SAGI RAMA KRISHNAM RAJU ENGINEERING COLLEGE

(AUTONOMOUS)

(Approved by AICTE, New Delhi, Affiliated to JNTUK, Kakinada)

Accredited by NAAC with 'A+' Grade

Recognised as Scientific and Industrial Research Organisation

SRKR MARG, CHINA AMIRAM, BHIMAVARAM – 534204 W.G.Dt., A.P., INDIA

Estd. 1980

Regulation: R23

INFORMATION TECHNOLOGY (Honors)

COURSE STRUCTURE
(With effect from 2023-24 admitted Batch onwards)

Course Code	Course Name	Year/ Sem	Cr	L	T	P	C.I.E	S.E.E	Total Marks
B23ITH101	Switching Routing and Wireless Essentials	III-I	3	3	0	0	30	70	100
B23ITH201	Enterprise Networking Security Automation	III-II	3	3	0	0	30	70	100
B23ITH301	Cyber Operations	IV-I	3	3	0	0	30	70	100
B23ITH401	*MOOCS-I	III-I to IV-I	3	--	--	--	--	--	100
B23ITH501	*MOOCS-II	III-I to IV-I	3	--	--	--	--	--	100
B23ITH601	*MOOCS-III	III-I to IV-I	3	--	--	--	--	--	100
		TOTAL	**18**	**12**	**0**	**0**	**120**	**280**	**600**

*Three MOOCS courses of any **INFORMATION TECHNOLOGY** related Program Core Courses from NPTEL/SWAYAM with a minimum duration of12 weeks (3 Credits) courses other than the courses offered need to be taken by prior information to the concern. These courses should be completed between III Year I Semester to IV Year I Semester

Subject Code	Category	L	T	P	C	I.M	E.M	Exam
B23ITH101	**Honors**	**3**	**--**	**--**	**3**	**30**	**70**	**3 Hrs**

SWITCHING, ROUTING AND WIRELESS ESSENTIALS

(Honors Degree Course in ME)

Course Objectives:

1.	Understand and configure network switching and routing essentials by setting up switches, routers, VLANs, and troubleshooting network access layer issues.
2.	Implement secure and efficient network configurations by utilizing STP, Ether Channel, DHCP, VLAN trunking, and Inter-VLAN routing for scalable network design.
3.	Analyze and configure dynamic and static routing protocols to establish robust IP routing tables and optimize packet forwarding mechanisms.
4.	Examine and deploy wireless LAN technologies by configuring WLAN standards, security mechanisms, and troubleshooting wireless threats.

Course Outcomes: By the end of the course, the student should have the ability to:

S.No	Outcome	Knowledge Level
1.	Use the appropriate commands and perform basic switch and router configuration.	K3
2.	Build VLANs and configure inter VLAN routing.	K3
3.	Explain STP, DHCPv4, FHRP, Switch security concepts.	K2
4	Demonstrate static routing configuration skills.	K3
5	Illustrate WLAN concepts, WLAN security, and WLAN configuration steps.	K3

SYLLABUS

UNIT-I **(10 Hrs)**	Configuring a switch with initial settings: Switch boot sequence, Switch LEDs, recover from system crash, Switch management access & SVI configuration example; Configuring a switch with initial settings: Duplex communication, configure switchport at physical layer, AUTO-MDIX, Switch verification commands; Network access layer issues, Interface input output errors, troubleshooting network access layer issues.; Secure remote access: Telnet operation, SSH operation, configure SSH, verify SSH. Basic router configuration: Configure basic router settings, Dual stack topology, configure router interfaces, IPv4 loopback interfaces.; Verify directly connected networks: interface verification commands, verify interface status, verify IPv6 link local and multicast addresses, verify interface configuration, verify routes, filtering show command output, command history.; Switching Concepts: Frame forwarding methods, collision domains, broad domains, Features of the switch that alleviate congestion.; VLANs: Overview, definitions, types.

