INTRODUCTION

The CompTIA Mobility+ certification is an internationally recognized validation of skills and knowledge required of IT practitioners working in mobile computing environments.

Test Purpose: The CompTIA Mobility+ Certification Exam will certify that the successful candidate has the knowledge and skills required to understand and research capabilities of mobile devices and features of over-the-air technologies. The successful candidate will also deploy, integrate, support and manage a mobile environment ensuring proper security measures are implemented for devices and platforms while maintaining usability.

Recommended Skills/Knowledge: It is recommended that CompTIA Mobility+ candidates to have the following:

- CompTIA Network+ or equivalent working knowledge.
- Have at least 18 months of work experience in administration of mobile devices in the enterprise.

The table below lists the domains measured by this examination and the extent to which they are represented.

<table>
<thead>
<tr>
<th>Domain</th>
<th>% of Examination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Over-the-Air Technologies</td>
<td>13%</td>
</tr>
<tr>
<td>2.0 Network Infrastructure</td>
<td>15%</td>
</tr>
<tr>
<td>3.0 Mobile Device Management</td>
<td>28%</td>
</tr>
<tr>
<td>4.0 Security</td>
<td>20%</td>
</tr>
<tr>
<td>5.0 Troubleshooting</td>
<td>24%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
CompTIA Authorized Materials Use Policy

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse or condone utilizing any content provided by unauthorized third-party training sites, aka 'brain dumps'. Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies webpage:
http://certification.comptia.org/Training/testingcenters/policies.aspx

Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement (http://certification.comptia.org/Training/testingcenters/policies/agreement.aspx) at the time of exam delivery.

If a candidate has a question as to whether study materials are considered unauthorized (aka brain dumps), he/she should perform a search using CertGuard's engine, found here:
http://www.certguard.com/search.asp

Or verify against this list:

**Note: The lists of examples provided in bulleted format below each objective are not exhaustive lists. Other examples of technologies, processes or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document.

*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.*

(A list of acronyms used in these objectives appears at the end of this document.)
1.0 Over-the-Air Technologies

1.1 Compare and contrast different cellular technologies

- CDMA
- TDMA
- GSM
  - Edge
  - GPRS
- WiMAX
- UMTS
- CSD
- EVDO
- HSPA
- HSPA+
- LTE
- Roaming & switching between network types

1.2 Given a scenario, configure and implement WiFi client technologies using appropriate options.

- Bluetooth
- PAN
- 802.11a, b, g, n, ac
  - Relevant operating frequencies and channels
- SSID
  - Broadcast/hidden system
- Authentication methods
- Portable hotspots

1.3 Compare and contrast RF principles and their functionality

- RF characteristics
  - Frequencies
  - Modulation
  - Bandwidth
  - Wavelength
  - Amplitude
  - Phase
- Propagation theory
  - Absorption
  - Refraction
  - Reflection
  - Attenuation
1.4 Interpret site survey to ensure over the air communication

- Capacity
- Coverage
- Signal strength
- Receive Signal Strength Indicator
- Spectrum analysis
- Frequency analysis
- Site survey documentation / site map
  - Wireless vs. cellular site survey
- Post-site survey

### 2.0 Network Infrastructure

#### 2.1 Compare and contrast physical and logical infrastructure technologies and protocols

- Topologies
  - Mesh
  - Point-to-point
  - Point-to-multipoint
  - Adhoc
- Firewall settings
  - Port configuration
  - Protocols
  - Filtering
  - DMZ
- Devices
  - Gateways
  - Proxies
  - VPN concentrator
  - Autonomous access points
  - Wireless LAN
2.2 Explain the technologies used for traversing wireless to wired networks.

