

# CompTIA Cheatsheet

## Essential guide for CompTIA certification success

This comprehensive cheatsheet provides quick reference to CompTIA certification paths, core concepts, key terminology, and study strategies, ideal for beginners and experienced IT professionals pursuing CompTIA credentials.

Core Certifications	Study Strategies	Key Concepts
A+, Network+, Security+ overview	Effective preparation methods	Essential technical knowledge
Exam Tips		Career Paths
Test-taking strategies		Certification progression routes

## CompTIA Certification Overview

### Core Certifications

Foundation certifications for IT career success.

<p><b># CompTIA A+ (220-1101, 220-1102)</b></p> <ul style="list-style-type: none"><li>- Hardware and mobile devices</li><li>- Operating systems and software</li><li>- Security and networking basics</li><li>- Operational procedures</li></ul>
<p><b># CompTIA Network+ (N10-008)</b></p> <ul style="list-style-type: none"><li>- Network fundamentals</li><li>- Network implementations</li><li>- Network operations</li><li>- Network security</li><li>- Network troubleshooting</li></ul>
<p><b># CompTIA Security+ (SY0-601)</b></p> <ul style="list-style-type: none"><li>- Attacks, threats, and vulnerabilities</li><li>- Architecture and design</li><li>- Implementation</li><li>- Operations and incident response</li><li>- Governance, risk, and compliance</li></ul>

### Specialized Certifications

Advanced and specialized IT credentials.

<p><b># CompTIA PenTest+ (PT0-002)</b></p> <ul style="list-style-type: none"><li>- Planning and scoping penetration tests</li><li>- Information gathering and vulnerability identification</li><li>- Attacks and exploits</li><li>- Reporting and communication</li></ul>
<p><b># CompTIA CySA+ (CS0-002)</b></p> <ul style="list-style-type: none"><li>- Threat and vulnerability management</li><li>- Software and systems security</li><li>- Security operations and monitoring</li><li>- Incident response</li><li>- Compliance and assessment</li></ul>

## CompTIA A+ Essentials

Core hardware, software, and troubleshooting concepts for IT support.

01	02	03
Hardware Components	Mobile Devices	Operating Systems

Essential computer hardware knowledge and troubleshooting.	Smartphones, tablets, and mobile device management.	Windows, macOS, Linux, and mobile OS management.
--	---	--

<p><b># CPU Types and Features</b></p> <ul style="list-style-type: none"><li>- Intel vs AMD processors</li><li>- Socket types (LGA, PGA, BGA)</li><li>- Core counts and threading</li><li>- Cache levels (L1, L2, L3)</li></ul>	<p><b># Mobile Device Types</b></p> <ul style="list-style-type: none"><li>- iOS vs Android architecture</li><li>- Laptop vs tablet form factors</li><li>- Wearable devices</li><li>- E-readers and smart devices</li></ul>	<p><b># Windows Administration</b></p> <ul style="list-style-type: none"><li>- Windows 10/11 editions</li><li>- User Account Control (UAC)</li><li>- Group Policy and Registry</li><li>- Windows Update management</li></ul>
<p><b># Memory (RAM)</b></p> <ul style="list-style-type: none"><li>- DDR4, DDR5 specifications</li><li>- ECC vs non-ECC memory</li><li>- SODIMM vs DIMM form factors</li><li>- Memory channels and speeds</li></ul>	<p><b># Mobile Connectivity</b></p> <ul style="list-style-type: none"><li>- Wi-Fi standards (802.11a/b/g/n/ac/ax)</li><li>- Cellular technologies (3G, 4G, 5G)</li><li>- Bluetooth versions and profiles</li><li>- NFC and mobile payments</li></ul>	<p><b># macOS Management</b></p> <ul style="list-style-type: none"><li>- System Preferences</li><li>- Keychain Access</li><li>- Time Machine backups</li><li>- App Store and Gatekeeper</li></ul>
<p><b># Storage Technologies</b></p> <ul style="list-style-type: none"><li>- HDD vs SSD vs NVMe</li><li>- SATA, PCIe interfaces</li><li>- RAID configurations (0,1,5,10)</li><li>- M.2 form factors</li></ul>	<p><b># Mobile Security</b></p> <ul style="list-style-type: none"><li>- Screen locks and biometrics</li><li>- Mobile device management (MDM)</li><li>- App security and permissions</li><li>- Remote wipe capabilities</li></ul>	<p><b># Linux Basics</b></p> <ul style="list-style-type: none"><li>- File system hierarchy</li><li>- Command line operations</li><li>- Package management</li><li>- User and group permissions</li></ul>

## Network+ Fundamentals

### OSI Model & TCP/IP

Network layer understanding and protocol knowledge.

