UCK UNIVERZITNÉ CENTRUM KOŠICE

ONLINE

CCNP ENTERPRISE

CCNP ENCOR + **CCNP ENARSI**

300 – 410
Implementing CISCO Enterprise
Advanced Routing and Services

350 – 401
Implementing and Operating CISCO
Enterprise Network Core Technologies

JANUÁR 2024 – HARONOGRAM VÝUČBY CCNP ENARSI

PONDELOK	UTOROK	STREDA	ŠTVRTOK	PIATOK	SOBOTA	NE
1	2	3	4	5	6	7
8	9	10	11	12	13 08:00 – 16:00 hod. 1. stretnutie CCNP ENARSI	14
15	16	17 16:00 – 20:00 hod. Benefitné stretnutie CCNP ENARSI	18	19	20 08:00 – 16:00 hod. 2. stretnutie CCNP ENARSI	21
22	23	24 16:00 – 20:00 hod. Benefitné stretnutie CCNP ENARSI	25	26	27 08:00 – 16:00 hod. 3. stretnutie CCNP ENARSI	28
29	30	31 16:00 – 20:00 hod. Benefitné stretnutie CCNP ENARSI				

FEBRUÁR 2024 – HARONOGRAM VÝUČBY CCNP ENARSI

PONDELOK	UTOROK	STREDA	ŠTVRTOK	PIATOK	SOBOTA	NE
			1	2	3 08:00 – 16:00 hod. 4. stretnutie CCNP ENARSI	4
5	6	7 16:00 – 20:00 hod. Benefitné stretnutie CCNP ENARSI	8	9	10 08:00 – 16:00 hod. 5. stretnutie CCNP ENARSI	11
12	13	14 16:00 – 20:00 hod. Benefitné stretnutie CCNP ENARSI	15	16	17 08:00 – 16:00 hod. 6. stretnutie CCNP ENARSI	18
19	20	21 16:00 – 20:00 hod. Benefitné stretnutie CCNP ENARSI	22	23	24 08:00 – 16:00 hod. 1. stretnutie CCNP ENARSI Teoretické a praktické testovanie	25
26	27	28	29			

1. meeting – content of the segment CCNP ENARSI
1.0: IPv4/IPv6 addressing, advanced EIGRP

1.1 IPv4/IPv6 Addressing and Routing Review

1.1. a IPv4 Addressing	A review of IPv4 addressing and issues you might face and how to troubleshoot them.
1.1. b DHCP for IPv4	DHCP operations, potential issues, output of various DHCP **show** commands.
1.1. c IPv6 Addressing	**A** brief review of IPv6 addressing
1.1. d IPv6 SLAAC, Stateful DHCPv6 and Stateless DHCPv6	How clients obtain IPv6 addressing information using SLACC, stateful DHCPv6, and stateless DHCPv6.
1.1. e Packet-Forwarding Process	Packet-forwarding process and the commands to verify the entries in the data structures that are used for this process.
1.1. f Routing Information Sources	Explanation of routing information sources, how the routing table interacts with various data structures to populate itself with the best information.
1.1. g Static Routes	Configuration and verification of IPv4 and IPv6 static routes.
1.1. h Trouble Tickets	A number of trouble tickets are provided to demonstrate how a structured troubleshooting process is used to solve a reported problem.

1.2 EIGRP

1.2. a EIGRP Fundamentals	How EIGRP establishes a neighborship with other routers and how routes are exchanged with other routers.
1.2. b EIGRP Configuration Modes	Explanation of the two methods of configuring EIGRP with a baseline configuration.
1.2. c Path Metric Calculation	How EIGRP calculates the path metric to identify the best and alternate loop-free paths.

1.3 Advanced EIGRP

1.3. a Failure Detection and Timers	How EIGRP detects the absence of a neighbor and the convergence process.
1.3. b Route Summarization	Explanation of the logic and configuration of summarizing routes on a router.
1.3. c WAN Considerations	Reviews common design considerations with using EIGRP in a WAN.
1.3. d Route Manipulation	Techniques for filtering or manipulating route metrics.