- Bandwidth and user limitations
  - Backhauling traffic
  - QoS
  - Traffic shaping
- Hardware differences
- Traffic routing
- IP addressing
  - TCP
  - UDP
  - NAT
  - DNS
  - DHCP
- MAC address
- SNMP
- ICMP
- PoE for APs to switches

2.3 Explain the layers of the OSI model.

- Layer 1 – Physical
- Layer 2 – Data link
- Layer 3 – Network
- Layer 4 – Transport
- Layer 5 – Session
- Layer 6 – Presentation
- Layer 7 – Application

2.4 Explain disaster recovery principles and how it affects mobile devices.

- Server backups
- Device backups
- Directory services server
- Frequency of backups
- High availability
- DR locations
2.5 Compare and contrast common network ports and protocols for mobile devices

- 20/21 – FTP
- 22 – SFTP
- 23 – Telnet
- 25 – SMTP
- 53 – DNS
- 80 – HTTP
- 110 – POP3
- 135 – MAPI
- 143 – IMAP
- 389 – LDAP/AD
- 443 – SSL
- 465 – SMTP
- 587 – Alternate SMTP
- 990 – ftps
- 993 – IMAP over SSL
- 2175 – Airsync
- 2195 – APNS
- 2196 – Feedback
- 3389 – RDP
- 4101 – SRP
- 5223 – Jabber
- 5228-5230 – GCM

3.0 Mobile Device Management

3.1 Explain policy required to certify device capabilities.

- Adherence to IT policies and security policies
  - Balance security with usability
- Differences between vendor default applications
- OS modifications and customization
  - OS vendor
  - OEM
  - Telecommunication vendor
- Backup, Restore and Recovery policies

3.2 Compare and contrast mobility solutions to enterprise requirements.

- Mobile Device Management
  - Password strength
Remote wipe
Remote lock/unlock
Application store

Mobile application management
Application store

Pushing content
Device platform support
Infrastructure support
On-premise vs. SaaS
Administrative permissions
Multi-instance
High availability
Device groupings
Location-based services
Geo-location
Geo-fencing

Monitoring and reporting capabilities and features
Interoperability with other products/devices
Telecommunication expense management
Self-service portal
Captive portal

3.3 Install and configure mobile solutions based on given requirements.

Liaise with appropriate personnel to ensure infrastructure can accept solutions
Profile creation
Directory services setup
Initial certificate issuance
EULA
Sandboxing
Containerization
Group profiles based on given requirements
Corporate-owned
BYOD
Executive
Management
Consultant
B2B
Initiate pilot, testing and evaluation
Create and update documentation
• Report feedback post-pilot
• SDLC
• Approve, train and launch

3.4 Implement mobile device on-boarding and off-boarding procedures.
• Device activation on cellular networks
• Mobile hardware that facilitates OTA access
  o Wireless cards, cellular cards, SD cards
• On-boarding and provision process
  o Manual
  o Self-service
  o Batch
  o Remote
  o IMEI or ICCID
  o Device enrollment (SCEP)
  o Profile installations
• Off-boarding and de-provisioning
  o Employee terminations
  o Migrations
  o Applications
  o Content
  o Recycle
  o Proper asset disposal
  o Deactivation

3.5 Implement mobile device operations and management procedures.
• Centralized content and application distribution and content management system
  o Distribution methods
    ▪ Server-based
    ▪ Content updates/changes
    ▪ Application changes
    ▪ Permissions
• Deployment best practices
  o Number of devices
  o Number of users
• Remote capabilities
  o Lock/unlock
  o Remote wipe
  o Remote control
  o Location services
  o Reporting
• Lifecycle operations
  o Certificate expiration/renewal
  o Updates
  o Upgrades
  o Patches
• Change management
• End of life
  o OSs
  o Devices
  o Applications

3.6 Execute best practice for mobile device backup, data recovery and data segregation.
  • Device backup for corporate data to corporate server
  • Device backup of personal data to vendor/third party server
  • Backup to local device: internal storage, SD card, SIM
  • Data recovery
    o Testing backups
    o Restoring corporate data
    o Restoring personal data

3.7 Use best practices to maintain awareness of new technologies including changes that affect mobile devices.
  • OS vendors
  • OEMs (hardware)
  • Telecommunication vendors
  • Third party application vendors
  • New risks and threats

3.8 Configure and deploy mobile applications and associated technologies
  • Messaging standards
    o MAPI
    o IMAP
    o POP
    o SMTP
  • Vendor proxy and gateway server settings
  • Information traffic topology
    o Third party NOC vs. on-premise vs. hosted
  • Push notification technologies
    o APNS
    o GCM
    o ActiveSync
  • In-house application requirements
4.0 Security

