Implementing Cisco Service Provider Mobility UMTS Networks (600-210)

Exam Description:

The Implementing Cisco UMTS Packet Core Networks (600-210 SPUMTS) exam is a 90-minute, 65–75 question assessment within Cisco’s Service Provider Specialist certification. This exam tests a candidate's knowledge of the skills required to understand and implement technologies, components, architecture fundamentals and products that are found in Universal Mobile Telecommunications System (UMTS) packet core networks. The exam includes information on standardized technologies that are implemented on the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN), as well as, their interaction with authentication, charging, and billing components in the network of the mobile operator. This exam also includes configuration details of how these components are implemented on the Cisco ASR 5000 Series system. This exam is a requirement in order to attain the Cisco Service Provider Mobility UMTS to LTE Specialist certification. Candidates can prepare for this exam by taking the Implementing Cisco Service Provider Mobility UMTS Networks (SPUMTS) v1.0 training course.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

3% 1.0 GPRS/UMTS
1.1 Understand and describe GSM/GPRS and UMTS architecture

11% 2.0 SS7 GTT/MAP
2.1 Describe application of SS7 in wireless networks
2.2 Describe SIGTRAN protocol stacks (M3UA) and MTP3 based routing
2.3 Describe SCCP layer and Global Title Translation (GTT) mechanism
2.4 Analyze Global Title Translation (GTT) Case studies in mobile
2.5 Describe Application layer protocols

15% 3.0 Tunneling Protocols (GTP)
3.1 Describe the basics of GTP and packet structure
3.2 Identify different versions of GTP and compare them
3.3 Describe GTP tunnel, location and mobility management messages and their relevance
3.4 Describe failure and Recovery procedures
3.5 Configure GTP end points between UMTS nodes and LTE nodes
3.6 Troubleshoot GTP

20% 4.0 SGSN (3G UMTS Node)
4.1 Network functions 2G/3G SGSN and call flows
4.1.a Describe SGSN architecture and interfaces
4.1.b Identify SGSN functions
4.1.c Describe protocol stacks and procedures
4.1.d Describe mobility management signaling and call flows
4.1.e Describe session management signaling and call flows
4.1.f Describe G5 interface procedures
4.1.g Describe Gd interface procedures

4.2 Configuration
4.2.a Configuration of IU interfaces over both IU/IP and IU/ATM
4.2.b Configuration of the Gr interface for both narrow band SS7 and sigtran
4.2.c Configuration of the Gn/Gp interface
4.2.d Configuration of the Gs interface towards the MSC
4.2.e Configuration of the Gb interface
4.2.f Configuration of the Gd interface
4.2.g Describe SGSN Operator policy structure and feature sets
4.2.h Configure SGSN Operator policy and feature sets
4.2.i Troubleshooting SGSN configurations

4.3 Policing architecture
4.3.a Describe SGSN pooling, key benefits and design considerations
4.3.b Configure SGSN pooling
4.3.c Describe offloading mechanism in pooling
4.3.d Configure MSC pooling architecture
4.3.e Describe MSC offloading in an SGSN pooled network

4.4 Direct tunnel
4.4.a Implement direct tunnel in a SGSN network
4.4.b Explain subscriber movement from one tunnel to two tunnel functionality
4.4.c Troubleshooting Direct tunnel

4.5 Network sharing
4.5.a Describe and implement MOCN architecture
4.5.b Describe and implement GWCN architecture

4.6 Security functions
4.6.a Describe GSM and UMTS security principles
4.6.b Describe different security architecture in UMTS

4.7 QoS functions
4.7.a Describe session management QoS functions
4.7.b Describe R99 and R97 QoS Conversion
4.7.c Configure QoS negotiations and override function

4.8 S4-SGSN
4.8.a Describe evolution to S4-SGSN
4.8.b Describe Mobility management signaling and call flows for S4-SGSN
4.8.c Describe location management signaling and call flows for S4-SGSN
4.8.d  Describe location management signaling and call flows for S4-SGSN
4.8.e  Configure basic S4-SGSN
4.8.f  Troubleshooting S4-SGSN

12%  5.0  Diameter (MPC centric)
  5.1  Define and understand diameter base protocol
  5.2  Understand transport layer functionality of diameter protocol
  5.3  Understand and implement diameter routing agents
  5.4  Understand diameter peer discovery
  5.5  Understanding diameter message processing
  5.6  Understanding diameter error handling mechanism
  5.7  Describe and understand diameter re-authorization procedure
  5.8  Describe and understand DCCA model