1.4 Troubleshooting EIGRP for IPv4

1.4. a Troubleshooting EIGRP for IPv4 Neighbor Adjacencies	Why neighbor relationships for IPv4 EIGRP might not be formed and how to identify them.
1.4. b Troubleshooting EIGRP for IPv4 Routes	Exploration of the reasons EIGRP for IPv4 routes might be missing from a router's EIGRP table or routing table and how to determine why they are missing.
1.4. c Troubleshooting Miscellaneous EIGRP for IPv4 Issues	Identification of some additional issues you might face while using EIGRP, how to identify them, and how to solve them.
1.4. d EIGRP for IPv4 Trouble Tickets	A number of trouble tickets are provided to demonstrate how a structured troubleshooting process is used to solve a reported problem.

1.5 EIGRPv6

1.5. a EIGRPv6 Fundamentals	An overview of EIGRPv6 and the correlation to EIGRP for routing IPv4 networks.
1.5. b Troubleshooting EIGRPv6 Neighbor Issues	Why EIGRPv6 neighbor relationships may not be formed and how to identify them.
1.5. c Troubleshooting EIGRPv6 Routes	Why EIGRPv6 routes might be missing and how to determine why they are missing.
1.5. d Troubleshooting Named EIGRP	Introduction of the **show** commands that you can use to troubleshoot named EIGRP configurations.
1.5. e EIGRPv6 and Named EIGRP Trouble Tickets	A number of trouble tickets are provided to demonstrate how a structured troubleshooting process is used to solve a reported problem.

Practical labs

Troubleshoot IPv4/IPv6 addressing issues

Troubleshoot IPv4 and IPv4 static routing

Implementation of basic and advanced features for EIGRP and EIGRPv6

Troubleshoot EIGRP for IPv4 and IPv6

2. meeting – content of the segment CCNP ENARSI
2.0: Advanced routing techniques used in OSPFv2 and OSPFv3

2.1 OSPF	
2.1. a OSPF Fundamentals	An overview of the OSPF routing protocol.
2.1. b OSPF Configuration	How to configure a router with basic OSPF functionality.
2.1. c The Designated Router and Backup Designated Router	Description of the function of the designated router and how it provides scalability for broadcast network segments.
2.1. d OSPF Network Types	An overview of the OSPF network types and their impact to OSPF's behavior.
2.1. e Failure Detection	How OSPF detects and verifies the health of OSPF neighbor routers.
2.1. f Authentication	Function of authentication and how it is configured.
2.2 Advanced OSPF	
2.2. a Link-State Advertisements	How OSPF stores, communicates, and builds the topology from link-state advertisements (LSAs).
2.2. b OSPF Stubby Areas	Method that OSPF provides for filtering external routes while still providing connectivity to them.
2.2. c OSPF Path Selection	How OSPF makes path selection choicesfor routes learned within the OSPF routing domain.
2.2. d Summarization of Routes	How network summarization works with OSPF.
2.2. e Discontiguous Network	Explanation of a discontiguous network and why it cannot distribute routes to all areas properly.
2.2. f Virtual Links	How OSPF repairs a discontiguous network.
2.3 Troubleshooting OSPFv2	
2.3. a Troubleshootign OSPFv2 Neighbor Adjacencies	Why OSPFv2 neighbor adjacencies sometimes do not form and how to identify them.
2.3. b Troubleshooting OSPFv2 Routes	Why OSPFv2 routes might be missing from the link-state database (LSDB) and routing table and how to determine why they are missing.
2.3. c Troubleshooting Miscellaneous OSPV2 Issues	This section focuses on tracking link-state advertisements (LSAs) through the network, route summarization, discontiguous areas, load balancing, and default routes.
2.3. d OSPFv2 Trouble Tickets	A number of trouble tickets are provided to demonstrate how a structured troubleshooting process is used to solve a reported problem.
2.4 OSPFv3	
2.4. a OSPFv3 Fundamentals	An overview of the OSPFv3 routing protocol, its similarities to OSPFv2, and its configuration.
2.4. b OSPFv3 Configuration	How OSPFv3 is used for exchanging IPv6 routes.
2.4. c OSPFv3 LSA Flooding Scope	A deeper view of the OSPFv3 ink-state advertisement (LSA) structure and the comparison to OSPFv2
2.5 Troubleshooting OSPFv3	
2.5. a Troubleshooting OSPv3 for IPv6	Various commands are shown to troubleshoot OSPFv3 issues.
2.5. b OSPFv3 Trouble Tickets	A number of trouble tickets are provided to demonstrate how a structured troubleshooting process is used to solve a reported problem.
2.5. c Troubleshooting OSPFv3 Address Families	Description if the commands used to troubleshoot issues related to OSPFv3 address family configurations.
2.5. d OSPFv3 AF Trouble Ticket	A number of trouble tickets are provided to demonstrate how a structured troubleshooting process is used to solve a reported problem.
Practical labs	
Implementation of stub areas for OSPFv2/OSPFv3	
Troubleshoot OSPFv2/OSPFv3	