4.1 Identify various encryption methods for securing mobile environments.

- Data in-transit
  - IPSEC
  - VPN
  - SSL
  - HTTPS
  - WPA/TKIP
  - WPA2
  - TLS
  - SRTP
  - RSA
  - WEP
  - SSH
  - RC4
  - CCMP
  - EAP methods

- Data at rest
  - AES
  - DES
  - 3DES
  - Two-Fish
  - ECC

- Full disk encryption
- Block level encryption
- File level encryption
- Folder level encryption
- Removable media encryption

4.2 Configure access control on the mobile device using best practices.
• Authentication concepts
  o Multifactor
    ▪ Biometric
    ▪ Credentials
    ▪ Tokens
    ▪ Pin
  o Device access
  o Wireless networks
    ▪ Enterprise vs. personal
  o Application access

• PKI concepts
• Certificate management
• Software-based container access and data segregation

4.3 Explain monitoring and reporting techniques to address security requirements
• Device compliance and report audit information
• Third party device monitoring applications (SIEM)
• Monitor appropriate logs pertaining to mobile device activity/traffic

4.4 Explain risks, threats and mitigation strategies affecting the mobile ecosystem.
• Wireless risks
  o Rogue access points
  o DoS
  o Tower spoofing
  o Jamming
  o War Driving
  o Man-in-the-middle
  o Weak keys

• Software risks
  o App store usage
  o Virus
  o Trojans
  o Worm
  o Malware
  o Spyware
  o Jailbreak
  o Rooting
  o Keylogging
  o Unsupported OS

• Organizational risks
  o BYOD ramifications
  o Securing personal devices
• Removable media
• Wiping personal data
• Unknown devices on network/server

• Hardware risks
  • Device cloning
  • Device theft
  • Device loss

• Mitigation strategies
  • Antivirus
  • Software firewalls
  • Access levels
  • Permissions
  • Host-based and network-based IDS/IPS
  • Anti-malware
  • Application sandboxing
  • Trusted platform modules
  • Data containers
  • Content filtering
  • DLP
  • Device hardening
  • Physical port disabling

4.5 Given a scenario, execute appropriate incident response and remediation steps
  • Incident identification
  • Determine and perform policy-based response
  • Report incident
    • Escalate
    • Document
    • Capture logs

5.0 Troubleshooting

5.1 Given a scenario, implement the following troubleshooting methodology.
  • Identify the problem
    • Information gathering
    • Identify symptoms
    • Question users
    • Determine if anything has changed
  • Establish a theory of probable cause
    • Question the obvious
  • Test the theory to determine cause
Once theory is confirmed determine next steps to resolve problem
   - If theory is not confirmed re-establish new theory or escalate
   - Establish a plan of action to resolve the problem and identify potential effects
   - Implement the solution or escalate as necessary
   - Verify full system functionality and if applicable implement preventative measures
   - Document findings, actions and outcomes

5.2 Given a scenario, troubleshoot common device problems.
   - Battery life
   - Sync issues
   - Power supply problems
   - Password reset
   - Device crash
   - Power outage

5.3 Given a scenario, troubleshoot common application problems.
   - Missing applications
   - Configuration changes
   - App store problems
   - Email issues
   - Location services problems
   - OS and application upgrade issues
   - Profile authentication and authorization issues

5.4 Given a scenario, troubleshoot common over-the-air connectivity problems.
   - Latency
   - No cellular signal
   - No network connectivity
   - Roaming issues
   - Cellular activation
   - Email issues
   - VPN issues
   - Certificate issues
   - APN issues
   - Port configuration issues
   - Network saturation

5.5 Given a scenario, troubleshoot common security problems.
   - Expired certificate
   - Authentication failure
- Firewall misconfiguration
- False positives
- False negatives
- Non-expiring passwords
- Expired passwords
- Content filtering misconfigured
CompTIA Mobility+ Acronyms

