

Transition Guide for The Official CompTIA® Network+® (Exam N10-008)

This transition guide is written for instructors who have used the previous *The Official CompTIA Network+ Guides (Exam N10-007)* courseware, and who are looking to come up to speed on the new version of the courseware to support the updated N10-008 exam objectives.

Exam Syllabus Changes

This section identifies changes made between the N10-007 exam objectives document and the N10-008 exam.

Domains and Weighting

The N10-008 exam objectives have a similar domain structure and weighting to the previous version:

N10-008 Exam Domains	N10-007 Exam Domains
1.0 Networking Fundamentals (24%)	1.0 Networking Concepts (23%)
2.0 Network Implementations (19%)	2.0 Infrastructure (18%)
3.0 Network Operations (16%)	3.0 Network Operations (17%)
4.0 Network Security (19%)	4.0 Network Security (20%)
5.0 Network Troubleshooting (22%)	5.0 Network Troubleshooting and Tools (22%)

Objectives Mapping

Each numbered objective is expanded by illustrative subobjective or content example bullet lists. Considering the objective and the range of content examples, 007 objectives can be mapped approximately to 008 equivalents as follows but pay close attention where the Bloom's taxonomy of an objective is changed. Some objectives move between level 2 (explain/compare/summarize) to level 3 (use/apply/configure/install/deploy/troubleshoot). These are highlighted in bold.

N10-008 Exam Objectives	N10-007 Exam Objectives
1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.	1.2 Explain devices, applications, protocols, and services at their appropriate OSI layers. 1.3 Explain the concepts and characteristics of routing and switching.
1.2 Explain the characteristics of network topologies and network types.	1.5 Compare and contrast the characteristics of network topologies, types, and technologies. 2.4 Explain the purposes of virtualization and network storage technologies. 2.5 Compare and contrast WAN technologies.

N10-008 Exam Objectives	N10-007 Exam Objectives
1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	2.1 Given a scenario, deploy the appropriate cabling solution.
1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.	1.3 Explain the concepts and characteristics of routing and switching. 1.4 Given a scenario, configure the appropriate IP addressing components.
1.5 Explain common ports and protocols, their application, and encrypted alternatives.	1.1 Explain the purposes and uses of ports and protocols.
1.6 Explain the use and purpose of network services.	1.8 Explain the functions of network services.
1.7 Explain basic corporate and datacenter network architecture.	New objective but does Incorporate SAN elements from 2.4 Explain the purposes of virtualization and network storage technologies.
1.8 Summarize cloud concepts and connectivity options.	1.7 Summarize cloud concepts and their purposes.
2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.	2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them. 2.3 Explain the purposes and use cases for advanced networking devices.
2.2 Compare and contrast routing technologies and bandwidth management concepts.	1.3 Explain the concepts and characteristics of routing and switching.
2.3 Given a scenario, configure and deploy common Ethernet switching features.	1.3 Explain the concepts and characteristics of routing and switching.
2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.	1.6 Given a scenario, implement the appropriate wireless technologies and configurations. 4.3 Given a scenario, secure a basic wireless network.
3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.	New objective but does incorporate some elements of 3.3 Explain common scanning, monitoring and patching processes and summarize their expected outputs.
3.2 Explain the purpose of organizational documents and policies.	3.1 Given a scenario, use appropriate documentation and diagrams to manage the network. 3.5 Identify policies and best practices.