3. meeting – content of the segment CCNP ENARSI
3.0: Advanced routing techniques used in BGP and MP-BGP

3.1 BGP

3.1. a BGP Fundamentals	An overview of the fundamentals of the BGP routing protocol.
3.1. b Basic BGP Configuration	Process of configuring BGP to establish a neighbor session and how routes are exchanged between peers.
3.1. c Understanding BGP Sessions Types and Behaviors	An overview of how route summarization works with BGP and some of the design considerations related to summarization.
3.1. d Multiprotocol BGP for IPv6	How BGP provides support for IPv6 routing and its configuration.

3.2 Advanced BGP

3.2. a Route Summarization	An overview of the how route summarization works with Border Gateway Protocol (BGP) and some design considerations related to summarization.
3.2. b BGP Route Filtering and Manipulation	Filtration and manipulation of routes based on network prefix, AS_Path, or other BGP path attributes.
3.2. c BGP Communities	Explanation of BGP communities and how the well-known communities influence prefix advertisements along with how they are used for conditional prefix filtering or manipulation.
3.2. d Maximum Prefix	How a router can limit the number of prefixes received to ensure that the BGP table does not exceed its capacity.
3.2. e Configuration Scalability	The use of peer groups and peer templates to assist with BGP configurations on routers with a lot of BGP sessions.

3.3 BGP Path Selection

3.3. a Understanding BGP Path Selection	Review of the first step of path selection, which involves selecting the longest prefix length.
3.3. b BGP Best Path	Description of the logic used by BGP to identify the best path when multiple routes are installed in the BGP table.
3.3. c BGP Equal-Cost Multipath	How additional paths are presented to the Routing Information Base (RIB) for installation into the routing table.

3.4 Troubleshooting BGP

3.4. a Troubleshooting BGP Neighbor Adjacencies	This section examines issues that may prevent a BGP neighbor relationship from forming and how to recognize and troubleshoot these issues.
3.4. b Troubleshooting BGP Routes	Focus is on issues that may prevent BGP routes from being learned or advertised and how to recognize and troubleshoot these issues.
3.4. c Troubleshooting BGP Path Selection	How BGP determines the best path to reach a destination network and the importance of understanding how this process works for troubleshooting purposes.
3.4. d Troubleshooting BGP for IPv6	Methods used to successfully troubleshoot additional issues related to BGP for IPv6 that are not seen with BGP for IPv4.
3.4. e BGP Trouble Tickets	A number of trouble tickets are used for a structured troubleshooting process to solve a reported problem.
3.4. f MP-BGP Trouble Tickets	A number of trouble tickets are used for a structured troubleshooting process to solve a reported problem.

Practical labs

Implementation of MP-BGP

Manipulation with BGP attributes

Troubleshoot BGP

4. meeting – content of the segment CCNP ENARSI
4.0: Route redistribution

4.1 Route Maps and Conditional Forwarding

4.1. a Conditional Matching	An overview of how network prefixes can be conditionally matched with ACLs or prefix lists.
4.1. b Route Maps	Explanation of the structure of a route map and how conditional matching and conditional actions can be combined to filter or manipulate routes.
4.1. c Conditional Forwarding of Packets	How a router forwards packets down different paths based on the network traffic.
4.1. d Trouble Tickets	Three trouble tickets are provided to demonstrate how a structured troubleshooting process can be used to solve a reported problem.

4.2 Route Redistribution

4.2. a Redistribution Overview	An overview of redistribution fundamentals and rules of redistribution of routes between routing protocols.
4.2. b Protocol-Specific Configuration	Explanation of protocol specific behaviors and configuration examples for redistribution of routes between routing protocols.