**Introduction**
The following is a list of acronyms which appear on the CompTIA Mobility+ exams. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as a part of a comprehensive exam preparation program.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Spelled Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>APN</td>
<td>Access Point Name</td>
</tr>
<tr>
<td>APNS</td>
<td>Apple Push Notification Service</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td>B2B</td>
<td>Business to business</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring your own Device</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority / Certification Authority</td>
</tr>
<tr>
<td>CCE</td>
<td>Common Configuration Enumeration</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>CDR</td>
<td>Call Data Recording</td>
</tr>
<tr>
<td>CME</td>
<td>Coronal Mass Ejection</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>CSD</td>
<td>circuit Switch Data</td>
</tr>
<tr>
<td>CSMA/CA</td>
<td>Carrier Sense Multiple Access with Collision Avoidance</td>
</tr>
<tr>
<td>CSMA/CD</td>
<td>Carrier Sense Multiple Access with Collision Detection</td>
</tr>
<tr>
<td>CUE</td>
<td>Common</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DLP</td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td>DM</td>
<td>Device Manager</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service</td>
</tr>
<tr>
<td>DR</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>EAS</td>
<td>Exchange Active Solution</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
</tr>
<tr>
<td>EULA</td>
<td>End User License Agreement</td>
</tr>
<tr>
<td>EVDO</td>
<td>Evolution Data Optimized</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>FTPS</td>
<td>FTP over SSL</td>
</tr>
<tr>
<td>GCM</td>
<td>Galois/ Counter Mode</td>
</tr>
<tr>
<td>GCMS</td>
<td>Google Cloud Messaging for Android</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GSM</td>
<td>Global Standard for Mobility</td>
</tr>
<tr>
<td>HA</td>
<td>High Availability</td>
</tr>
<tr>
<td>HSPA</td>
<td>High Speed Packet Access</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>IASE</td>
<td>Info Assurance Support Environment</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Message Address Protocol</td>
</tr>
<tr>
<td>IMAPS</td>
<td>Secure IMAP</td>
</tr>
<tr>
<td>IMS</td>
<td>Industrial, Medical, Scientific</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>KCD</td>
<td>Kerberos Constrained Delegation</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>MaaS</td>
<td>Mobility as a Service</td>
</tr>
<tr>
<td>MAM</td>
<td>Mobile Application Management</td>
</tr>
<tr>
<td>MAPI</td>
<td>Messaging Application Programming Interface</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>MDM</td>
<td>Mobile Device Management</td>
</tr>
<tr>
<td>MEAP</td>
<td>Mobile Enterprise Application Platform</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple Input Multiple Output</td>
</tr>
<tr>
<td>MMCA</td>
<td>Multiple Mobile Channel Access</td>
</tr>
<tr>
<td>NAC</td>
<td>Network Access Control</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>NIPS</td>
<td>Network Intrusion Prevention System</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Center</td>
</tr>
<tr>
<td>OCSP</td>
<td>Online Certificate Security Protocol</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnect</td>
</tr>
<tr>
<td>PAN</td>
<td>Personal Area Network</td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
</tr>
<tr>
<td>PIM</td>
<td>Personal Information Manager</td>
</tr>
<tr>
<td>PLE</td>
<td>Power Line Ethernet</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
</tr>
<tr>
<td>POP</td>
<td>Post Office Protocol</td>
</tr>
<tr>
<td>PRL</td>
<td>Preferred Roaming List</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RPT</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received Signal Strength Indicator</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SDLC</td>
<td>System Development Life Cycle</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure FTP</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hashing Algorithm</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
</tbody>
</table>
Suggested Classroom Equipment to have for Mobility+ Certification Training

** CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Mobility+ exam. This list may also be helpful for training companies who wish to
create a lab component to their training offering. The bulleted lists below each topic are a sample list and not exhaustive.

**Equipment**
- Messaging server
- MDM server
- High powered laptop
- Tablets
- Smart phone
- Access point
- Router
- Switch
- Air cards
- Hot spots
- Project/large screen with adapters
- Wireless LAN controller
- PoE injector
- Pico cell
- VPN concentrator
- Firewall
- Hardware tokens (secure IDs)

**Spare parts/hardware**
- Cables (CAT5)
- Removable media
- Various antenna types
- Power adapters
- Sync cables
- SD cards

**Tools**
- Spectrum analyzer
- Crimpers

**Software**
- Android
- iOS
- Various operating systems: OSx, Windows, Linux, Unix
- Messaging client software
- Certificate management software
- MDM, MAM, MCM software
Other

- Internet connection