<p><b># OSI 7-Layer Model</b></p> <p>Layer 7: Application (HTTP, HTTPS, FTP)</p> <p>Layer 6: Presentation (SSL, TLS)</p> <p>Layer 5: Session (NetBIOS, RPC)</p> <p>Layer 4: Transport (TCP, UDP)</p> <p>Layer 3: Network (IP, ICMP, OSPF)</p> <p>Layer 2: Data Link (Ethernet, PPP)</p> <p>Layer 1: Physical (Cables, Hubs)</p>
<p><b># TCP/IP Suite</b></p> <ul style="list-style-type: none"><li>- IPv4 vs IPv6 addressing</li><li>- Subnetting and CIDR notation</li><li>- DHCP and DNS services</li><li>- ARP and ICMP protocols</li></ul>

### Network Devices

Routers, switches, and networking equipment.

<p><b># Layer 2 Devices</b></p> <ul style="list-style-type: none"><li>- Switches and VLANs</li><li>- Spanning Tree Protocol (STP)</li><li>- Port security and MAC filtering</li></ul>
<p><b># Layer 3 Devices</b></p> <ul style="list-style-type: none"><li>- Routers and routing tables</li><li>- Static vs dynamic routing</li><li>- OSPF, EIGRP, BGP protocols</li><li>- NAT and PAT translation</li></ul>

## Security+ Core Concepts

### Security Fundamentals

CIA triad and basic security principles.

<p><b># CIA Triad</b></p> <p>Confidentiality: Data privacy and encryption</p> <p>Integrity: Data accuracy and authenticity</p> <p>Availability: System uptime and accessibility</p>
<p><b># Authentication Factors</b></p> <p>Something you know: Passwords, PINs</p> <p>Something you have: Tokens, smart cards</p> <p>Something you are: Biometrics</p> <p>Something you do: Behavior patterns</p> <p>Somewhere you are: Location-based</p>

### Threat Landscape

Common attacks and threat actors.

<p><b># Attack Types</b></p> <ul style="list-style-type: none"><li>- Phishing and social engineering</li><li>- Malware (viruses, trojans, ransomware)</li><li>- DDoS and DoS attacks</li><li>- Man-in-the-middle attacks</li><li>- SQL injection and XSS</li><li>- Zero-day exploits</li></ul>
<p><b># Threat Actors</b></p> <ul style="list-style-type: none"><li>- Script kiddies</li><li>- Hacktivists</li><li>- Organized crime</li><li>- Nation-state actors</li><li>- Insider threats</li></ul>

## Study Strategies & Tips

Effective methods for CompTIA certification preparation.

### Study Planning

Create a structured approach to certification preparation.

<p><b># Study Schedule</b></p> <p>Week 1-2: Review exam objectives</p> <p>Week 3-6: Core material study</p> <p>Week 7-8: Hands-on practice</p> <p>Week 9-10: Practice exams</p> <p>Week 11-12: Final review and exam</p>
<p><b># Study Materials</b></p> <ul style="list-style-type: none"><li>- Official CompTIA study guides</li><li>- Video training courses</li><li>- Practice exams and simulators</li><li>- Hands-on lab exercises</li><li>- Study groups and forums</li></ul>

### Hands-On Practice

Practical experience to reinforce theoretical knowledge.

<p><b># Lab Environments</b></p> <ul style="list-style-type: none"><li>- VMware or VirtualBox VMs</li><li>- Home lab setup</li><li>- Cloud-based labs (AWS, Azure)</li><li>- CompTIA simulation software</li></ul>
<p><b># Practical Skills</b></p> <ul style="list-style-type: none"><li>- Building and troubleshooting PCs</li><li>- Network configuration</li><li>- Security tool implementation</li><li>- Command line proficiency</li></ul>

## Technical Acronyms & Terminology

Essential CompTIA acronyms and technical terms.

### Networking Acronyms

Common networking terms and abbreviations.

