Objectives Map: CompTIA Network+

Topic	Chapter(s)
1.0 Network Technologies	
1.1 Explain the function of common networking protocols	
TCP	2, 7, 8, 9, 10, 11, 12, 13, 17
FTP	9
UDP	9
TCP/IP suite	2, 7, 8, 9
DHCP	7
TFTP	9
DNS	10
HTTP(S)	9
ARP	7
SIP (VoIP)	14
RTP (VoIP)	14
SSH	11
POP3	9
NTP	11
IMAP4	9
Telnet	8, 9
SMTP	9
SNMP2/3	11
ICMP	9
IGMP	9
TLS	9, 11
1.2 Identify commonly used TCP and UDP default ports	
TCP ports:	
FTP – 20, 21	9
SSH – 22	9
TELNET – 23	9
SMTP – 25	9
DNS – 53	10
HTTP – 80	9
POP3 – 110	9
NTP – 123	11

Topic	Chapter(s)
IMAP4 – 143	9
HTTPS – 443	9
UDP ports:	
TFTP – 69	9
DNS – 53	10
BOOTPS/DHCP – 67	7
SNMP – 161	11
1.3 Identify the following address formats	
IPv6	13
IPv4	7
MAC addressing	2, 13
1.4 Given a scenario, evaluate the proper use of the following addressing technologies and addressing schemes	
Addressing Technologies:	
Subnetting	2, 7
Classful vs. classless (e.g. CIDR, Supernetting)	7
NAT	8
PAT	8
SNAT	8
Public vs. private	7
DHCP (static, dynamic APIPA)	7
Addressing schemes:	
Unicast	7
Multicast	7
Broadcast	2, 4, 7
1.5 Identify common IPv4 and IPv6 routing protocols	
Link state:	
OSPF	8
IS-IS	8
Distance vector:	
RIP	8
RIPv2	8
BGP	8
Hybrid:	
EIGRP	8
1.6 Explain the purpose and properties of routing	
IGP vs. EGP	8
Static vs. dynamic	8
Next hop	8
Understanding routing tables and how they pertain to path selection	8
Explain convergence (steady state)	8

Topic	Chapter(s)
1.7 Compare the characteristics of wireless communication standards	
802.11 a/b/g/n:	
Speeds	16
Distance	16
Channels	16
Frequency	16
Authentication and encryption:	
WPA	16
WEP	16
RADIUS	11, 16
TKIP	16
2.0 Network Media and Topologies	
2.1 Categorize standard cable types and their properties	
Type:	
CAT3, CAT5, CAT5e, CAT6	3
STP, UTP	3
Multimode fiber, single-mode fiber	3
Coaxial	3
RG-59	3
RG-6	3
Serial	3
Plenum vs. Non-plenum	3
Properties:	
Transmission speeds	4, 5
Distance	4, 5
Duplex	4, 5
Noise immunity (security, EMI)	3
Frequency	4, 5
2.2 Identify common connector types	
RJ-11	3
RJ-45	3
BNC	3
SC	3
ST	3
LC	3
RS-232	3
RG-59	3
RG-6	3
2.3 Identify common physical network topologies	
Star	3
Mesh	3
Bus	3
Ring	3

Topic	Chapter(s)
Point to point	3
Point to multipoint	3
Hybrid	3
2.4 Given a scenario, differentiate and implement appropriate wiring standards	
568A	4
568B	4
Straight vs. cross-over	4
Rollover	8
Loopback	6
2.5 Categorize WAN technology types and properties	
Type:	
Frame relay	14
E1/T1	14
ADSL	14
SDSL	14
VDSL	14
Cable modem	14
Satellite	14
E3/T3	14
OC-x	14
Wireless	14
ATM	14
SONET	14
MPLS	14
ISDN BRI	14
ISDN PRI	14
POTS	14
PSTN	14
Properties:	
Circuit switch	14
Packet switch	14
Speed	14
Transmission media	14
Distance	14
2.6 Categorize LAN technology types and properties	
Types:	
Ethernet	3, 4, 5
10BaseT	4
100BaseTX	5
100BaseFX	5
1000BaseT	5
1000BaseX	5
10GBaseSR	5

Topic	Chapter(s)
10GBaseLR	5
10GBaseER	5
10GBaseSW	5
10GBaseLW	5
10GBaseEW	5
10GBaseT	5
Properties:	
CSMA/CD	4
Broadcast	3, 4
Collision	4
Bonding	6
Speed	4, 5
Distance	4,5
2.7 Explain common logical network topologies and their characteristics	
Peer to peer	12
Client/server	12
VPN	12
VLAN	12
2.8 Install components of wiring distribution	
Vertical and horizontal cross connects	6
Patch panels	6
66 block	6
MDFs	6
IDFs	6
25 pair	6
100 pair	6
110 block	6
Demarc	6
Demarc extension	6
Smart jack	6
Verify wiring installation	6
Verify wiring termination	6
3.0 Network Devices	
3.1 Install, configure and differentiate between common network devices	
Hub	2, 4
Repeater	4
Modem	11, 14
NIC	2, 4, 6
Media converters	4
Basic switch	4
Bridge	4
Wireless access point	16