UNIT-II (8 Hrs)	VLANs in a Multi-Switched Environment: Defining VLAN trunks, Networks without VLANs, Networks with VLANs, VLAN identification with a Tag.; Native VLANs and 802.1Q tagging, Voice VLAN tagging, Voice VLAN verification.; VLAN: Configuration, VLAN ranges in Catalyst Switch, VLAN creation commands with example, VLAN port assignment commands.; Data and Voice VLAN example, verify VLAN information, change VLAN port membership, Delete VLANs. VLAN trunks: Trunk configuration commands, Trunk configuration example, verify trunk configuration, reset the trunk to default.; Dynamic Trunking Protocol (DTP): Introduction to DTP, Negotiated Interface Modes, Results of a DTP configuration, verify DTP mode.; Inter VLAN routing: Definitions, Legacy inter-VLAN routing, ‘router-on-a-stick’ inter-VLAN routing.; Inter-VLAN Routing on a Layer 3 Switch, Router-on-a-Stick Scenario (configurations)
UNIT-III (12 Hrs)	Part 1:Purpose of STP, STP operations: Steps to a Loop-Free Topology, Elect the root bridge, Elect the root ports, Elect designated ports, Elect alternate (blocked) ports.; Elect a Root Port from Multiple Equal-Cost Paths, STP Timers and Port States, Operational Details of Each Port State, Per-VLAN Spanning Tree, Different Versions of STP.; EtherChannel: Link aggregation, EtherChannel technology, Advantages of EtherChannel.; EtherChannel implementation restrictions, AutoNegotiation Protocols, PAgP operation, LACP Operation, Configure EtherChannel, verify EtherChannel; DHCPv4: Server and Client, DHCPv4 operation, configure a Cisco IOS DHCPv4 Server.; Verify DHCPv4 is Operational, Disable the Cisco IOS DHCPv4 Server, DHCPv4 Relay; Other Service Broadcasts Relayed, Configure a DHCPv4 Client. Part 2:First Hop Redundancy Protocols (FHRP): Default Gateway Limitations, Router Redundancy, Steps for Router Failover, FHRP Options; HSRP Overview, HSRP Priority and Preemption, HSRP States and Times.; LAN Security: Endpoint security: Network attacks today, Network security devices, Endpoint protection.; Cisco ESA, Cisco WSA, Access Control: Authentication with a Local Password, AAA components. 802.1X, Layer 2 Vulnerabilities, Switch attack categories, Switch attack mitigation techniques.; MAC address table attack, mitigation, VLAN hopping attack.; VLAN Double-Tagging attack, DHCP attacks.; ARP Attacks, STP Attacks, and CDP Reconnaissance.
UNIT-IV (8 Hrs)	Routing concepts: Functions of router, example, longest match for IPv4 and IPv6, Build the routing table.; Packet forwarding decision process, Packet forwarding mechanism; IP routing table: Route source, routing table principles, routing table entries, directly connected networks, static routes.; Dynamic routing protocols, Dynamic Routes in the Routing Table, Default route, structure of IPv4 routing table, structure of IPv6 routing table, Administrative distance. Static Vs Dynamic routing, Dynamic routing evolution, Dynamic routing protocol concepts, best path, load balancing.; IP Static routing: Types, next hop options, ip route command, ipv6 route command, configuring static routing.; Default static route, floating static routes.; Host routes, troubleshooting static and default routes.

UNIT-V (8 Hrs)	Wireless LAN (WLAN): Benefits, Types, Wireless technologies, 802.11 standards.; Wireless standard organizations, WLAN components.; WLAN Operation, 802.11 wireless topology modes, BSS and ESS, 802.11 frame structure.; CSMA/CA, Wireless client and AP association, Passive and Active discover modes, CAPWAP.Channel management: Frequency Channel saturation, Channel selection, plan a WLAN deployment.; WLAN threats: DoS attacks, Rouge access points, MITM attack, Securing WLAN: SSID Cloaking and MAC Address Filtering.; 802.11 Original Authentication Methods, Shared Key Authentication Methods, Authenticating a Home User, Encryption Methods, Authentication in the Enterprise, WPA 3.; The Wireless Router, WLAN configuration steps.
Text Books:	
1.	Switching, Routing, and Wireless Essentials v7.0 (SRWE) Companion Guide, Cisco Press.
References:	
1.	Cisco Networking Academy, CCNAv7, Switching, Routing, and Wireless Essentials Course

