. TCP/IP
   - Explain Network Interface Layer
   - Explain Internet Layer
   - Explain Transport Layer
   - Explain Application Layer

Objective 2: Show competency in your ability to describe the relationship between network devices, applications and protocols and the OSI model.

- Identify hub
- Identify bridge
- Identify NIC (Network Interface Card)
- Identify various encryption devices
- Identify switch
- Identify multilayer switch
- Identify router
- Identify MAC address and its components
- Identify IP address
- Explain EUI-64

- Explain frames
- Explain packets

Objective 3: Show competency in your ability to describe the purposes and properties of IP addressing.

- Identify address classes
  - A, B, C and D
  - Public vs. Private
- Explain Classless (CIDR) (Classless Inter-Domain Routing)
- Explain IPv4 vs. IPv6 (formatting)
- Explain Subnetting
- Explain MAC address format
- Explain Multicast vs. unicast vs. broadcast
- Explain APIPA (Automatic Private IP Addressing)

Objective 4: Show competency in your ability to describe the purposes and properties of routing and switching.

- Define routing metrics
  - Hop counts
  - MTU (Maximum Transition Unit), bandwidth
  - Costs
  - Latency
- Routing tables
- RIP (Routing Information Protocol)
- Link state vs. distance vector vs. hybrid
- Static vs. dynamic
- Next hop
- Spanning Tree Protocol
- VLAN (802.1q) (Virtual Local Area Network)
- Port mirroring
- Broadcast domain vs. collision domain
- IGP (Internet Gateway Protocol) vs. EGP (Exterior Gateway Protocol)
- Convergence (steady state)

Objective 5: Show competency in identifying TCP and UDP ports and their numbers.
FTP (File Transfer Protocol) – 20, 21

- SSH (Secure Shell) – 22
- TELNET – 23
- SMTP (Simple Mail Transfer Protocol) – 25
- DNS (Domain Name System) – 53
- DHCP (Dynamic Host Configuration Protocol) – 67, 68
- HTTP (Hypertext Transfer Protocol) – 80
- POP3 (Post Office Protocol) -110
- IMAP (Internet Message Access Protocol) – 143
- HTTPS (Hypertext Transfer Protocol Secure) – 443
- RDP (Remote Desktop Protocol) – 3389

Objective 6: Show competency in understanding networking protocols and DNS components.

1. Networking Protocols

- Explain TCP (Transmission Control Protocol)
- Explain TCP/IP suite
- Explain UDP (User Datagram Protocol)

- Explain FTP (File Transfer Protocol)
- Explain TFTP (Trivial File Transfer Protocol)
- Explain DHCP (Dynamic Host Configuration Protocol)
- Explain DNS (Domain Name System)
- Explain HTTP (Hypertext Transfer Protocol)
- Explain HTTPS (Hypertext Transfer Protocol Secure)
- Explain ARP (Address Resolution Protocol)
- Explain SIP (Session Initiation Protocol) (VoIP) (Voice Over Internet Protocol)
- Explain RTP (Real-Time Transfer Protocol) (VoIP)
- Explain SSH (Secure Shell)
- Explain POP3 (Post Office Protocol)
- Explain IMAP4(Internet Message Access Protocol)
- Explain NTP (Network Time Protocol)
- Explain Telnet
- Explain SMTP (Simple Mail Transfer Protocol)
- Explain SNMP2/3 (Simple Network Management Protocol)
- Explain ICMP (Internet Control Message Protocol)
- Explain IGMP (Internet Group Management Protocol)
- Explain TLS (Transport Layer Security)

2. DNS Components
   - Explain DNS servers
   - Explain DNS records
     - A
     - AAAA
     - MX
     - CNAME
     - PTR
   - Explain Dynamic DNS

STANDARD 2 — 7% of Exam Blueprint

Students will understand how install and configure networks.

Objective 1: Show competency in your ability to install and configure routers and switches.

- Explain routing tables
- Explain NAT (Network Address Translation)
- Explain PAT (Port Address Translation)
- Explain VLAN (Virtual Local Area Network) (trunking)
- Explain managed vs. unmanaged switches
- Interface configurations
  - Identify full duplex
  - Identify half duplex
  - Identify IP addressing
  - Identify port speeds
  - Identify MAC filtering

Objective 2: Show competency in installing and configuring a SOHO network.