N10-008 Exam Objectives	N10-007 Exam Objectives
3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.	3.2 Compare and contrast business continuity and disaster recovery concepts.
4.1 Explain common security concepts.	New objective but does incorporate some elements of 4.2 Explain authentication and access controls.
4.2 Compare and contrast common types of attacks.	4.4 Summarize common networking attacks.
4.3 Given a scenario, apply network hardening techniques.	4.5 Given a scenario, implement network device hardening. 4.6 Explain common mitigation techniques and their purposes.
4.4 Compare and contrast remote access methods and security implications.	3.4 Given a scenario, use remote access methods.
4.5 Explain the importance of physical security.	4.1 Summarize the purposes of physical security devices.
5.1 Explain the network troubleshooting methodology.	5.1 Explain the network troubleshooting methodology.
5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	5.2 Given a scenario, use the appropriate tool. 5.3 Given a scenario, troubleshoot common wired connectivity and performance issues.
5.3 Given a scenario, use the appropriate network software tools and commands.	5.2 Given a scenario, use the appropriate tool.
5.4 Given a scenario, troubleshoot common wireless connectivity issues.	5.4 Given a scenario, troubleshoot common wireless connectivity issues.
5.5 Given a scenario, troubleshoot general networking issues.	5.5 Given a scenario, troubleshoot common network service issues.

The following are formally identified as gap objectives:

- 1.7 Explain basic corporate and datacenter network architecture (becomes gap objective 1.1).
- 2.3 Given a scenario, configure and deploy common Ethernet switching features (becomes gap objective 1.2).
- 3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.
- 3.2 Explain the purpose of organizational documents and policies.
- 5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools (becomes gap objective 4.1).

From 007, objectives 2.4 *Explain the purposes of virtualization and network storage technologies* and 2.5 *Compare and contrast WAN technologies* are not separately represented in 008 (for the most part they become examples within 1.2 and 1.7).

New Content Example Items

The following table lists the content examples within each 008 objective that are either new or in a substantially different objective context. Note that for each exam objectives document, these bullet lists are intended to be illustrative and not definitive.

N10-008 Exam Objectives	New Content Examples
1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.	Data encapsulation and decapsulation within the OSI model context examples are listed in detail (previously simply "Protocol data units")
1.2 Explain the characteristics of network topologies and network types.	Hybrid, Peer-to-peer, Client-server, Software-defined wide area network (SDWAN), Multipoint generic routing encapsulation (mGRE), Network function virtualization (NFV), Leased line (previously more detailed T1 etc), Metro-optical (previously Metropolitan Ethernet)
1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.	Twinaxial, Enhanced quad small form-factor pluggable (QSFP+), Krone, Bix, 10BASE-T, 40GBASE-T, 100BASE-FX, 100BASE-SX, 10GBASE-SR, 10GBASE-LR, Coarse wavelength division multiplexing (CWDM), Dense wavelength division multiplexing (DWDM)
1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.	RFC1918, Anycast, Link local, Shorthand notation, Subinterfaces
1.5 Explain common ports and protocols, their application, and encrypted alternatives.	Syslog, SMTP TLS, IMAP over SSL, POP3 over SSL, SQL Server, SQLnet, MySQL, GRE, AH, ESP
1.6 Explain the use and purpose of network services.	Scope (was Pool), UDP forwarding, SOA, Root DNS servers, Zone transfers, Authoritative name servers, TTL (was under DHCP in 007, which was probably an error), DNS caching, Recursive lookup/iterative lookup, NTP (Stratum, Clients, Servers)
1.7 Explain basic corporate and datacenter network architecture.	All except SAN examples
1.8 Summarize cloud concepts and connectivity options.	Community, Desktop as a service (DaaS), Infrastructure as code, Automation/orchestration, Virtual private network (VPN), Private-direct connection to cloud provider, Multitenancy, Elasticity, Scalability