Course Code:B23ITH101

SAGI RAMA KRISHNAM RAJU ENGINEERING COLLEGE (A) **R23**

III B.Tech. I Semester MODEL QUESTION PAPER

SWITCHING, ROUTING, AND WIRELESS ESSENTIALS

(Honors Degree Course in ME)

Time: 3 Hrs. **Max. Marks: 70 M**

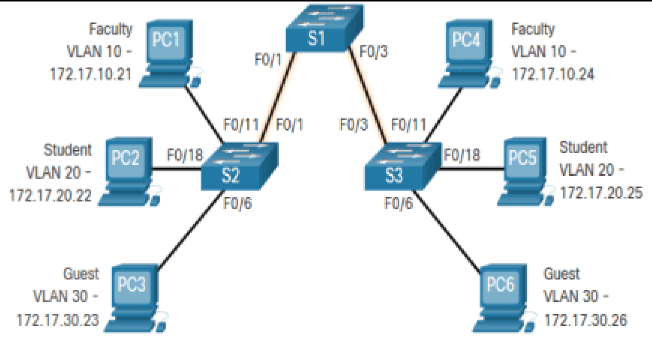
Answer Question No.1 compulsorily

Answer **ONE Question** from **EACH UNIT**

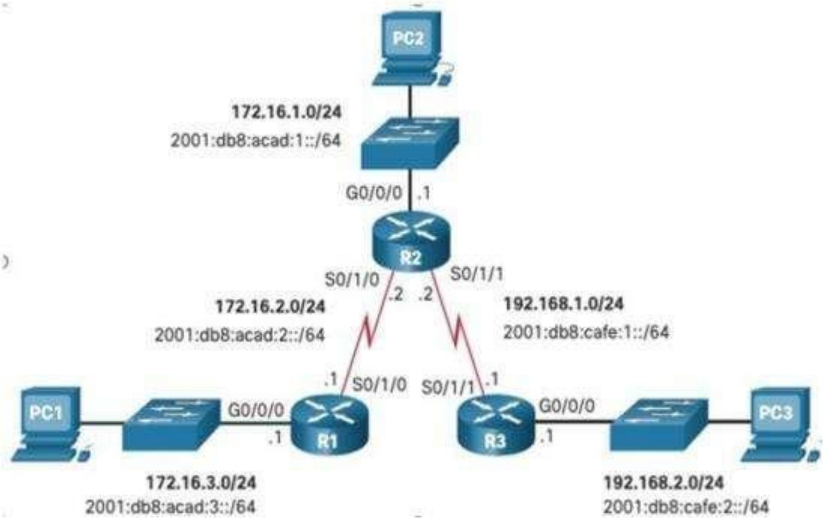
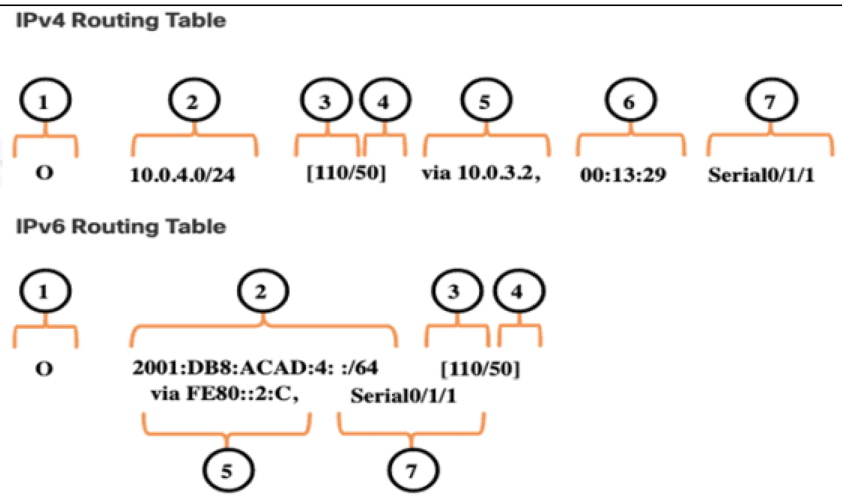
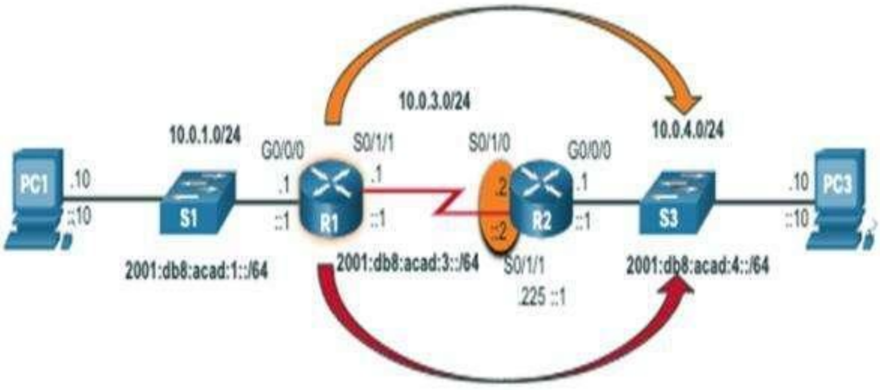
Assume suitable data if necessary

