INTRODUCTION

The CompTIA CTP+ examination certifies that the successful candidate has the necessary knowledge to perform basic requirements analysis, and specify, implement and manage basic components of data, voice and multimedia convergence applications and understand basic problem analysis and resolution for converged technologies. The CTP exam validates that an individual has the core knowledge and skills required by equipment manufacturers, their channel partners, and end-users to sell and service convergence technologies.
The CTP exam is quite rigorous. It certifies professional-level knowledge in three knowledge domains essential to the industry: Data networking, Telephony networking, and Convergence networking.

It is recommended that a typical candidate have CompTIA Network+ certification or equivalent knowledge, though CompTIA Network+ certification is not a prerequisite in order to take the CompTIA CTP+ certification exam. In addition, candidates are encouraged to have 18 to 24 months of work experience in areas that include data networking, telephony, and other convergence related technologies.

This examination blueprint includes domain weighting, test objectives, and sample content.

Candidates are encouraged to use this document to guide their studies. The contents of the examination blueprint help prioritize topics and provide a guide of what to expect on this exam. The table below lists the domains measured by this examination and the extent to which they are represented.

Domain	% of Examination
1. Data and Internet Protocol (IP) Networking for Convergent Networks	45%
2. Voice and Telephone Services, Functions and Technologies	15%
3. Convergence Technologies	40%
Total	**100%**

**Note: The bulleted lists below each objective are not exhaustive lists. Even though they are not included in this document, other examples of technologies, processes or tasks pertaining to each objective may also be included on the exam.

CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

Domain 1 Data and Internet Protocol (IP) Networking for Convergent Networks

1.1 Relate networking models and standards to convergence networking practices.

- Identify the major industry bodies and standards (e.g., International Telecommunication Union [ITU], International Organization for Standardization [ISO], Internet Engineering Task Force [IETF], Internet Society [ISOC], Internet Architecture Board [IAB], Electronic Industries Alliance [EIA], Telecommunications Industry Association [TIA]), and obtain and read standards documents.
- Identify the layers of the Open Systems Interconnection reference model (OSI/RM), and describe the function of each layer.
- Relate networking and convergence protocols, services and equipment to each OSI/RM layer.
- Relate common networking and convergence protocols, services and equipment to each of the four layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) model.
- Explain data encapsulation (e.g., data, segment, packet, frame) in relation to frame assembly and function on the network.

1.2 Identify appropriate local area network/wide area network (LAN/WAN) infrastructures.

- Define common network topologies (e.g., star, full mesh, partial mesh, wireless mesh, point-to-point, core, edge) and identify structured cable distribution schemes (e.g., floor, building, campus distributors/cross-connections, wiring closets).
- Identify the functions of routers, switches, firewalls, core and edge networks, modems (analog/cable/digital subscriber line [DSL]) and hubs in relation to data networking hardware, including the function of switches in Voice-over-IP (VoIP) implementations.
- Define networking methods, standards and protocols, and their characteristics (e.g., peer-to-peer, 802.3, Point-to-Point Protocol [PPP], Point-to-Point Protocol over Ethernet [PPPoE], frame relay, asynchronous transfer mode [ATM]).
- Define the Spanning Tree Protocol (STP), including 802.1d, GARP VLAN Registration Protocol (GVRP), Rapid Spanning Tree Protocol (RSTP).
- Define and contrast data communications equipment (DCE) and data terminating equipment (DTE).

- Identify network media (e.g., wireless/satellite, Category 5/5e, 6 and 7, shielded twisted pair [STP], fiber optic [single mode, multimode]), and identify proper cabling procedures in specific environments (e.g., PVC vs. fire-resistant, improper cable bending, cable run protection).
- Identify cable terminators (e.g., RJ-45, RJ-11, Amphenol, V.24, other RJ-nn and ITU/V.nnn standards).
- Compare and contrast straight-through, crossover, rolled and null-modem cabling.
- Explain the concept of protocol tunneling, and identify elements and benefits of using a Virtual Private Network (VPN) in a convergent network, including IPsec (tunnel and transport modes), Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), potential issues with VPN clients.
- Define unicasting, broadcasting, multicasting and anycasting.
- Explain the format and function of Media Access Control (MAC) addresses, including relevance to converged networks (e.g., Quality of Service [QoS], hunt groups).
- Compare and contrast the use of E-carrier, T-carrier, Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) and Integrated Services Digital Network (ISDN) technologies for data and voice networks, including bandwidths of common technologies.