13%  6.0  Tunneling Protocols (Others)
  6.1  Basics of tunneling and encryption
       6.1.a  Identify application of tunneling in wireless data networks
  6.2  GRE
       6.2.a  Identify applications of GRE in wireless data networks
       6.2.b  Configure GRE tunnels
       6.2.c  Troubleshoot GRE tunnels
  6.3  Layer 2 Tunneling Protocol (L2TP)
       6.3.a  Identify applications of L2TP in wireless data networks
       6.3.b  Describe LNS selection and load balancing
       6.3.c  Describe L2TP over IPSec
       6.3.d  Configuring L2TP tunnels
       6.3.e  Troubleshoot L2TP tunnels
  6.4  Internet Protocol Security (IPsec)
       6.4.a  Configure IPSec tunnels on the GGSN
       6.4.b  Identify applications of IPSec tunnels as applied to Mobile wireless networks
       6.4.c  Describe IPSec for IPV6
       6.4.d  Troubleshoot IPSec
  6.5  MPLS over BGP
       6.5.a  Describe MPLS over BGP in Mobile Packet Core Networks
       6.5.b  Configure MPLS over BGP
       6.5.c  Troubleshoot MPLS over BGP

13%  7.0  GGSN (3G UMTS node)
  7.1  Architecture Overview
       7.1.a  Identify key functions of the GGSN, and also understanding of the various interfaces
  7.2  Implement Gn/Gp Interface
       7.2.a  Describe GTP protocol
7.2.b Describe call flows for mobility management/session management
7.2.c Configure Gn/Gp Interface
7.2.d Troubleshoot Gn/Gp Interface

7.3 APN
7.3.a Identify various IP address allocation mechanisms
7.3.b Describe the concept of virtual APNs
7.3.c Describe IP source address validation and access control list
7.3.d Configure APN
7.3.e Troubleshoot APN

7.4 Implement Gx Interface
7.4.a Identify important diameter AVPs needed for Gx
7.4.b Describe basic Gx call flows
7.4.c Configure Gx interface
7.4.d Troubleshoot Gx interface
7.4.e Configure failure handling modes
7.4.f Selection of OCS based on static configuration, RADIUS attributes and PCRF
7.4.g Describe out-of-quota redirection handling

7.5 Implement Gy Interface
7.5.a Identify important diameter AVPs needed for Gy
7.5.b Describe basic Gy call flows
7.5.c Configure Gy interface
7.5.d Troubleshoot Gy interface
7.5.e Identify and describe common policy use cases
7.5.f Configure failure handling modes
7.5.g Configure usage monitoring over Gy

7.6 Implement AAA Interface
7.6.a Describe basic AAA authentication and accounting call flows
7.6.b Identify and describe important RADIUS attributes for authentication and accounting
7.6.c Configure AAA interface
7.6.d Troubleshoot AAA interface

7.7 Internetworking with non-3GPP access networks
7.7.a Describe non-3GPP IRAT handovers to GPRS/UMTS networks
7.7.b Configure Gn' interface
7.7.c Troubleshooting non-3GPP access networks

7.8 Gi interface
7.8.a Configure and implement various IP transport types
7.8.b Configure and implement static and dynamic routing protocols

8.0 Inline Services
8.1 Packet inspection
8.1.a Explain common L7 applications
8.1.b Describe packet processing by the traffic inspection engine
8.1.c Describe and configure rules to be used for traffic inspection
8.1.d Describe and configure charging rules
8.1.e Configure charging policies
8.1.f Design and configure rulebases, and the priorities for the rules and their corresponding charging policies
8.1.g Describe handling of VOIP traffic
8.1.h Configure post processing rules
8.1.i Troubleshoot packet Inspection

8.2 P2P detection
8.2.a Configure the rules for the various P2P applications
8.2.b Describe mechanism of updating the software to detect newer P2P applications

8.3 Content filtering
8.3.a Describe the various content filtering mechanisms available
8.3.b Describe ICAP protocol
8.3.c Configure content filtering
8.3.d Troubleshoot content filtering

8.4 Firewall policies
8.4.a Describe the basics of stateful attacks
8.4.b Configure access rules
8.4.c Troubleshoot firewall policies

8.5 NAT
8.5.a Configure NAT IP Pools, and Port Chunk Groups to be used
8.5.b Configure the NAT accounting records
8.5.c Troubleshoot NAT

8.6 Event-based charging
8.6.a Configure Event Data Records (EDRs)
8.6.b Configuration flow based charging records (Enhanced GCDR Records)
8.6.c Describe report generation using EDRs for different types

8.7 Fraud detection
8.7.a Describe DNS snooping
8.7.b Explain the various mechanisms available for detection of tethered traffic
8.7.c Describe updating the database for the list of known tethered devices
8.7.d Configure fraud detection
8.7.e Troubleshoot fraud detection

8.8 HTTP header enrichment
8.8.a Describe HTTP header enrichment
8.8.b Configure HTTP header enrichment
8.8.c Troubleshoot HTTP header enrichment