Certification Exam Objectives: Mobility+ Exam (MB0-001)

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.

Domain	% of Examination
1.0 Over-the-Air Technologies	13%
2.0 Network Infrastructure	15%
3.0 Mobile Device Management	28%
4.0 Security	20%
5.0 Troubleshooting	24%
Total	**100%**

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:
http://certification.comptia.org/Training/testingcenters/policies/unauthorized.aspx

**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

    - Interference
- Antennas
    - Omni-directional
    - Semi-directional
    - Bi-directional
    - YAGI
    - Parabolic dish
- Faraday cage

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

    - Controller
    - Lightweight AP
- Services and settings
    - ActiveSync
    - Dynamic VLAN
    - Subnetting

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 – SSMTP
- 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
    - Wireless cards, cellular cards, SD cards
- On-boarding and provision process
    - Manual
    - Self-service
    - Batch
    - Remote
    - IMEI or ICCID
    - Device enrollment (SCEP)
    - Profile installations
- Off-boarding and de-provisioning
    - Employee terminations
    - Migrations
    - Applications
    - Content
    - Recycle
    - Proper asset disposal
    - Deactivation

3.5 Implement mobile device operations and management procedures.

- Centralized content and application distribution and content management system
    - Distribution methods
        - Server-based
        - Content updates/changes
        - Application changes
        - Permissions
- Deployment best practices
    - Number of devices
    - Number of users
- Remote capabilities
    - Lock/unlock
    - Remote wipe
    - Remote control
    - Location services
    - Reporting

- Lifecycle operations
    - Certificate expiration/renewal
    - Updates
    - Upgrades
    - Patches
- Change management
- End of life
    - OSs
    - Devices
    - 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
    - Testing backups
    - Restoring corporate data
    - 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
    - MAPI
    - IMAP
    - POP
    - SMTP
- Vendor proxy and gateway server settings
- Information traffic topology
    - Third party NOC vs. on-premise vs. hosted
- Push notification technologies
    - APNS
    - GCM
    - ActiveSync
- In-house application requirements

    - App publishing
    - Platforms
    - Vendor requirements
    - Certificates
    - Data communication
- Types of mobile applications
    - Native app
    - Web app
    - Hybrid app

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
    - Multifactor
        - Biometric
        - Credentials
        - Tokens
        - Pin
    - Device access
    - Wireless networks
        - Enterprise vs. personal
    - 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
    - Rogue access points
    - DoS
    - Tower spoofing
    - Jamming
    - War Driving
    - Man-in-the-middle
    - Weak keys
- Software risks
    - App store usage
    - Virus
    - Trojans
    - Worm
    - Malware
    - Spyware
    - Jailbreak
    - Rooting
    - Keylogging
    - Unsupported OS
- Organizational risks
    - BYOD ramifications
    - 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.

Acronym	Spelled Out
ACL	Access Control List
AD	Active Directory
AP	Access Point
APN	Access Point Name
APNS	Apple Push Notification Service
AUP	Acceptable Use Policy
B2B	Business to business
BYOD	Bring your own Device
CA	Certificate Authority / Certification Authority
CCE	Common Configuration Enumeration
CDMA	Code Division Multiple Access
CDR	Call Data Recording
CME	Coronal Mass Ejection
CRL	Certificate Revocation List
CSD	circuit Switch Data
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CUE	Common
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DM	Device Manager
DMZ	Demilitarized Zone
DNS	Domain Name Service
DR	Disaster Recovery
EAS	Exchange Active Solution
ECC	Elliptic Curve Cryptography
EULA	End User License Agreement
EVDO	Evolution Data Optimized
FTP	File Transfer Protocol
FTPS	FTP over SSL
GCM	Galois/ Counter Mode
GCM	Google Cloud Messaging for Android
GPRS	General Packet Radio Service
GSM	Global Standard for Mobility
HA	High Availability
HSPA	High Speed Packet Access
HTTP	Hyper Text Transfer Protocol
IDS	Intrusion Detection System

IASE	Info Assurance Support Environment
IETF	Internet Engineering Task Force
IMAP	Internet Message Address Protocol
IMAPS	Secure IMAP
IMS	Industrial, Medical, Scientific
IP	Internet Protocol
IPS	Intrusion Prevention System
KCD	Kerberos Constrained Delegation
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LTE	Long Term Evolution
MaaS	Mobility as a Service
MAM	Mobile Application Management
MAPI	Messaging Application Programming Interface
MD5	Message Digest 5
MDM	Mobile Device Management
MEAP	Mobile Enterprise Application Platform
MIB	Management Information Base
MIMO	Multiple Input Multiple Output
MMCA	Multiple Mobile Channel Access
NAC	Network Access Control
NAT	Network Address Translation
NFC	Near Field Communication
NIPS	Network Intrusion Prevention System
NOC	Network Operations Center
OCSP	Online Certificate Security Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
OSI	Open Systems Interconnect
PAN	Personal Area Network
PAT	Port Address Translation
PGP	Pretty Good Privacy
PIM	Personal Information Manager
PLE	Power Line Ethernet
PoE	Power over Ethernet
POP	Post Office Protocol
PRL	Preferred Roaming List
QoS	Quality of Service
RDP	Remote Desktop Protocol
RF	Radio Frequency
RPT	Recovery Point Objective
RSSI	Received Signal Strength Indicator
RTO	Recovery Time Objective
SaaS	Software as a Service
SDLC	System Development Life Cycle
SFTP	Secure FTP
SIM	Subscriber Identity Module
SIEM	Security Information and Event Management
SHA	Secure Hashing Algorithm
SLA	Service Level Agreement

SMTP	Simple Mail Transport Protocol
SOHO	Small Office Home Office
SRP	Server Router Protocol
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSMTP	Secure SMTP
SSP	Self Service Portal
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TEM	Telecom Expense Management
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications Standards
USCC	United States CyberCom
VLAN	Virtual LAN
VoIP	Voice Over IP
VPN	Virtual Private Network
VPP	Volume Purchase Program
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access

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