NOVEMBER 2023 – HARMONOGRAM VÝUČBY CCNP ENCOR

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

DECEMBER 2023 – HARMONOGRAM VÝUČBY CCNP ENCOR

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

1. meeting – content of the segment CCNP ENCOR 1.0: switching and routing of packets, STP	
1.1. Packet Forwarding	
1.1. a Network Device Communication	How switches forward traffic from a Layer 2 perspective and routers forward traffic from a Layer 3 perspective.
1.1. b Forwarding Architectures	Mechanisms used in routers and switches to forweard network traffic.
1.2 Spanning Tree Protocol	
1.2. a Spanning Tree Protocol Fundamentals	Overview of how switches become aware of other switches and prevent forwarding loops.
1.2. b Rapid Spanning Tree Protocol	Exploration of the improvements over STP.
1.3 Advanced STP Tuning	
1.3. a STP Topology Tuning	Options for modifying the root bridge location or moving blocking ports to designated ports.
1.3. b Additional STP Protection Mechanisms	Exploration of protections mechanisms such as root guard, BPDU guard and STP loop guard.
1.4 Multiple Spanning Tree Protocol	
1.4 a Multiple Spanning Tree Protocol	**Exploration of operation and benefits of MST**
Practical labs	
Implementation of basic and advanced STP (RSTP) features	
Implementation of MSTP in a Cisco switched environment	

2. meeting – content of the segment CCNP ENCOR 2.0: VTP, Etherchannel and IP routing essentials	
2.1 VLAN Trunks and EtherChannel Bundles	
2.1. a VLAN Trunking Protocol	An overview of synchronization of VLAN database across multiple switches, explanation and comparison of each version.
2.1. b Dynamic Trunkning Protocol	Modes of operation, DTP frame, best configuration practices.
2.1. c EtherChannel Bundles	How multiple physical interfaces can be combined to form a logical interface to increase throughput and provide seamless resiliency.
2.2 IP Routing Essentials	
2.2. a Routing Protocol Overview	Exploration of how different routing protocols advertise and identify routes.
2.2. b Path Selection	Explanation the logic a router uses to identify the best route and install it in the routing table.
2.2. c Static Routing	A brief overview of fundamental static route concepts.
2.2. d Virtual Routing and Forwarding	Explanation of the creation of logical routers on a physical router.
2.3 EIGRP	
2.3. a EIGRP Fundamentals	How EIGRP establishes a neighbor adjacency with other routers and how routes are exchanged with other routers.
2.3. b Path Metric Calculation	How EIGRP calculates the path metric to identify the best and alternate loop-free paths.
2.3. c Failure Detection and Timers	How EIGRP detects the absence of a neighbor and the convergence process.
2.3. d Route Summarization	Explanation of the logic and configuration related to summarizing routes on a router.
Practical labs	
implementation of VTP	
Implementation of EtherChannel with fine tuning of LACP protocol	
Implementation of VRF-Lite	

3. meeting – content of the segment CCNP ENCOR
3.0: OSPFv2 and OSPFv3

3.1 OSPF	
3.1. a OSPF Fundamentals	An overview of communication between OSPF routers.
3.1. b OSPF Configuration	OSPF configuration techniques and commands that can be executed to verify the exchange of routes.
3.1. c Default Route Advertisement	How default routes are advertised in OSPF.
3.1. d Common OSPF Optimizations	Common OSPF settings for optimizing the operation of the protocol.
3.2 Advanced OSPF	
3.2. a Areas	Benefits and functions of areas within an OSPF routing domain.
3.2. b Link-State Announcements	How OSPF stores, communicates, and builds a topology from the link-state announcements (LSAs).
3.2. c Discontiguous Networks	Why a discontiguous network design will not distribute routes to all areas properly.
3.2. d OSPF Path Selection	How OSPF makes path selection choices for routes learned within the OSPF routing domain.
3.2. e Summarization of Routes	Explanation of how network summarization works with OSPF.
3.2. f Route Filtering	How OSPF routes can be filtered on a router.
3.3 OSPFv3	
3.3. a OSPFv3 Fundamentals	An overview of the OSPFv3 routing protocol and the similarities to OSPFv2.
3.3. b OSPFv3 Configuration	Configuration and verification of an OSPFv3 environment.
3.3. c IPv4 Support in OSPFv3	How OSPFv3 can be used for exchanging IPv4 routes.
Practical labs	
Implementation of Multi-Area OSPFv2	
Implementation of Multi-Area OSPFv3	
OSPFv2 – summarization and filtering	