<p><b># Protocols &amp; Standards</b></p> <p>HTTP/HTTPS: Web protocols</p> <p>FTP/SFTP: File transfer</p> <p>SMTP/POP3/IMAP: Email</p> <p>DNS: Domain Name System</p> <p>DHCP: Dynamic Host Configuration</p> <p>TCP/UDP: Transport protocols</p> <p>IP: Internet Protocol</p> <p>ICMP: Internet Control Message</p>
<p><b># Wireless &amp; Security</b></p> <p>WPA/WPA2: Wi-Fi Protected Access</p> <p>SSID: Service Set Identifier</p> <p>MAC: Media Access Control</p> <p>VPN: Virtual Private Network</p> <p>VLAN: Virtual Local Area Network</p> <p>QoS: Quality of Service</p>

### Hardware & Software

Computer hardware and software terminology.

<p><b># Storage &amp; Memory</b></p> <p>HDD: Hard Disk Drive</p> <p>SSD: Solid State Drive</p> <p>RAM: Random Access Memory</p> <p>ROM: Read-Only Memory</p> <p>BIOS/UEFI: System firmware</p> <p>RAID: Redundant Array of Independent Disks</p>
<p><b># Interfaces &amp; Ports</b></p> <p>USB: Universal Serial Bus</p> <p>SATA: Serial ATA</p> <p>PCIe: Peripheral Component Interconnect Express</p> <p>HDMI: High-Definition Multimedia Interface</p> <p>VGA: Video Graphics Array</p> <p>RJ45: Ethernet connector</p>

## Certification Career Paths

Strategic progression through CompTIA certifications.

1	2
<p><b>Entry Level</b></p> <p><b>CompTIA A+</b></p> <p>Foundation certification for IT support roles, covering hardware, software, and basic troubleshooting skills.</p>	<p><b>Infrastructure</b></p> <p><b>Network+ &amp; Server+</b></p> <p>Build networking and server administration expertise for infrastructure roles.</p>
3	4
<p><b>Security Focus</b></p> <p><b>Security+ &amp; CySA+</b></p> <p>Develop cybersecurity knowledge for security analyst and administrator positions.</p>	<p><b>Specialization</b></p> <p><b>PenTest+ &amp; Cloud+</b></p> <p>Advanced specializations in penetration testing and cloud technologies.</p>

## Common Port Numbers

Essential port numbers for CompTIA Network+ and Security+ exams.

### Well-Known Ports (0-1023)

Standard ports for common network services.

<p><b># Web &amp; File Transfer</b></p> <p>Port 20/21: FTP (File Transfer Protocol)</p> <p>Port 22: SSH (Secure Shell)</p> <p>Port 23: Telnet</p> <p>Port 25: SMTP (Simple Mail Transfer Protocol)</p> <p>Port 53: DNS (Domain Name System)</p> <p>Port 67/68: DHCP (Dynamic Host Configuration)</p> <p>Port 69: TFTP (Trivial File Transfer Protocol)</p> <p>Port 80: HTTP (Hypertext Transfer Protocol)</p> <p>Port 110: POP3 (Post Office Protocol v3)</p> <p>Port 143: IMAP (Internet Message Access Protocol)</p> <p>Port 161/162: SNMP (Simple Network Management)</p> <p>Port 443: HTTPS (HTTP Secure)</p> <p>Port 993: IMAPS (IMAP Secure)</p> <p>Port 995: POP3S (POP3 Secure)</p>
---

## Troubleshooting Methodologies

Systematic approaches to problem-solving in IT environments.

### CompTIA Troubleshooting Steps

Standard methodology for technical problem resolution.

<p><b># 6-Step Process</b></p> <p>1. Identify the problem</p> <ul style="list-style-type: none"><li>- Gather information</li><li>- Question users about symptoms</li><li>- Identify changes to system</li><li>- Duplicate problem if possible</li></ul> <p>2. Establish a theory of probable cause</p> <ul style="list-style-type: none"><li>- Question the obvious</li><li>- Consider multiple approaches</li><li>- Start with simple solutions</li></ul> <p>3. Test the theory to prove cause</p> <ul style="list-style-type: none"><li>- If the theory confirmed, proceed</li><li>- If not, establish new theory</li><li>- Escalate if necessary</li></ul>
---

## Performance-Based Question Tips

Strategies for CompTIA simulation and hands-on questions.

### A+ Performance Questions

Common simulation scenarios and solutions.