10 x 2 = 20 Marks

<table>
<tr><th></th><th></th><th></th><th>CO</th><th>KL</th><th>M</th></tr>
<tr><td>1.</td><td>a).</td><td>Identify the correct order of the switch boot sequence.</td><td>1</td><td>2</td><td>2</td></tr>
<tr><td></td><td>b).</td><td>Differentiate MAC address table and ARP Table.</td><td>1</td><td>2</td><td>2</td></tr>
<tr><td></td><td>c).</td><td>State two advantages of Layer 3 switch.</td><td>2</td><td>2</td><td>2</td></tr>
<tr><td></td><td>d).</td><td>Express the need for Native VLAN.</td><td>2</td><td>2</td><td>2</td></tr>
<tr><td></td><td>e).</td><td>Recognize the major cause of Layer 2 loops.</td><td>3</td><td>2</td><td>2</td></tr>
<tr><td></td><td>f).</td><td>Show the correct order of DHCP client server message types.</td><td>3</td><td>1</td><td>2</td></tr>
<tr><td></td><td>g).</td><td>Given below is the routing table entries of a certain router, consider the packet with destination IP address: 192.168.1.65 has arrived at this router, what is the next hop that the packet will be routed to? Justify.
<table>
<tr><th>Destination Network</th><th>Subnet Mask</th><th>Next Hop</th></tr>
<tr><td>192.168.0.0</td><td>255.255.0.0 (/16)</td><td>Router A</td></tr>
<tr><td>192.168.1.0</td><td>255.255.255.0 (/24)</td><td>Router B</td></tr>
<tr><td>192.168.1.64</td><td>255.255.255.192 (/26)</td><td>Router C</td></tr>
</table></td><td>4</td><td>3</td><td>2</td></tr>
<tr><td></td><td>h).</td><td>Justify the need for a default static route and show the command for the same.</td><td>4</td><td>2</td><td>2</td></tr>
<tr><td></td><td>i).</td><td>Differentiate autonomous and controller-based access points.</td><td>5</td><td>2</td><td>2</td></tr>
<tr><td></td><td>j).</td><td>State any four threats on wireless LAN.</td><td>5</td><td>1</td><td>2</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6"><b>5 x 10 = 50 Marks</b></td></tr>
<tr><td></td><td></td><td><b>UNIT-1</b></td><td></td><td></td><td></td></tr>
<tr><td>2.</td><td>a).</td><td>Explain the switch boot sequence.</td><td>1</td><td>2</td><td>5</td></tr>
<tr><td></td><td>b).</td><td>Configure SSH on a Cisco switch by choosing the appropriate commands in proper order.</td><td>1</td><td>3</td><td>5</td></tr>
<tr><td></td><td></td><td><b>OR</b></td><td></td><td></td><td></td></tr>
<tr><td>3.</td><td>a).</td><td>Show any five switch verification commands and describe.</td><td>1</td><td>2</td><td>5</td></tr>
<tr><td></td><td>b).</td><td>Configure a cisco router with basic router configuration steps.</td><td>1</td><td>3</td><td>5</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td><b>UNIT-2</b></td><td></td><td></td><td></td></tr>
<tr><td><b>4.</b></td><td><b>a).</b></td><td>Explain the benefits of VLANs</td><td><b>2</b></td><td><b>2</b></td><td><b>4</b></td></tr>
<tr><td></td><td>b).</td><td>