N10-008 Exam Objectives	New Content Examples
2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.	Layer 3 capable switch, Cable/DSL modem (previously just modems), Repeater, VPN headend (was concentrator), Printer, Physical access control devices, Cameras, Heating, ventilation, and air conditioning (HVAC) sensors, Internet of Things (IoT), Refrigerator, Smart speakers, Smart thermostats, Smart doorbells, Industrial control systems/supervisory control and data acquisition (SCADA)
2.2 Compare and contrast routing technologies and bandwidth management concepts.	Administrative distance, Exterior vs. interior, Time to live
2.3 Given a scenario, configure and deploy common Ethernet switching features.	Voice VLAN, Link Aggregation Control Protocol (LACP), Duplex, Speed, Flow control, Auto-medium-dependent interface crossover (MDI-X)
2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.	ax, Wi-Fi 4/5/6, Regulatory impacts, Service set identifier (SSID), Basic service set, Extended service set, Independent basic service set (Ad-hoc), Roaming, Long-Term Evolution (LTE), 3G, 4G, 5G
3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.	Mostly new examples
3.2 Explain the purpose of organizational documents and policies.	Disaster recovery plan, Business continuity plan, Security policy, Floor plan, Site survey report, Audit and assessment report, Baseline configurations, Service-level agreement (SLA), Memorandum of understanding (MOU)
3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.	Multipathing, Cluster switches/routers/firewalls, PDUs, HVAC, Fire suppression, Cloud site, Active-active vs. active-passive, Multiple Internet service providers (ISPs)/diverse paths, Virtual Router Redundancy Protocol (VRRP)/First Hop Redundancy Protocol (FHRP), Recovery time objective (RTO), Recovery point objective (RPO), Network device backup/restore (State, Configuration)

N10-008 Exam Objectives	New Content Examples
4.1 Explain common security concepts.	Confidentiality, integrity, availability (CIA), External threats, Common vulnerabilities and exposures (CVE), Zero-day, Least privilege, Role-based access, Zero Trust, Defense in depth, Separation of duties, Risk Management (Security risk assessments, Threat assessment, Vulnerability assessment, Posture assessment, Business risk assessments, Process assessment, Vendor assessment)
4.2 Compare and contrast common types of attacks.	Botnet/command and control, Dictionary password attacks, MAC/IP spoofing (previously just spoofing), Malware, Human and environmental (Tailgating, Piggybacking, Shoulder surfing)
4.3 Given a scenario, apply network hardening techniques.	Secure SNMP, Router Advertisement (RA) Guard, Dynamic ARP inspection, Control plane policing, Private VLANs, Firewall rules (Explicit deny, Implicit deny), Wireless client isolation, Guest network isolation, IoT access considerations
4.4 Compare and contrast remote access methods and security implications.	Clientless VPN, Split tunnel vs. full tunnel, Remote desktop gateway, Virtual desktop, Authentication and authorization considerations, In-band versus out-of-band (previously just out-of-band)
4.5 Explain the importance of physical security.	Employee training, Locking racks, Locking cabinets, - Access control vestibule (previously known as a mantrap), Smart lockers, Factory reset/wipe configuration, Sanitize devices for disposal
5.1 Explain the network troubleshooting methodology.	None
5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.	Specifications and limitations (Throughput, Speed, Distance), Cable considerations (shielded/unshielded and plenum not previously listed under troubleshooting; riser is new), Cable application (Rollover cable/console cable, Crossover cable, Power over Ethernet), Decibel (dB) loss, Dirty optical cables, Wire map, Tap, Fusion splicers, Snips/cutters, Cable stripper

N10-008 Exam Objectives	New Content Examples
5.3 Given a scenario, use the appropriate network software tools and commands.	Iperf, NetFlow analyzers, Trivial File Transfer Protocol (TFTP) server, Terminal emulator, IP scanner, hostname, telnet, Basic network platform commands (show interface, show config, show route)
5.4 Given a scenario, troubleshoot common wireless connectivity issues.	Specifications and limitations (Throughput, Speed, Distance, Received signal strength indication (RSSI) signal strength, Effective isotropic radiated power (EIRP)/power settings), Considerations (Antennas, Placement, Type, Polarization, Channel utilization, AP association time, Site survey), Antenna cable attenuation/signal loss, Insufficient wireless coverage, Captive portal issues, Client disassociation issues
5.5 Given a scenario, troubleshoot general networking issues.	Considerations (Device configuration review, Routing tables, Interface status, VLAN assignment, Network performance baselines), Collisions, Broadcast storm, Multicast flooding, Asymmetrical routing, Switching loops, Routing loops, Incorrect DNS, Missing route, Low optical link budget, Incorrect VLAN, DNS issues (was name resolution issues), NTP issues (was time issues), BYOD challenges, Licensed feature issues, Network performance issues