<p><b># Hardware Troubleshooting</b></p> <ul style="list-style-type: none"><li>- Identify failed components in PC builds</li><li>- Configure BIOS/UEFI settings</li><li>- Install and configure RAM</li><li>- Connect storage devices properly</li><li>- Troubleshoot power supply issues</li></ul>
<p><b># Operating System Tasks</b></p> <ul style="list-style-type: none"><li>- Windows installation and configuration</li><li>- User account and permission management</li><li>- Network settings configuration</li><li>- Device driver installation</li><li>- System file and registry repairs</li></ul>

### Network+ Simulations

Network configuration and troubleshooting scenarios.

<p><b># Network Configuration</b></p> <ul style="list-style-type: none"><li>- VLAN setup and port assignments</li><li>- Router ACL configuration</li><li>- Switch port security settings</li><li>- Wireless network setup</li><li>- IP addressing and subnetting</li></ul>
<p><b># Troubleshooting Tasks</b></p> <ul style="list-style-type: none"><li>- Cable testing and replacement</li><li>- Network connectivity diagnosis</li><li>- DNS and DHCP troubleshooting</li><li>- Performance optimization</li><li>- Security implementation</li></ul>

## Exam Registration & Logistics

<p><b>Exam Registration Process</b></p> <p>Steps to schedule and prepare for CompTIA exams.</p>
---

<p><b># Registration Steps</b></p> <ol style="list-style-type: none"><li>1. Create Pearson VUE account</li><li>2. Select certification exam</li><li>3. Choose testing center or online option</li><li>4. Schedule exam date and time</li><li>5. Pay exam fee</li><li>6. Receive confirmation email</li></ol>
<p><b># Exam Costs (USD, approximate)</b></p> <p>CompTIA A+: \$239 per exam (2 exams)</p> <p>CompTIA Network+: \$358</p> <p>CompTIA Security+: \$370</p> <p>CompTIA Cloud+: \$358</p> <p>CompTIA PenTest+: \$370</p> <p>CompTIA CySA+: \$392</p>

<p><b>Test Day Preparation</b></p> <p>What to expect and bring on exam day.</p>
---

<p><b># Required Items</b></p> <ul style="list-style-type: none"><li>- Valid government-issued photo ID</li><li>- Confirmation email/number</li><li>- Arrive 30 minutes early</li><li>- No personal items in testing room</li></ul>
<p><b># Exam Format</b></p> <ul style="list-style-type: none"><li>- Multiple choice questions</li><li>- Performance-based questions (simulations)</li><li>- Drag-and-drop questions</li><li>- Hot spot questions</li><li>- Time limits vary by exam (90-165 minutes)</li></ul>

<p><b># Certification Validity</b></p> <p>Most CompTIA certifications: 3 years</p> <p>CompTIA A+: Permanent (no expiration)</p>
<p><b># Continuing Education Units (CEUs)</b></p> <p>Security+: 50 CEUs over 3 years</p> <p>Network+: 30 CEUs over 3 years</p> <p>Cloud+: 30 CEUs over 3 years</p>
<p><b># CEU Activities</b></p> <ul style="list-style-type: none"><li>- Training courses and webinars</li><li>- Industry conferences</li><li>- Publishing articles</li><li>- Volunteering</li><li>- Higher-level certifications</li></ul>

<p><b># Incident Response</b></p> <ul style="list-style-type: none"><li>- Log analysis and interpretation</li><li>- Threat identification</li><li>- Vulnerability assessment</li><li>- Security control implementation</li><li>- Risk mitigation strategies</li></ul>
---

<p><b># Success Strategies</b></p> <ul style="list-style-type: none"><li>- Read instructions carefully and completely</li><li>- Take screenshots before making changes</li><li>- Test configurations after implementing</li><li>- Use process of elimination</li><li>- Manage time effectively</li><li>- Practice with simulation software</li><li>- Understand underlying concepts, not just steps</li></ul>
---

<p><b>General Simulation Tips</b></p> <p>Best practices for performance-based questions.</p>
--

<p><b>Career Benefits</b></p> <p>Value and recognition of CompTIA certifications.</p>
---

<p><b>Certification Maintenance</b></p> <p>Continuing education and certification renewal.</p>
--

<p><b>Security+ Scenarios</b></p> <p>Security implementation and incident response.</p>
---