Refer the exhibit. Configure the following
i) Create three VLANs 10, 20, 30 on S2 and S3 and name them as shown in the figure.
ii) Faculty, Student, and Guest VLANs are data VLANS. Assign the VLANs to the switch ports as shown in the topology for switch S2 and S3</td><td>2</td><td>3</td><td>6</td></tr>
<tr><td></td><td></td><td><b>OR</b></td><td></td><td></td><td></td></tr>
<tr><td>5.</td><td>a).</td><td>Explain native VLAN and voice VLAN.</td><td>2</td><td>2</td><td>5</td></tr>
<tr><td></td><td>b).</td><td><table>
<tr><th>Sub interface</th><th>VLAN</th><th>IP Address</th></tr>
<tr><td>G0/0/1.10</td><td>10</td><td>192.168.10.1/24</td></tr>
<tr><td>G0/0/1.20</td><td>20</td><td>192.168.20.1/24</td></tr>
<tr><td>G0/0/1.30</td><td>99</td><td>192.168.99.1/24</td></tr>
</table>
The table shows the IP addresses of the sub-interfaces of router R1’s G0/0/1 interface. Configure the router R1 to support router on a stick inter VLAN routing.</td><td>2</td><td>3</td><td>5</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td><b>UNIT-3</b></td><td></td><td></td><td></td></tr>
<tr><td>6.</td><td>a).</td><td>Explain the major steps in STP.</td><td>3</td><td>2</td><td>5</td></tr>
<tr><td></td><td>b).</td><td>When a switch has multiple equal-cost paths to the root bridge, how does the switch determine a root port? Explain.</td><td>3</td><td>2</td><td>5</td></tr>
<tr><td></td><td></td><td><b>OR</b></td><td></td><td></td><td></td></tr>
<tr><td>7.</td><td>a).</td><td>Explain DHCP attacks.</td><td>3</td><td>2</td><td>5</td></tr>
<tr><td></td><td>b).</td><td>Explain FHRP.</td><td>3</td><td>2</td><td>5</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td><b>UNIT-4</b></td><td></td><td></td><td></td></tr>
<tr><td>8.</td><td>a).</td><td>Explain the structure of the routing table with examples.</td><td>4</td><td>2</td><td>5</td></tr>
</table>