1.3 Plan an Internet Protocol (IP) network.

- Determine which Internet Protocol (IP) version to implement (e.g., IPv4 vs. IPv6).
- Compare and contrast the IPv4 and IPv6 address formats.
- Identify network, host and broadcast addresses.
- Explain private network addressing, including benefits and drawbacks in a converged network.
- Identify the importance of the subnet mask, including custom subnetting.
- Determine the number of host addresses in a subnet.
- Determine the network address/number when given a host address and subnet mask.
- Identify the subnet mask by bit count and by dotted decimal notation, and define Classless Interdomain Routing (CIDR).

- Define common internal and external routing protocols (e.g., distance vector, link-state, Routing Information Protocol [RIP/RIP2], Open Shortest Path First [OSPF], Border Gateway Protocol [BGP], Exterior Gateway Protocol [EGP], Internet Group Management Protocol [IGMP], Interior Gateway Routing Protocol [IGRP], Enhanced IGRP [EIGRP]), and distinguish between internal and external routing protocol functions.
- Explain dynamic, static and default routes, and describe the function of routing tables.
- Identify Domain Name System (DNS) features and functions (e.g., hierarchical model, zones, use of User Datagram Protocol [UDP] and Transmission Control Protocol [TCP], primary/master and secondary/slave servers, zone transfers, DNS Security [DNSSEC], convergence-specific options such as SRV and NAPTR record entries).
- Explain Network Address Translation (NAT), including address translation tables, different types of NAT (e.g., Port Address Translation [PAT], static, dynamic), and NAT issues in convergent networks.
- Explain functions and benefits of automatic addressing (e.g., Dynamic Hardware Configuration Protocol [DHCP], Automatic Private IP Addressing [APIPA], BOOTstrap Protocol [BOOTP]), including protocol steps (e.g., discover, offer, request, acknowledgment, renewal), and troubleshooting handsets, PCs and all IP-enabled devices.
- Compare and contrast connection-oriented and connectionless transport, including TCP handshake, sequence number, maximum segment size, maximum transmission unit (MTU), checksum, benefits and drawbacks of each transport type.
- Define and identify well-known, registered and random/dynamic ports.
- Identify common ports and services, especially foundational services, including Secure Shell (SSH), Hypertext Transfer Protocol (HTTP), Domain Name System (DNS), Network Time Protocol (NTP), Lightweight Directory Access Protocol (LDAP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP3), Simple Network Management Protocol (SNMP) (v1, v2 and v3 with Remote Monitoring [RMON]), Web-based configuration service ports and utilities, and Telnet.
- Describe the impact of proxies on convergent network communications.

1.4 Describe wireless networks.

- Identify wireless networking equipment functionality and standards (e.g., Direct Sequence Spread Spectrum [DSSS], Global System for Mobile communications

[GSM], benefits of dual-cell and Wireless Fidelity [WiFi] phones, Code Division Multiple Access [CDMA], General Packet Radio Service [GPRS]).

- Identify critical settings in an access point (AP).
- Describe wireless client settings, including authentication, encryption, preferred networks, channels.
- Explain the functions of Wired Equivalent Privacy (WEP), 802.11i/WiFi Protected Access (WPA) (home use and enterprise), 802.1x and Remote Authentication Dial-In User Service (RADIUS).
- Identify and describe common security issues inherent to wireless networks.

1.5 Troubleshoot convergent networks.

- Use the Internet Control Message Protocol (ICMP) to determine connectivity, including reading ping and traceroute output, describing ways that various equipment uses ICMP and UDP.
- Identify common configuration errors in IP devices.
- Explain the effects of Network Address Translation (NAT) and Port Address Translation (PAT) on convergence solutions such as Session Initiation Protocol (SIP), including workarounds and solutions (e.g., Simple Traversal of UDP through NAT [STUN], Universal Plug and Play (UPnP), Traversal Using Relay NAT [TURN], Application Layer Gateway [ALG]).
- List common troubleshooting steps (consulting professional sources [online, print]; determining root cause; distinguishing between hardware and software error; reading, creating and modifying logs; escalating issues).

1.6 Identify elements and benefits of a virtual LAN (VLAN).

- Describe fundamental VLAN functions, features and concepts, including collision domain, broadcast domain, 802.1p, 802.1q, tagged frames, VLAN frame formats, colors, VLAN/LAN membership/segmentation (e.g., port-based, MAC-based, protocol-based, authentication, dark fiber).
- Identify benefits of using a VLAN (e.g., separating voice, video and data; performance improvement; load balancing; traffic shaping and separation; topology independence; protocol management).
- Identify typical problems that occur without a VLAN (e.g., congestion, poor voice quality, dropped calls).