<p><b>Security Configuration</b></p> <ul style="list-style-type: none"><li>- Firewall rule creation</li><li>- User access control setup</li><li>- Certificate management</li><li>- Encryption implementation</li><li>- Network segmentation</li></ul>
<p><b>Incident Response</b></p> <ul style="list-style-type: none"><li>- Log analysis and interpretation</li><li>- Threat identification</li><li>- Vulnerability assessment</li><li>- Security control implementation</li><li>- Risk mitigation strategies</li></ul>

<p><b>Network+ Scenarios</b></p> <p>Network configuration and troubleshooting scenarios.</p>
--

<p><b>Network Configuration</b></p> <ul style="list-style-type: none"><li>- VLAN setup and port assignments</li><li>- Router ACL configuration</li><li>- Switch port security settings</li><li>- Wireless network setup</li><li>- IP addressing and subnetting</li></ul>
<p><b>Troubleshooting Tasks</b></p> <ul style="list-style-type: none"><li>- Cable testing and replacement</li><li>- Network connectivity diagnosis</li><li>- DNS and DHCP troubleshooting</li><li>- Performance optimization</li><li>- Security implementation</li></ul>

<p><b>Exam Registration &amp; Logistics</b></p> <p>Steps to schedule and prepare for CompTIA exams.</p>
---

<p><b>Registration Steps</b></p> <ol style="list-style-type: none"><li>1. Create Pearson VUE account</li><li>2. Select certification exam</li><li>3. Choose testing center or online option</li><li>4. Schedule exam date and time</li><li>5. Pay exam fee</li><li>6. Receive confirmation email</li></ol>
<p><b>Exam Costs (USD, approximate)</b></p> <p>CompTIA A+: \$239 per exam (2 exams)</p> <p>CompTIA Network+: \$358</p> <p>CompTIA Security+: \$370</p> <p>CompTIA Cloud+: \$358</p> <p>CompTIA PenTest+: \$370</p> <p>CompTIA CySA+: \$392</p>

<p><b>Test Day Preparation</b></p> <p>What to expect and bring on exam day.</p>
---

<p><b>Required Items</b></p> <ul style="list-style-type: none"><li>- Valid government-issued photo ID</li><li>- Confirmation email/number</li><li>- Arrive 30 minutes early</li><li>- No personal items in testing room</li></ul>
<p><b>Exam Format</b></p> <ul style="list-style-type: none"><li>- Multiple choice questions</li><li>- Performance-based questions (simulations)</li><li>- Drag-and-drop questions</li><li>- Hot spot questions</li><li>- Time limits vary by exam (90-165 minutes)</li></ul>

<p><b>Certification Validity</b></p> <p>Most CompTIA certifications: 3 years</p> <p>CompTIA A+: Permanent (no expiration)</p>
<p><b>Continuing Education Units (CEUs)</b></p> <p>Security+: 50 CEUs over 3 years</p> <p>Network+: 30 CEUs over 3 years</p> <p>Cloud+: 30 CEUs over 3 years</p>
<p><b>CEU Activities</b></p> <ul style="list-style-type: none"><li>- Training courses and webinars</li><li>- Industry conferences</li><li>- Publishing articles</li><li>- Volunteering</li><li>- Higher-level certifications</li></ul>

<p><b>Incident Response</b></p> <ul style="list-style-type: none"><li>- Log analysis and interpretation</li><li>- Threat identification</li><li>- Vulnerability assessment</li><li>- Security control implementation</li><li>- Risk mitigation strategies</li></ul>
---

<p><b>Success Strategies</b></p> <ul style="list-style-type: none"><li>- Read instructions carefully and completely</li><li>- Take screenshots before making changes</li><li>- Test configurations after implementing</li><li>- Use process of elimination</li><li>- Manage time effectively</li><li>- Practice with simulation software</li><li>- Understand underlying concepts, not just steps</li></ul>
---

<p><b>General Simulation Tips</b></p> <p>Best practices for performance-based questions.</p>
--

<p><b>Career Benefits</b></p> <p>Value and recognition of CompTIA certifications.</p>
---

<p><b>Certification Maintenance</b></p> <p>Continuing education and certification renewal.</p>
--

<p><b>Security+ Scenarios</b></p> <p>Security implementation and incident response.</p>
---

<p><b>Security Configuration</b></p> <ul style="list-style-type: none"><li>- Firewall rule creation</li><li>- User access control setup</li><li>- Certificate management</li><li>- Encryption implementation</li><li>- Network segmentation</li></ul>
<p><b>Incident Response</b></p> <ul style="list-style-type: none"><li>- Log analysis and interpretation</li><li>- Threat identification</li><li>- Vulnerability assessment</li><li>- Security control implementation</li><li>- Risk mitigation strategies</li></ul>