Inclusive Language

Use of terminology that exhibits non-inclusive language or inappropriate metaphor is being phased out. Note that exam items may continue to use the deprecated terminology for some time:

Updated Terminology	Deprecated Terminology
On-path attack	Man-in-the-Middle/Man-in-the-Browser
Screened subnet	Demilitarized Zone (DMZ)
Authorized, unauthorized, semi-authorized hacker	White/black/grey hat
Know, unknown, and partially known environments	White/black/grey box
Access control vestibule	Mantrap
Allow list/approved list	Whitelist
Block list/deny list	Blacklist
Person-made disaster	Man-made disaster

LICENSED FOR USE ONLY BY: NADIA AFFANDI · 14256331 · NOV 11 2021

Omitted Subobjectives/Bullet List Items

The following 007 content examples are no longer explicitly called out in the 008 objectives. Some are retained in the acronym list. Where appropriate, some of these content examples continue to be covered in the 008 courseware, especially if they remain in the acronyms list.

N10-007 Exam Objectives	Content Examples That Do Not Appear in 008
1.1 Explain the purposes and uses of ports and protocols.	H.323
1.2 Explain devices, applications, protocols, and services at their appropriate OSI layers.	Broadcast and collision domains (though implicit in other examples), CSMA/CA, Port forwarding, DiffServ, CoS, Distributed switching (now three-tier), Packet-switched vs. circuit-switched network
1.5 Compare and contrast the characteristics of network topologies, types, and technologies.	Technologies that facilitate the Internet of Things (IoT): Z-Wave, Ant+, Bluetooth, NFC, IR, RFID, 802.11
1.6 Given a scenario, implement the appropriate wireless technologies and configurations.	TDMA
1.7 Summarize cloud concepts and their purposes.	Relationship between local and cloud resources
1.8 Explain the functions of network services.	Third-party/cloud-hosted DNS, IPAM
2.1 Given a scenario, deploy the appropriate cabling solution.	BNC, DB-9, DB-25, GBIC, Cat 3, RG-59
2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them.	Wireless range extender
2.3 Explain the purposes and use cases for advanced networking devices.	UTM appliance, NGFW/Layer 7 firewall, VoIP PBX, Content filter
2.4 Explain the purposes of virtualization and network storage technologies.	Virtual firewall, virtual router, NAS, InfiniBand
2.5 Compare and contrast WAN technologies.	ISDN, T1/T3, E1/E3, OC-3 – OC-192, Dial-up, PRI, ATM, Frame relay, PPPoE, PPP, DMVPN, SIP trunk, CSU/DSU
3.1 Given a scenario, use appropriate documentation and diagrams to manage the network.	Diagram symbols, Work instructions, Labeling
3.2 Compare and contrast business continuity and disaster recovery concepts.	Power management (Dual power supplies, Redundant circuits), Backups (Full, Differential, Incremental, Snapshots)
3.4 Given a scenario, use remote access methods.	VPN (SSL/TLS/DTLS), Telnet (though does appear under tools), HTTPS/management URL, OOB Modem, Console router

N10-007 Exam Objectives	Content Examples That Do Not Appear in 008
3.5 Identify policies and best practices.	Privileged user agreement, Licensing restrictions (though does appear as troubleshooting issue), International export controls, Safety procedures and policies
4.3 Given a scenario, secure a basic wireless network.	PEAP, EAP-FAST, EAP-TLS
4.4 Summarize common networking attacks.	Logic bomb, War driving
4.5 Given a scenario, implement network device hardening.	File hashing, Generating new keys
4.6 Explain common mitigation techniques and their purposes.	Signature management, Flood guard, BPDU guard, Root guard, File integrity monitoring, Honeynet
5.2 Given a scenario, use the appropriate tool.	iptables, pathping
5.3 Given a scenario, troubleshoot common wired connectivity and performance issues.	Crosstalk
5.4 Given a scenario, troubleshoot common wireless connectivity issues.	Reflection, Refraction, Absorption, Overcapacity, Frequency mismatch

Course Outline Comparison

This section identifies changes made to the course study guide.