1. Basic requirements
   - Identify list of requirements
   - Identify cable length

- Identify device types/requirements
- Identify environment limitations
- Identify equipment limitations
- Identify compatibility requirements

2. Wireless requirements
   - Identify WAP (Wireless Application Protocol) placement
   - Identify antenna types
   - Identify interference
   - Identify Frequencies
   - Identify channels
   - Identify wireless standards
   - Identify SSID (Service Set Identifier) (enable/disable)
   - Identify compatibility (802.11 a/b/g/n)

Objective 3: Show competency in understanding the purpose of DHCP.

- Compare static vs. dynamic IP addressing
- Explain reservations
- Explain scopes
- Explain leases
- Explain options (DNS servers, suffixes)

Objective 4: Show competency in troubleshooting routers and switches.

- Recognize switching loop
- Recognize bad cables/improper cable types
- Recognize VLAN assignment
- Recognize port configuration
- Recognize mismatched MTU/MUT black hole
- Recognize power failure
- Recognize bad modules (SFPs, GBICs)
- Recognize bad/missing routes
- Recognize incorrect gateway
- Recognize incorrect subnet mask
- Recognize duplicate
- IP address
- Recognize incorrect DNS

STANDARD 3 — 27% of Exam Blueprint

Students will understand how various network media and topologies.

Objective 1: Show competency in your ability to recognize network media types and connectors.

1. Media Types
   - Identify fiber cable:
     - Multimode
     - Singlemode
   - UTP (Unshielded Twisted Pair)
     - STP (Shielded Twisted Pair)
     - CAT3 (Category 3)
     - CAT5 (Category 5)
     - CAT5e (Category 5e)
     - CAT6 (Category 6)
     - CAT6a (Category 6a)

- Coaxial
- Crossover
- T1 Crossover
- Straight-through

- Identify plenum vs. non-plenum
- Identify media converters:
  - Singlemode fiber-to-Ethernet
  - Multimode fiber-to-Ethernet
  - Fiber-to-Coaxial
  - Singlemode-to-multimode fiber
- Explain distance limitations and speed limitations
- Explain broadband over powerline

2. Connectors
   - Identify Fiber:
     - ST (Straight Tip)
     - SC (Standard Connector)
     - LC (Local Connector)
     - MTRJ (Mechanical Transfer Registered Jack)
   - Identify Copper:
     - RJ-45 (Registered Jack-45)
     - RJ-11 (Registered Jack-11)
     - BNC (Bayonet Neill–Concelman)
     - F-connector
     - DB-9 (RS-232)
     - Patch panel
     - 110 block (T568A, T568B)

Objective 2: Show competency in your ability to explain different network topologies and technologies.

1. Foundational
   - Recognize MPLS (Multi-protocol Label Switching)
   - Recognize point-to-point
   - Recognize point-to-multipoint
   - Recognize ring
   - Recognize star
   - Recognize mesh
   - Recognize bus
   - Recognize peer-to-peer
   - Recognize client-server
   - Recognize hybrid
2. WAN (Wide Area Network) Technologies
   - Types:
     - Explain T1/E1
     - Explain T3/E3
     - Explain DS (Digital Signal) 3
     - Explain OC (Optical Carrier) x
     - Explain SONET (Synchronous Optical Network)
     - Explain SDH (Synchronous Digital Hierarchy)
     - Explain DWDM (Dense Wavelength Division Multiplexing)

- Explain satellite
- Explain ISDN (Integrated Service Digital Network)
- Explain cable
- Explain DSL (Digital Subscriber Line)
- Explain cellular
- Explain WiMAX
- Explain LTE (Long-Term Evolution)
- Explain HSPA+ (High Speed Packet Access)
- Explain fiber
- Explain dial-up
- Explain PON (Passive Optical Network)
- Explain frame relay
- Explain ATMs (Asynchronous Transfer Mode)