1.7 Define Quality of Service (QoS).

- Describe the need for Quality of Service (QoS) in converged networks, including identifying problems that occur without QoS (e.g., jitter, clipping, frame loss, delay, disordered packet delivery, dropped packets, corrupted packets).
- Identify Quality of Service (QoS) technologies (e.g., Resource Reservation Protocol [RSVP], Differentiated Services [DiffServ], Multiprotocol Label Switching [MPLS], 802.1p, 802.1q, 802.1d, queuing, Integrated Services [IntServ]), describe network neutrality issues, and identify proprietary and open-source solutions.
- Compare and contrast best-effort delivery and QoS with traffic shaping.
- Compare and contrast QoS with Class of Service (CoS).
- Describe the Type of Service (TOS) field in an IP packet.
- Summarize the importance of QoS to real-time solutions, such as voice calls and video teleconferencing.
- Explain the roles of 802.1p, 802.1q and 802.1d when providing QoS, including implementation of traffic shaping using VLANs or protocols.
- Describe QoS on wireless networks (802.11e), including Wireless Multimedia Extensions (WME)/WiFi Multimedia (WMM).

Domain 2 Voice and Telephony Services, Functions and Technologies

2.1 Define codecs and Pulse Code Modulation (PCM).

- Define codec, and describe the G.711 protocol.
- Define Pulse Code Modulation (PCM), and distinguish between the μ-Law and A-Law companding algorithms.

2.2 Define Integrated Services Digital Network (ISDN) elements and concepts.

- Identify basic ISDN services and protocols, including time slots, channels, ISDN2e/Basic Rate Interface (BRI), ISDN30/Primary Rate Interface (PRI).
- Define the Q.931, Q.932, I.430 and Q.921/High-level Data Link Control (HDLC) standards, including identifying the typical call progress signals (e.g., alerting, call proceeding, etc.).
- Define Signaling System 7 (SS7)/Common Channel Signaling 7 (C7) functions, including call setup, management and teardown; signaling links; signaling

points (e.g., service switching point [SSP], signal transfer point [STP], service control point [SCP]).

- Define QSIG, H.450 (including supplementary services), Digital Access Signaling System 1 (DASS1), private networking, and Digital Private Network Signaling System (DPNSS).

2.3 Identify common voice services and feature sets.

- Explain common feature sets for voice calls, including call waiting, call blocking, call forwarding, call monitoring, callback, and additional private network features.
- Explain Direct Inward Dialing (DID).
- Define hunt groups.
- Identify elements of a call center or contact center, including call routing, caller ID, automatic call distributors, pop-ups, instant messaging/chat, e-mail, real-time voice and data recording/storage, hosted solutions, and elements of Computer Telephony Integration (CTI).

2.4 Identify and troubleshoot problems with voice calls in digital and analog environments.

- Identify and use appropriate troubleshooting tools (e.g., four-pair tester, tone-and-probe kit, analog and/or digital butt set, volt meter, time domain reflectometer).
- Identify symptoms of improper clocking configuration (e.g., problems with synchronization).
- Identify safety procedures for working with convergent network equipment (e.g., power, proper grounding, electrostatic discharge [ESD], radio frequency interference [RFI], electromagnetic interference [EMI]).
- Resolve problems when connecting time division multiplexing (TDM) networks (e.g., in-band and out-of-band signaling, digital and analog setup messages, safety practices and standards, crosstalk, split, line imbalance, open, short, grounding issues, echo cancellation in two-wire-to-four-wire hybrids).
- Explain the purpose of network termination equipment (NTE), including timing, conversion of signaling types, troubleshooting interface.

Domain 3 Convergence Technologies

3.1 Identify essential elements of a convergent network.

- List essential steps for qualifying a network's ability to support convergence (e.g., cable inspection, existing and maximum device capacity, replacing hubs with switches, Power over Ethernet [PoE] requirements, VLAN creation, conducting network reconnaissance).
- Compare and contrast circuit-switched and packet-switched technologies, including ways that packets traverse multiple WAN links, and call and call flow descriptions.
- Describe the features of Telephony Application Programming Interface (TAPI) and Messaging Application Programming Interface (MAPI) in a converged solution.
- Implement Telephone Number Mapping (ENUM), elements of global and private numbering plans, Local Number Portability (LNP)/Wireless LNP, end-point addressing, path selection, calling classes, digit manipulation, overlapping number ranges.
- Identify common G.7xx codecs and their bandwidth requirements in a converged environment (e.g., G.711, G.729, G.729a, G.726 and others).
- Describe the impact of compression on voice quality, and identify issues involved when converting voice to analog and digital formats.
- Identify benefits and drawbacks of various codecs in relation to bandwidth and voice quality.
- Calculate and estimate bandwidth usage for various codecs, including considerations of overhead, connection quality, and other factors that affect theoretical calculations (e.g., capacity planning, choosing connection speeds).
- Recommend codecs for use with local/in-network/within-LAN calls, and for across WAN connections.
- Explain wireless convergence technologies, including Digital Enhanced Cordless Telecommunications (DECT) and DECT layers, Personal Wireless Telephone (PWT), Generic Access Profile (GAP), expected ranges for interference-free communication, and the MHz ranges for each standard.
- Identify the features, benefits, problems and management of presencing, including single sign-on, features available in various devices.