As with 007, the course is presented as a number of topics, each mapped to a discrete job task. Groups of between two and four topics that are closely related are collected into lessons.

Compared to 007, the 008 courseware has been divided into a larger number of lessons and topics with the aim of restricting the size of each topic to no more than ten subject headings. This greater number of lessons does not represent a major increase in the overall course length, however. While there are more content examples to cover, every effort has been made to constrain the overall length of the study guide by condensing text under subject headings.

In a five-day presentation, the course covers the following themes:

- Day One—Networking at the OSI Physical and Data Link layers (Lessons 1-4).
- Day Two—Networking at the OSI Network layer (Lessons 5-8).
- Day Three—Networking at the OSI upper layers (Lessons 9-12).
- Day Four—Security concepts, wireless networks, and WAN/remote access (Lessons 13-16).
- Day Five—Site security and cloud/datacenter concepts (Lessons 17-20).

Compared to 007, complex subjects have been simplified or moved from early lessons and a new topic on SOHO routers aims to summarize basic concepts covered by A+ for students who may not have completed that certification. PHY and cable installation have been consolidated to sequential lessons and compressed. Coverage of security content has been re-sequenced and compressed.

This table compares the outline at lesson level of the new 008 courseware to that of the 007 courseware:

N10-008 Courseware	N10-007 Courseware
Lesson 1: Comparing OSI Model Network Functions	Lesson 1: Explaining the OSI and TCP/IP Models
Lesson 2: Deploying Ethernet Cabling	Lesson 2: Explaining Properties of Network Traffic Lesson 12: Deploying and Troubleshooting Cabling Solutions
Lesson 3: Deploying Ethernet Switching	Lesson 2: Explaining Properties of Network Traffic Lesson 3: Installing and Configuring Switched Networks
Lesson 4: Troubleshooting Ethernet Networks	Lesson 12: Deploying and Troubleshooting Cabling Solutions
Lesson 5: Explaining IPv4 Addressing	Lesson 4: Configuring IP Networks
Lesson 6: Supporting IPv4 and IPv6 Networks	Lesson 4: Configuring IP Networks
Lesson 7: Configuring and Troubleshooting Routers	Lesson 5: Installing and Configuring Routed Networks
Lesson 8: Explaining Network Topologies and Types	Lesson 3: Installing and Configuring Switched Networks
Lesson 9: Explaining Transport Layer Protocols	Lesson 6: Configuring and Monitoring Ports and Protocols
Lesson 10: Explaining Network Services	Lesson 6: Configuring and Monitoring Ports and Protocols
Lesson 11: Explaining Network Applications	Lesson 7: Explaining Network Application and Storage Issues
Lesson 12: Ensuring Network Availability	Lesson 8: Monitoring and Troubleshooting Networks
Lesson 13: Explaining Common Security Concepts	Lesson 9: Explaining Networking Attacks and Mitigations Lesson 11: Explaining Authentication and Access Controls
Lesson 14: Supporting and Troubleshooting Secure Networks	Lesson 10: Installing and Configuring Security Devices Lesson 11: Explaining Authentication and Access Controls
Lesson 15: Deploying and Troubleshooting Wireless Networks	Lesson 13: Implementing and Troubleshooting Wireless Technologies

N10-008 Courseware	N10-007 Courseware
Lesson 16: Comparing WAN Links and Remote Access Methods	Lesson 14: Comparing and Contrasting WAN Technologies Lesson 15: Using Remote Access Methods
Lesson 17: Explaining Organizational and Physical Security Concepts	Lesson 16: Identifying Site Policies and Best Practices
Lesson 18: Explaining Disaster Recovery and High Availability Concepts	Lesson 16: Identifying Site Policies and Best Practices
Lesson 19: Applying Network Hardening Techniques	Lesson 9: Explaining Networking Attacks and Mitigations
Lesson 20: Summarizing Cloud and Datacenter Architecture	Lesson 7: Explaining Network Application and Storage Issues

Activity Design Changes

Hands-on activities for *The Official CompTIA Network+ (Exam N10-008)* courses are available as a CertMaster Labs option. CertMaster Labs use a virtualized environment hosted by Learn on Demand Systems. Compared to the previous CompTIA Labs offering, CertMaster Labs are designed for assessment, enabling students to have their success in lab tasks graded and scored upon completion. CertMaster Labs can be integrated with CertMaster Learn, providing single sign-on to a one learning platform where learning and hands-on tasks can take place with a single grade reporting and analysis interface.