<p><b>Network+ Scenarios</b></p> <p>Network configuration and troubleshooting scenarios.</p>
--

<p><b>Network Configuration</b></p> <ul style="list-style-type: none"><li>- VLAN setup and port assignments</li><li>- Router ACL configuration</li><li>- Switch port security settings</li><li>- Wireless network setup</li><li>- IP addressing and subnetting</li></ul>
<p><b>Troubleshooting Tasks</b></p> <ul style="list-style-type: none"><li>- Cable testing and replacement</li><li>- Network connectivity diagnosis</li><li>- DNS and DHCP troubleshooting</li><li>- Performance optimization</li><li>- Security implementation</li></ul>

<p><b>Exam Registration &amp; Logistics</b></p> <p>Steps to schedule and prepare for CompTIA exams.</p>
---

<p><b>Registration Steps</b></p> <ol style="list-style-type: none"><li>1. Create Pearson VUE account</li><li>2. Select certification exam</li><li>3. Choose testing center or online option</li><li>4. Schedule exam date and time</li><li>5. Pay exam fee</li><li>6. Receive confirmation email</li></ol>
<p><b>Exam Costs (USD, approximate)</b></p> <p>CompTIA A+: \$239 per exam (2 exams)</p> <p>CompTIA Network+: \$358</p> <p>CompTIA Security+: \$370</p> <p>CompTIA Cloud+: \$358</p> <p>CompTIA PenTest+: \$370</p> <p>CompTIA CySA+: \$392</p>

<p><b>Test Day Preparation</b></p> <p>What to expect and bring on exam day.</p>
---

<p><b>Required Items</b></p> <ul style="list-style-type: none"><li>- Valid government-issued photo ID</li><li>- Confirmation email/number</li><li>- Arrive 30 minutes early</li><li>- No personal items in testing room</li></ul>
<p><b>Exam Format</b></p> <ul style="list-style-type: none"><li>- Multiple choice questions</li><li>- Performance-based questions (simulations)</li><li>- Drag-and-drop questions</li><li>- Hot spot questions</li><li>- Time limits vary by exam (90-165 minutes)</li></ul>

<p><b>Certification Validity</b></p> <p>Most CompTIA certifications: 3 years</p> <p>CompTIA A+: Permanent (no expiration)</p>
<p><b>Continuing Education Units (CEUs)</b></p> <p>Security+: 50 CEUs over 3 years</p> <p>Network+: 30 CEUs over 3 years</p> <p>Cloud+: 30 CEUs over 3 years</p>
<p><b>CEU Activities</b></p> <ul style="list-style-type: none"><li>- Training courses and webinars</li><li>- Industry conferences</li><li>- Publishing articles</li><li>- Volunteering</li><li>- Higher-level certifications</li></ul>

<p><b>Incident Response</b></p> <ul style="list-style-type: none"><li>- Log analysis and interpretation</li><li>- Threat identification</li><li>- Vulnerability assessment</li><li>- Security control implementation</li><li>- Risk mitigation strategies</li></ul>
---

<p><b>Success Strategies</b></p> <ul style="list-style-type: none"><li>- Read instructions carefully and completely</li><li>- Take screenshots before making changes</li><li>- Test configurations after implementing</li><li>- Use process of elimination</li><li>- Manage time effectively</li><li>- Practice with simulation software</li><li>- Understand underlying concepts, not just steps</li></ul>
---

<p><b>General Simulation Tips</b></p> <p>Best practices for performance-based questions.</p>
--

<p><b>Career Benefits</b></p> <p>Value and recognition of CompTIA certifications.</p>
---

<p><b>Certification Maintenance</b></p> <p>Continuing education and certification renewal.</p>
--

<p><b>Security+ Scenarios</b></p> <p>Security implementation and incident response.</p>
---

<p><b>Security Configuration</b></p> <ul style="list-style-type: none"><li>- Firewall rule creation</li><li>- User access control setup</li><li>- Certificate management</li><li>- Encryption implementation</li><li>- Network segmentation</li></ul>
<p><b>Incident Response</b></p> <ul style="list-style-type: none"><li>- Log analysis and interpretation</li><li>- Threat identification</li><li>- Vulnerability assessment</li><li>- Security control implementation</li><li>- Risk mitigation strategies</li></ul>