4. meeting – content of the segment CCNP ENCOR
4.0: BGP

4.1 BGP	
4.1. a BGP Fundamentals	An overview of the fundamentals of the BGP routing protocol.
4.1. b Basic BGP Configuration	Step by step process of configuring BGP to establish a neighbor session and how routes are exchanged between peers.
4.1 c Route Summarization	An overview of how route summarization works with BGP and some of the design considerations with summarization.
4.1 d Multiprotocol BGP for IPv6	How BGP provides support for IPv6 routing and configuration.
4.2 Advanced BGP	
4.2. a BGP Multihoming	Methods of providing resiliency through redundant BGP connections, along with desired and undesired design considerations for Internet and MPLS connections (branch and data center).
4.2. b Conditional Matching	An overview of how network prefixes can be conditionally matched with ACLs, prefix lists, and regular expressions.
4.2. c Route Maps	Structure of a route map and how conditional matching and conditional actions can be combined to filter or manipulate routes.
4.2. d BGP Route Filtering and Manipulation	How conditional matching and route maps work by applying real-world use cases to demonstrate the filtering or manipulation of BGP routes.
4.2. e BGP Communities	Explanation of the BGP well-known mandatory path attribute and how it can be used to tag a prefix to have route policies applied by routers in the same autonomous system or in an external autonomous system.

4.2. f Understanding BGP Path Selection	Description of the logic used by BGP to identify the best path when multiple routes are installed in the BGP table.
Practical labs	
Implementation of eBGP in IPv4 environment	
Implementation of MP-BGP for IPv4/IPv6 environment	
BGP Path Manipulation and BGP Communities	

5. meeting – content of the segment CCNP ENCOR
5.0: FHRP and VPN

5.1 IP Services	
5.1 a Time Synchronization	Description of the need for synchronizing time in an environment, operation of Network Time Protocol to keep time consistent across devices.
5.1. b First-Hop Redundancy Protocols	How multiple routers can provide resilient gateway functionality to hosts at the Layer 2/Layer 3 boundaries.
5.1. c Network Address Translation	How a router can translate IP addresses from one network realm to another.
5.2 Overlay Tunnels	
5.2. a Generic Routing Encapsulation (GRE)	Explanation, configuration and verification of GRE tunnels.
5.2. b IPSec Fundamentals	IPsec fundamentals and how to configure and verify IPsec.
5.2. c Cisco Location/ID Separation Protocol (LISP)	Explanation of architecture, protocols, and operation of LISP.
5.2. d Virtual Extensible Local Area Network (VXLAN)	Description of VXLAN as a data plane protocol that is open to operate with any control plane protocol.
Practical labs	
Implementation of NTP	
Implementation of HSRP. VRRP and GLBP protocols	
Implementation of GRE and IPSec site-to-site tunnels	

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

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

SELF STUDY – video lectures available	
Multicast	
Multicast Fundamentals	Multicast concepts and the need for multicast.
Multicast Addressing	Multicast address scopes used by multicast to operate at Layer 2 and Layer 3.
Internet Group Mangement Protocol (IGMP)	Explanation of how multicast receivers join multicast groups to start receiving multicast traffic using IGMPv2 or IGMPv3. IGMP snooping.
Protocol Independent Multicast	Concepts, operation, and features of PIM used to route multicast traffic across network segments from a multicast source to a group of receivers.
Rendezvous Points	Purpose, function, and operation of rendezvous points in a multicast network.
QoS	
The Need for QoS	Description of the leading causes of poor QoS and how can be alleviated by using QoS tools and mechanisms.
QoS Modes	Explanation of the three different models available for implementing QoS in a network: best effort, Integrated Services (IntServ), and Differentiated Services (DiffServ).
Classification and Marking	Description of classification, which is used to identify and assign IP traffic into different traffic classes, and marking, which is used to mark packets with a specified priority based on classification or traffic conditioning policies.