Assessment Mechanisms

CertMaster Labs are graded using two different mechanisms:

- Application (or task completion) is verified by running a script in the environment to ensure that the student has implemented the required configuration.
- Recollection, understanding, analysis, and evaluation is verified through multiple choice and short answer assessment items.

Assisted and Applied Lab Instruction Styles

Two complementary lab instruction styles give students a balanced learning experience:

- Assisted labs provide detailed steps with graded assessment and feedback for the completion of each lab task. Assisted labs are focused on one or two tasks related to content at the topic level and are designed for a 10-20 minute duration. In an assisted lab, students are free to change their responses and re-try tasks to improve their score.
- Applied labs provide students with a series of goal-oriented scenarios with graded assessment and feedback, but without detailed steps. Applied labs are designed as longer (30-40 minute) summary activities covering multiple lessons. In an applied lab, students cannot change their responses once submitted.

Integrated CertMaster Learn Launch and Reporting Solution

CertMaster Labs can be used either in instructor-led or self-paced training environments. Courses can be purchased on the CompTIA Store or distributed in a variety of ways through the LODS platform. We are also offering an integrated solution where CertMaster Labs are deployed through CertMaster Learn courses. When purchased together in a bundle, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan. As a result, learners experience both knowledge acquisition and hands-on skills attainment through a single login and seamless workflow. Additionally, organizations who purchase the integrated course will be able to review student and group lab scores in the CertMaster Learn Boost Dashboard and hold students accountable for lab work.

Course Setup Changes

As a result of these improvements, there is no scope to provide build instructions or steps for classroom-delivered lab activities. On-premises labs are not supported in the 008 courseware. Also, no printed or separate lab steps will be available—students must follow the steps and complete the grading activities within the lab platform.

Extensive review and discussion activities are provided for each topic. As always, sample responses for students are found in the Solutions section in the back of the student guide.

The CompTIA Learning Center

As with the 007 course, the 008 courseware is supported by additional resources available through the CompTIA Learning Center. The CompTIA Learning Center is an intuitive online platform that provides access to the eBook and all accompanying resources to support The Official CompTIA curriculum. An access key to the CompTIA Learning Center is delivered upon purchase of the print or eBook. Resources include:

- **Online Reader:** An interactive online reader provides the ability to search, highlight, take notes, and bookmark passages in the eBook. Users can also access the eBook through the CompTIA eReader mobile app.
- **Resources:** Supporting materials for instructors are available for downloading from the Resources menu. In addition to course-specific delivery tips, and solutions to activities and discussion questions, instructors also have access to:
 - **PowerPoint Slides:** A complete set of PowerPoint slides is provided to facilitate the class, including lists, tables, diagrams, illustrations, and annotated screens, as well as Activity summaries.
 - **Presentation Planners:** Several Presentation Planners are provided in the Resources menu. The Planners help the instructor plan the class schedule and include examples of schedules for different course lengths, whether courses are continuous or offered separately across a multisession series.
- **Videos:** Brief videos supplement key topics in the course.
- **Assessments:** Practice questions help to verify a student's understanding of the material for each Lesson. Answers and feedback can be reviewed after each question, or at the end of the assessment. A timed Final Assessment provides a practice-test-like experience to help students determine their readiness for the CompTIA certification exam. Students can review correct answers and full feedback after attempting the Final Assessment.
- **Strengths and Weaknesses Dashboard:** After a student has attempted the assessments within the platform, their results are aggregated in the Strengths and Weaknesses dashboard to provide an indicator of their overall performance in the course.

The CompTIA Learning Center can be accessed at learn.comptia.org.