3.2 Identify requirements for transporting text, voice, video, modem and fax through a converged solution.

- Explain store-and-forward faxing, according to standards such as ITU T.37.
- Explain real-time faxing, according to standards such as ITU T.38.

- List unified message methods and benefits (e.g., fax, voice, text, video).

3.3 Identify methods for providing video services through a converged solution.

- Identify common and essential videoconferencing codecs, standards and practices (e.g., Moving Picture Experts Group [MPEG], Quarter Common Intermediate Format [QCIF], etc.), and choose the appropriate codecs for various bandwidths.
- Summarize television/video-calling standards and practices.
- Identify multimedia conferencing standards, including all subsets of T.120 (e.g., T.123, T.124, T.135).
- Explain fundamentals of Internet Protocol television (IPTV), including set-top box, Video on Demand, accepted codecs (e.g., Video Codec [VC-1]).

3.4 Explain how protocols such as Realtime Transport Protocol (RTP), Realtime Transport Control Protocol (RTCP), Session Initiation Protocol (SIP), H.323 and Media Gateway Control (Megaco) are used to carry and control convergent network traffic.

- Identify the functions of signaling protocols for converged networks (e.g., Session Initiation Protocol [SIP], H.323, H.225, H.320, H.450, Media Gateway Control Protocol [MGCP], Media Gateway Control [Megaco]).
- Identify the components of Session Initiation Protocol (SIP) and describe the format of an SIP Uniform Resource Identifier (URI).
- Compare and contrast SIP, H.323 and Megaco/MGCP.
- Compare and contrast the functions of gatekeepers, gateways and proxies in relation to SIP and H.323 devices.
- Define the Realtime Transport Protocol (RTP) and the Realtime Transport Control Protocol (RTCP).
- Identify the elements of the IP Multimedia Subsystem (IMS).

3.5 Identify common convergence devices.

- Explain power issues, including redundancy planning, Power over Ethernet (PoE)/802.3af, PoE classes, expected voltage, wattage, power sourcing equipment (PSE), powered devices (PDs).
- Identify the purpose and function of voice and videoconferencing hardware (e.g., Multipoint Control Unit [MCU], set-top box, Session Border Controller [SBC]).

- Compare and contrast traditional and IP-based private branch exchange (PBX) systems.
- Identify convergent terminal equipment and software, including analog telephone adapter (ATA), single line adapter, soft phones (WiFi, PDA, PC-based), analog phones, time division multiplexer (TDM), protocol-specific handsets (e.g., SIP, Megaco).

3.6 **Troubleshoot common convergence technology.**

- Define latency, jitter and wander.
- Implement methods for reducing or eliminating latency, jitter and wander (e.g., implementing a jitter buffer, implementing QoS, traffic shaping, VLANs).
- Explain the impact of large frames on real-time communications.
- Identify factors that affect the bandwidth of voice and video calls on convergent networks (e.g., latency, protocol incompatibility, MTU, codec choice, compression, QoS issues, packet reordering, loss of feature set).
- Identify problems in contacting emergency services through convergent networks.
- Use accepted industry standards such as the Mean Opinion Score (MOS) to determine voice and video quality, including MOS for popular codecs, standard MOS numbers, R-value and subjective video quality.
- Identify common network bottlenecks in convergent networks, including solutions (e.g., monitoring network devices and protocols, creating a baseline, changing configuration, upgrading hardware).
- Analyze traffic in a convergent network and resolve problems using a packet sniffer, monitoring software, and hardware solutions.
- Troubleshoot convergent communications over wireless networks.
- Parse a Call Detail Record (CDR) and list relevant entries.

3.7 Identify security issues for converged networks.

- Explain the practice and impact of VLAN hopping.
- Define denial-of-service (DOS) and distributed DOS (DDOS) attacks, and identify ways to counteract them, including common traffic types used (e.g., SYN, UDP or ICMP flood), reconfiguring core upstream routers, using alternative sites, intentional and unintentional DOS.

- Identify types of intrusion detection (e.g., host-based, network-based, defining effective signatures, proactive detection).
- Explain the significance and impact of MAC address movements, additions and changes.
- Back up, upgrade and scan systems to thwart attacks, including backup types, system patches, service packs, firmware upgrades, optimal backup schedule.
- Identify types and effects of attacks in convergent networks, including man-in-the-middle attacks (e.g., packet sniffing, TCP connection hijacking, registration hijacking), voice mail compromises, viruses, brute-force and dictionary attacks, zero-day attacks, illicit servers, toll fraud and unsolicited calls.