Policing and Shaping	How policing is used to enforce rate limiting, where excess IP traffic is either dropped, marked, or delayed.
Congestion Management and Avoidance	Description of congestion management, which is a queueing mechanism used to prioritize and protect IP traffic. It also describes congestion avoidance, which involves discarding IP traffic to avoid network congestion.
Wireless Signals and Modulation	
Understanding Basic Wireless Theory	Theory behind radio frequency (RF) signals, as well as measuring and comparing the power of RF signals.
Carrying Data Over an RF Signal	An overview of basic methods and standards that are involved in carrying data wirelessly between devices and the network.
Wireless Infrastructure	
Wireless LAN Topologies	Autonomous, cloud-based, centralized, embedded, and Mobility Express wireless architectures.
Pairing Lightweight APs and WLCs	Explanation of the process that lightweight APs must go through to discover and bind to a wireless LAN controller
Leveraging Antennas for Wireless Coverage	An overview of various antenna types and explains how each one alters the RF coverage over an area.
Understanding Wireless Roaming and Location Services	
Roaming Overview:	This section discusses client mobility from the AP and controller perspectives.
Roaming Between centralized Controllers	Explanation of the mechanisms that allow wireless devices to roam from one AP/controller pair onto another
Authenticating Wireless Clients	
Open Authentication	Authentication of wireless users using no credentials.
Authenticating with Pre-Shared Key	Authentication of clients with a static key that is shared prior to its use.
Authenticating with EAP	Authentication of clients with Extensible Authentication Protocol (EAP).
Authenticating with WebAuth	Authentication of clients through the use of a web page where credentials are entered.
Troubleshooting Wireless Connectivity	
Troubleshooting Client Connectivity from the WLC	How to use a wireless LAN controller as a troubleshooting tool to diagnose problems with wireless clients.
Troubleshooting Connectivity Problems at the AP	How to diagnose problems between a wireless LAN controller and an AP that might affect wireless client connectivity.
Enterprise Network Architecture	
Hierarchical LAN Design Model	Hierarchical network design, how it improves performance, simplifies design, increases scalability, and reduces troubleshooting time.
Enterprise Network Architecture Options	Different options available for deploying an enterprise campus architecture based on the hierarchical LAN design model.
Fabric Technologies	
Software-Defined Access (SD-Access)	Benefits of SD-Access over traditional campus networks as well as the components and features of the Cisco SD-Access solution.
Software-Defined WAN (SD-WAN)	Benefits of SD-WAN over traditional WANs as well as the components and features of the Cisco SD-WAN solution, including the orchestration plane, management plane, control plane, and data plane.
Network Assurance	
Network Diagnostic Tools	Use cases and operations of ping, traceroute, SNMP, and syslog.
Debugging	Value of using debugging as a troubleshooting tool and provides basic configuration examples.
NetFlow and Flexible Netflow	Benefits and operations of NetFlow and Flexible NetFlow.
Switched Port Analyzer (SPAN) Technologies	Benefits and operations of SPAN, RSPAN, and ERSPAN.
IP SLA	IP SLA and the value of automated network probes and monitoring.
Cisco DNA Center Assurance	A high-level overview of Cisco DNA Center Assurance and associated workflows for troubleshooting and diagnostics.

Secure Network Access Control	
Network Security Design for Threat Defense	Cisco security framework to protect networks from evolving cybersecurity threats.
Next-Generation Endpoint Security	Description of security components such as next-generation firewalls, Web Security Appliance (WSA), and Email Security Appliance (ESA).
Network Access Control (NAC)	Description of technologies such as 802.1x, Web Authentication (WebAuth), MAC Authentication Bypass (MAB), TrustSec and MACsec to enforce network access control
Secure Network Access Control	
Access Control Lists (ACLs)	How to configure and verify ACLs to secure the network infrastructure
Terminal Lines and Password Protection	How to configure and verify local network device access control through local usernames and passwords for authentication and how to configure and verify role-based access control (RBAC) through privilege levels.
Authentication, Authorization, and Accounting (AAA)	How to configure and verify network device access control on IOS through an AAA TACACS+ server.
Zone-Based Firewall (ZBFW)	How to configure and verify stateful firewall functionality on IOS routers.
Control Plane Policing	How to configure and verify CoPP, which is used to protect the route processor (RP) or CPU of a router.
Device Hardening	Additional configuration tips for hardening the security of IOS routers.
Virtualization	
Server Virtualization	Description of server virtualization technologies such as virtual machines, containers, and virtual switching.
Network Functions Virtualization	Description of the NFV architecture and its application to an enterprise network.
Foundational Network Programmability Concepts	
Command-Line Interface	An overview of the pros and cons of managing devices with the traditional command-line interface approach.
Application Programming Interface	Description of what APIs are, the different types of APIs, and how they are used.
Data Models and Supporting Protocols	Description of the most common data models and associated tools.
Cisco DevNet	A high-level overview of the various Cisco DevNet components and learning labs.
GitHub	Illustration of different use cases for version control and the power of community code sharing.
Basic Python Components and Scripts	Components of Python scripts and how to interpret them.
Introduction to Automation Tools	
Embedded Event Manager	Common use cases and operations of the on-box EEM automation tool as well as the Tcl scripting engine.
Agent-Based Automation Tools	Benefits and operations of the various agent-based automation tools.
Agentless Automation Tools	Benefits and operations of the various agentless automation tools.