4.3 Troubleshooting Redistribution

4.3. a Troubleshooting Advanced Redistribution Issues	How suboptimal routing and routing loops may occur when redistributing at multiple points in the network. In addition, you will discover how to recognize these redistribution issues and solve them.
4.3. b Troubleshooting IPv4 and IPv6 Redistribution	Redistribution troubleshooting issues for IPv4 and IPv6 routing protocols such as EIGRP, OSPF, and BGP.
4.3. c Redistribution Trouble Tickets	Trouble tickets are provided to demonstrate how to use a structured troubleshooting process to solve a reported problem

Practical labs

Configuration of route redistribution between IGP protocols

Configuration of route redistribution using BGP

Troubleshoot redistribution

---

5. meeting – content of the segment CCNP ENARSI
5.0: VRF, MPLS and MPLS Layer 3 VPN

5.1 VRF, MPLS, and MPLS Layer 3 VPNs

5.1. a Implementing and Verifying VRF-Lite	Introduction to VRF and how to configure and verify a VRF-Lite implementation.
5.1. b An Introduction to MPLS Operations	Introduction and exploration to MPLS and the main MPLS topics, such as LSRs, LDP, LSP, and label switching.
5.1. c An Introduction to MPLS Layer 3 VPNs	Introduction to the concept of MPLS Layer 3 VPNs.

5.2 DMVPN Tunnels

5.2. a Generic Routing Encapsulation (GRE) Tunnels	How GRE tunnels operate and explains the configuration of GRE tunnels.
5.2. b Next Hop Resolution Protocol (NHRP)	Description of the NHRP protocol and how it dynamically maps underlay IP addresses to overlay tunnel IP addresses.
5.2. c Dynamic Multipoint VPN (DMVPN)	Explanation of the three DMVPN phases and the technologies involved with DMVPN tunnels.
5.2. d DMVPN Configuration	Explanation of the configuration of DMVPN tunnels.
5.2. e Spoke-to-Spoke Communication	Explanation of how spoke-to-spoke DMVPN tunnels form.
5.2. f Problems with Overlay Networks	Description of common issues with overlay networks and optimal design concepts to prevent those issues.
5.2. g DMVPN Failure Detection and High Availability	DMVPN mechanisms to detect failure and methods for providing a resilient DMVPN network.
5.2. h IPv6 DMVPN Configuration	How DMVPN tunnels can use IPv6 networks as an underlay or overlay network

5.3 Securing DMVPN Tunnels

5.3. a Elements of Secure Transport	Explanation of the need for data integrity, data confidentiality, and data availability.

5.3. b IPSec Fundamentals	Explanation of the core concepts involved with IP security encryption.
5.3. c IPSec Tunnel Protection	This section explains how IPsec protection integrates with DMVPN tunnels.
5.4. Troubleshooting ACL and Prefix Lists	
5.4. a Troubleshooting IPv4 ACLs	How to read IPv4 ACLs so that you are more efficient at troubleshooting IPv4 ACL-related issues.
5.4. b Troubleshooting IPv6 ACLs	How to read IPv6 ACLs so that you are more efficient at troubleshooting IPv6 ACL-related issues.
5.4. c Troubleshooting Prefix Lists	How to efficiently examine a prefix list for troubleshooting purposes.
5.4. d Trouble Tickets	Trouble tickets are provided to demonstrate how to use a structured troubleshooting process to solve a reported problem.
Practical labs	
Implementation of DMVPN for IPv4 and IPv6	
Configuration of secure DMVPN tunnels	
VRF-Lite configuration	

6. meeting – content of the segment CCNP ENARSI
6.0: Module review, preparation for the final exam

7. meeting – content of the segment CCNP ENARSI
Theoretical and practical exam

SELF STUDY

Infrastructure Security	
Cisco IOS AAA Troubleshooting:	How to identify and troubleshoot issues related to AAA using the local database, a RADIUS server, and a TACACS+ server.
Troubleshooting Unicast Reverse Path Forwarding (uRPF):	Explanation of what to look for when having issues with uRPF.
Troubleshooting Control Plane Policing (CoPP):	CoPP and the items you should be considering when troubleshooting issues related to CoPP.
IPv6 First-Hop Security:	Description of IPv6 First-Hop Security features, such as RA Guard, DHCP Guard, ND inspection/snooping, and Source Guard.
Device Management and Management Tools Troubleshooting	
Device Management Troubleshooting	How to identify and troubleshoot issues related to console and vty access, as well as remote transfer tools. Various protocols are covered, including Telnet, SSH, TFTP, HTTP, HTTPS, and SCP
Management Tools Troubleshooting	How to use and troubleshoot various management tools, including syslog, SNMP, Cisco IP SLA, Object Tracking, NetFlow, and Flexible NetFlow. In addition, it examines Bidirectional Forwarding Detection (BFD) and Cisco DNA Center Assurance.