Topic	Chapter(s)
Basic router	2, 7, 9
Basic firewall	8, 17
Basic DHCP server	8
3.2 Identify the functions of specialized network devices	
Multilayer switch	12
Content switch	12
IDS/IPS	12
Load balancer	12
Multifunction network devices	12
DNS server	10
Bandwidth shaper	12
Proxy server	12
CSU/DSU	14
3.3 Explain the advanced features of a switch	
PoE	14
Spanning tree	4
VLAN	12
Trunking	12
Port mirroring	12
Port authentication	12
3.4 Implement a basic wireless network	
Install client	16
Access point placement	16
Install access point	16
Configure appropriate encryption	16
Configure channels and frequencies	16
Set ESSID and beacon	16
Verify installation	16
4.0 Network Management	
4.1 Explain the function of each layer of the OSI model	
Layer 1 – Physical	2
Layer 2 – Data Link	2
Layer 3 – Network	2
Layer 4 – Transport	2
Layer 5 – Session	2
Layer 6 – Presentation	2
Layer 7 – Application	2
4.2 Identify types of configuration management documentation	
Wiring schematics	18
Physical and logical network diagrams	18
Baselines	18
Policies, procedures and configurations	18
Regulations	18

Topic	Chapter(s)
4.3 Given a scenario, evaluate the network based on configuration management documentation	
Compare wiring schematics, physical and logical network diagrams, baselines, policies and procedures and configurations to network devices and infrastructure	18
Update wiring schematics, physical and logical network diagrams, configurations and job logs as needed	18
4.4 Conduct network monitoring to identify performance and connectivity issues using the following:	
Network monitoring utilities (e.g. packet sniffers, connectivity software, load testing, throughput testers)	15, 18
System logs, history logs, event logs	18
4.5 Explain different methods and rationales for network performance optimization	
Methods:	
QoS	18
Traffic shaping	18
Load balancing	18
High availability	18
Caching engines	18
Fault tolerance	18
Reasons:	
Latency sensitivity	18
High bandwidth applications	18
VoIP	18
Video applications	18
Uptime	18
4.6 Given a scenario, implement the following network troubleshooting methodology	
Information gathering; identify symptoms and problems	15
Identify the affected areas of the network	15
Determine if anything has changed	15
Establish the most probable cause	15
Determine if escalation is necessary	15
Create an action plan and solution identifying potential effects	15
Implement and test the solution	15
Identify the results and effects of the solution	15
Document the solution and the entire process	15
4.7 Given a scenario, troubleshoot common connectivity issues and select an appropriate solution	
Physical issues:	
Cross talk	6
Near End crosstalk	6
Attenuation	6
Collisions	6
Shorts	6
Open impedance mismatch (echo)	15
Interference	6

Topic	Chapter(s)
Logical issues:	
Port speed	5
Port duplex mismatch	5
Incorrect VLAN	12
Incorrect IP address	7, 15
Wrong gateway	7, 15
Wrong DNS	10, 15
Wrong subnet mask	7, 15
Issues that should be identified but escalated:	
Switching loop	15
Routing loop	15
Route problems	15
Proxy arp	15
Broadcast storms	15
Wireless Issues:	
Interference (bleed, environmental factors)	16
Incorrect encryption	16
Incorrect channel	16
Incorrect frequency	16
ESSID mismatch	16
Standard mismatch (802.11 a/b/g/n)	16
Distance	16
Bounce	16
Incorrect antenna placement	16
5.0 Network Tools	
5.1 Given a scenario, select the appropriate command line interface tool and interpret the output to verify functionality	
Traceroute	8, 15
Ipconfig	15
Ifconfig	15
Ping	7, 8, 9, 15
Arp ping	10, 15
Arp	15
Nslookup	10, 15
Hostname	15
Dig	10, 15
Mtr	8
Route	8, 15
Nbtstat	10, 15
Netstat	8, 9, 10, 15
5.2 Explain the purpose of network scanners	
Packet sniffers	15
Intrusion detection software	12
Intrusion prevention software	12
Port scanners	15

Topic	Chapter(s)
5.3 Given a scenario, utilize the appropriate hardware tools	
Cable testers	15
Protocol analyzer	15
Certifiers	15
TDR	15
OTDR	15
Multimeter	15
Toner probe	15
Butt set	15
Punch down tool	15
Cable stripper	15
Snips	15
Voltage event recorder	15
Temperature monitor	15
6.0 Network Security	
6.1 Explain the function of hardware and software security devices	
Network based firewall	17
Host based firewall	17
IDS	12
IPS	12
VPN concentrator	12
6.2 Explain common features of a firewall	
Application layer vs. network layer	17
Stateful vs. stateless	17
Scanning services	17
Content filtering	17
Signature identification	17
Zones	17
6.3 Explain the methods of network access security	
Filtering:	
ACL	11
MAC filtering	17
IP filtering	17
Tunneling and encryption	11, 12
SSL VPN	12
VPN	12
L2TP	12
PPTP	12
IPSEC	11, 12, 13
Remote access	14
RAS	14
RDP	14
PPPoE	14

Topic	Chapter(s)
PPP	11, 14
VNC	14
ICA	14
6.4 Explain methods of user authentication	
PKI	11
Kerberos	11
AAA	11
RADIUS	11
TACACS+	11
Network access control	11
802.1x	11
CHAP	11
MS-CHAP	11
EAP	11
6.5 Explain issues that affect device security	
Physical security	17
Restricting local and remote access	17
Secure methods vs. unsecure methods	11
SSH, HTTPS, SNMPv3, SFTP, SCP	9, 11
TELNET, HTTP, FTP, RSH, RCP, SNMPv1/2	9, 11
6.6 Identify common security threats and mitigation techniques	
Security threats:	
DoS	17
Viruses	17
Worms	17
Attackers	17
Man in the middle	17
Smurf	17
Rogue access points	17
Social engineering (phishing)	17
Mitigation techniques:	
Policies and procedures	17
User training	17
Patches and updates	17