	b).	Refer the exhibit.  PC2 172.16.1.0/24 2001:db8:acad:1::/64 G0/0/0 .1 R2 S0/1/0 .2 .2 S0/1/1 172.16.2.0/24 2001:db8:acad:2::/64 192.168.1.0/24 2001:db8:cafe:1::/64 .1 S0/1/0 S0/1/1 .1 PC1 G0/0/0 R1 .1 R3 G0/0/0 .1 PC3 172.16.3.0/24 2001:db8:acad:3::/64 192.168.2.0/24 2001:db8:cafe:2::/64 Assume that all the routers are already configured with the interface IP addresses as shown in the topology. Configure static routes in router R1 for all the remote destinations as per the topology.	4	3	5
		OR			
9.	**a).**	 IPv4 Routing Table 1 2 3 4 5 6 7 O 10.0.4.0/24 [110/50] via 10.0.3.2, 00:13:29 Serial0/1/1 IPv6 Routing Table 1 2 3 4 O 2001:DB8:ACAD:4: :/64 [110/50] via FE80::2:C, Serial0/1/1 5 7 Refer the exhibit. Identify all the fields 1 to 7 of IPv4 and IPv6 routing table entry.	**4**	**2**	**5**
	b).	Refer to the exhibit.  10.0.3.0/24 10.0.1.0/24 G0/0/0 S0/1/1 S0/1/0 G0/0/0 10.0.4.0/24 PC1 .10 ::10 S1 .1 ::1 R1 .1 ::1 .2 ::2 R2 .1 ::1 S3 .10 ::10 PC3 2001:db8:acad:1::/64 2001:db8:acad:3::/64 S0/1/1 225 ::1 2001:db8:acad:4::/64 Identify the directly connected networks and remote networks for	**4**	**3**	**5**

		routers R1 and R2. Configure static routes for the remote networks.			
		UNIT-5			
10.	a).	Explain wireless client Access Point (AP) association steps.	5	2	5
	b).	Discuss various threats that wireless LANs are susceptible to.	5	3	5
		OR			
11.	a).	Explain CSMA/CA.	5	2	5
	b).	Discuss various Wireless LAN security methods	5	3	5

CO-COURSE OUTCOME KL-KNOWLEDGE LEVEL M-MARKS

NOTE: Questions can be given as A, B splits or as a single Question for 10 marks

Subject Code	Category	L	T	P	C	I.M	E.M	Exam
B23ITH201	HON	3	--	--	3	30	70	3 Hrs

ENTERPRISE NETWORKING, SECURITY, AND AUTOMATION

(Honors Degree Course in ME)

Course Objectives:

1.	To learn dynamic routing, ACLs, NAT and WAN concepts and configurations.
2.	To gain an understanding of VPNs, traffic characteristics, network discovery protocols.
3.	To perform scalable network design and be able to trouble shoot.
4.	To gain knowledge of network automation and protocol vulnerabilities and security issues.

Course Outcomes: By the end of the course, the student should have the ability to:

S.No	Outcome	Knowledge Level
1.	Apply OSPF routing concepts and configure ACLs to control traffic flow and enhance network performance in enterprise networks.	K3
2.	Understand the mechanisms of NAT and WAN technologies and their roles in extending and securing enterprise network connectivity.	K2
3.	Apply VPN technologies, QoS mechanisms, and network discovery tools to enhance data transmission reliability and manage network resources effectively.	K3
4	Apply network design principles and structured troubleshooting methods to build scalable networks and resolve connectivity issues.	K3
5	Understand the fundamentals of network automation and security, including SDNs, APIs, and common network vulnerabilities and their countermeasures.	K3

SYLLABUS

UNIT-I (10 Hrs)	Dynamic routing and ACLs Introduction to OSPF, Components of OSPF, Link state operation, single area & multi-area OSPF; OSPF Packets, OSPF Operational States, establish neighbor adjacencies, Synchronizing OSPF database; Single area OSPF configuration; Multi-access OSPF, DR/BDR election process; OSPF Cost metrics, verify and modify hello and dead intervals, propagate default static route; ACLs, Purpose of ACL, ACL operation; Wildcard mask in ACL, Guidelines for creating ACLs; Standard ACLs.
UNIT-II (8 Hrs)	NAT and WAN Concepts Extended ACLs; What is NAT, How NAT works, NAT terminology; Types of NAT; Advantages and Disadvantages of NAT, Static NAT; Dynamic NAT; PAT, NAT64; WAN Concepts: LANs Vs WANs, WAN topologies, Traditional WAN connectivity; Modern WAN connectivity, Internet based connectivity.