<p><b>Network+ Scenarios</b></p> <p>Network configuration and troubleshooting scenarios.</p>
--

<p><b>Network Configuration</b></p> <ul style="list-style-type: none"><li>- VLAN setup and port assignments</li><li>- Router ACL configuration</li><li>- Switch port security settings</li><li>- Wireless network setup</li><li>- IP addressing and subnetting</li></ul>
<p><b>Troubleshooting Tasks</b></p> <ul style="list-style-type: none"><li>- Cable testing and replacement</li><li>- Network connectivity diagnosis</li><li>- DNS and DHCP troubleshooting</li><li>- Performance optimization</li><li>- Security implementation</li></ul>

<p><b>Exam Registration &amp; Logistics</b></p> <p>Steps to schedule and prepare for CompTIA exams.</p>
---

<p><b>Registration Steps</b></p> <ol style="list-style-type: none"><li>1. Create Pearson VUE account</li><li>2. Select certification exam</li><li>3. Choose testing center or online option</li><li>4. Schedule exam date and time</li><li>5. Pay exam fee</li><li>6. Receive confirmation email</li></ol>
<p><b>Exam Costs (USD, approximate)</b></p> <p>CompTIA A+: \$239 per exam (2 exams)</p> <p>CompTIA Network+: \$358</p> <p>CompTIA Security+: \$370</p> <p>CompTIA Cloud+: \$358</p> <p>CompTIA PenTest+: \$370</p> <p>CompTIA CySA+: \$392</p>

<p><b>Test Day Preparation</b></p> <p>What to expect and bring on exam day.</p>
---

<p><b>Required Items</b></p> <ul style="list-style-type: none"><li>- Valid government-issued photo ID</li><li>- Confirmation email/number</li><li>- Arrive 30 minutes early</li><li>- No personal items in testing room</li></ul>
<p><b>Exam Format</b></p> <ul style="list-style-type: none"><li>- Multiple choice questions</li><li>- Performance-based questions (simulations)</li><li>- Drag-and-drop questions</li><li>- Hot spot questions</li><li>- Time limits vary by exam (90-165 minutes)</li></ul>

<p><b>Certification Validity</b></p> <p>Most CompTIA certifications: 3 years</p> <p>CompTIA A+: Permanent (no expiration)</p>
<p><b>Continuing Education Units (CEUs)</b></p> <p>Security+: 50 CEUs over 3 years</p> <p>Network+: 30 CEUs over 3 years</p> <p>Cloud+: 30 CEUs over 3 years</p>
<p><b>CEU Activities</b></p> <ul style="list-style-type: none"><li>- Training courses and webinars</li><li>- Industry conferences</li><li>- Publishing articles</li><li>- Volunteering</li><li>- Higher-level certifications</li></ul>

<p><b>Incident Response</b></p> <ul style="list-style-type: none"><li>- Log analysis and interpretation</li><li>- Threat identification</li><li>- Vulnerability assessment</li><li>- Security control implementation</li><li>- Risk mitigation strategies</li></ul>
---

<p><b>Success Strategies</b></p> <ul style="list-style-type: none"><li>- Read instructions carefully and completely</li><li>- Take screenshots before making changes</li><li>- Test configurations after implementing</li><li>- Use process of elimination</li><li>- Manage time effectively</li><li>- Practice with simulation software</li><li>- Understand underlying concepts, not just steps</li></ul>
---

<p><b>General Simulation Tips</b></p> <p>Best practices for performance-based questions.</p>
--

<p><b>Career Benefits</b></p> <p>Value and recognition of CompTIA certifications.</p>
---

<p><b>Certification Maintenance</b></p> <p>Continuing education and certification renewal.</p>
--

<p><b>Security+ Scenarios</b></p> <p>Security implementation and incident response.</p>
---

<p><b>Security Configuration</b></p> <ul style="list-style-type: none"><li>- Firewall rule creation</li><li>- User access control setup</li><li>- Certificate management</li><li>- Encryption implementation</li><li>- Network segmentation</li></ul>
<p><b>Incident Response</b></p> <ul style="list-style-type: none"><li>- Log analysis and interpretation</li><li>- Threat identification</li><li>- Vulnerability assessment</li><li>- Security control implementation</li><li>- Risk mitigation strategies</li></ul>

<p><b>Network+ Scenarios</b></p> <p>Network configuration and troubleshooting scenarios.</p>
--

||
||
||