- Properties:
  - Explain circuit switch
  - Explain packet switch
  - Explain speed
  - Explain transmission media
  - Explain distance

3. LAN Technologies
   - Explain types of LAN technologies:
     - Ethernet
     - 10BaseT
     - 100BaseT
     - 1000BaseT
     - 100BaseTX
     - 100BaseFX
     - 1000BaseX
     - 10GBaseSR
     - 10GBaseLR
     - 10GBaseER
     - 10GBaseSW
     - 10GBaseLW
     - 10GBaseEW
     - 10GBaseT
   - Explain properties of LAN technologies:
     - CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
     - CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
     - Broadcast
     - Collision
     - Bonding
     - Speed
     - Distance

Objective 3: Show competency in identifying wiring distribution components.

- Identify IDF (Intermediate Distribution Frame)
- Identify MDF (Main Distribution Frame)
- Identify Demarc
- Identify Demarc extension
- Identify Smart jack
- Identify CSU/DSU (Channel Service Unit/Data Service Unit)

STANDARD 4 — 13% of Exam Blueprint

- **Students will understand how to troubleshoot connectivity problems.**

Objective 1: Show competency in your ability to troubleshoot hardware connectivity problems.

- Identify cable tester
- Identify cable certifier
- Identify crimper
- Identify butt set
- Identify toner probe
- Identify punch down tool
- Identify protocol analyzer
- Identify loop back plug
- Identify TDR (Time-Domain Reflectometer)
- Identify OTDR (Optical Time-Domain Reflectometer)
- Identify multimeter
- Identify environmental monitor

Objective 2: Show competency in your ability to troubleshoot software connectivity problems.

- Identify protocol analyzer
- Identify throughput testers
- Identify connectivity software
- Identify Ping
- Identify Tracert/Traceroute
- Identify Dig
- Identify Ipconfig/Ifconfig
- Identify Nslookup
- Identify Arp
- Identify Nbtstat
- Identify Netstat
- Identify Route

STANDARD 5 — 10% of Exam Blueprint

- **Students will understand how to secure a network.**

Objective 1: Show competency in your ability to implement wireless security.

- Encryption protocols:
  - WEP (Wired Equivalent Privacy)
  - WPA, WPA2, WPA Enterprise (Wi-Fi Protected Access)
- MAC address filtering
- Device placement

- Signal strength

Objective 2: Show competency in identifying network access security methods.

- ACL (Access Control List):
  - Explain MAC filtering
  - Explain IP filtering
  - Explain Port filtering
- Remote access:
  - Explain RAS (Remote Access Services)
  - Explain RDP (Remote Desktop Protocol)
  - Explain PPPoE (Point-to-Point Protocol over Ethernet)
  - Explain PPP (Point-to-Point Protocol)
  - Explain ICA (Independent Computing Architecture)
  - Explain SSH (Secure Shell)

Objective 3: Show competency in identifying user authentication methods.

- Explain MS-CHAP (Microsoft-Challenge-Handshake Authentication Protocol)
- Explain CHAP (Challenge-Handshake Authentication Protocol)
- Mitigation techniques:
  - Explain training and awareness
  - Explain patch management
  - Explain policies and procedures
  - Explain incident response

Objective 4: Show competency in installing a basic firewall.

- Types:
  - Identify software and hardware firewalls
- Explain port security
- Explain stateful inspection vs. packet filtering
- Explain firewall rules:
  - Block/allow
  - Implicit deny
  - ACL (Access Control List)
- Explain NAT/PAT (Network Address Translation)/(Port Address Translation)
- Explain DMZ (Demilitarized Zone)

STANDARD 6 — 5% of Exam Blueprint

- **Students will identify and understand general troubleshooting strategies for networks.**

Objective 1: Show competency in identifying the problem by knowing and doing the following:

- Gathering information
- Recognize symptoms
- Question users
- Establish a probable cause
- Test the probable cause
- Determine next steps to resolve problem
- If problem is not resolved, establish a plan of action to resolve the problem and identify potential effects
- Implement the solution or start the process over as necessary
- Verify full system functionality

- Implement preventative measures, if necessary
- Document findings, actions and outcomes