UNIT-III (12 Hrs)	VPN, QoS, Network discovery Part 1: VPN Technology; Types of VPNs; IPSec; Network Transmission Quality; Traffic characteristics; Queuing Algorithms, QoS Models; QoS implementation techniques: Avoiding packet loss, Classification and Marking; Congestion Avoidance, Shaping and Policing. Part 2: Device discovery with CDP; Device discovery with LLDP; NTP; SNMP; Syslog; Router and Switch File Maintenance; Password recovery procedure; IoS image management.
UNIT-IV (8 Hrs)	Network Design Hierarchical Networks; Scalable Networks; Switch Hardware; Router Hardware; Network Documentation; Network Trouble shooting process; Symptoms and Causes of Network Problems; Troubleshooting IP Connectivity.
UNIT-V (8 Hrs)	Network Automation and Security Network Virtualization, Cloud computing and Virtualization; Virtual network infrastructure, SDNs; Network Automation overview, data formats; APIs, REST IBN and Cisco DNA Center; Current state of Cyber security, IP Vulnerabilities and Threats; TCP and UDP vulnerabilities, ARP vulnerabilities, DNS attacks; DHCP attacks, Network security best practices.
Text Books:	
1.	Enterprise Networking, Security, and Automation Companion Guide CCNAv7, Cisco Press
References:	
1.	Cisco Networking Academy, CCNAv7, Enterprise Networking, Security, and Automation Course

.

Course Code: B23ITH201

SAGI RAMA KRISHNAM RAJU ENGINEERING COLLEGE (A) R23

III B.Tech. II Semester MODEL QUESTION PAPER

ENTERPRISE NETWORKING, SECURITY, AND AUTOMATION

(Honors Degree Course in ME)

Time: 3 Hrs. **Max. Marks: 70 M**

Answer Question No.1 compulsorily

Answer **ONE Question** from **EACH UNIT**

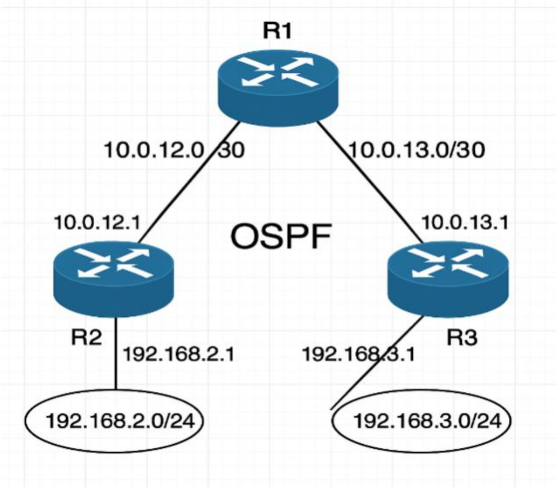
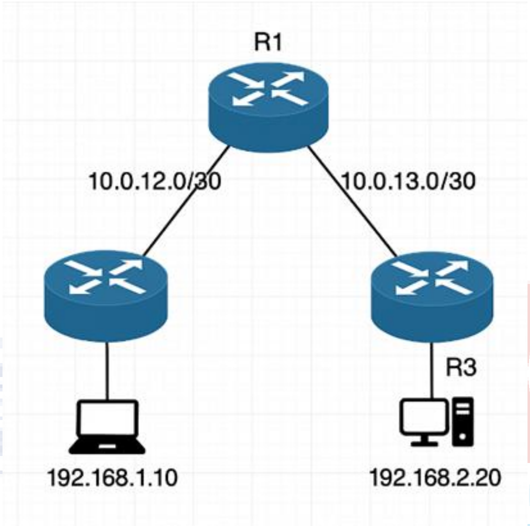
Assume suitable data if necessary

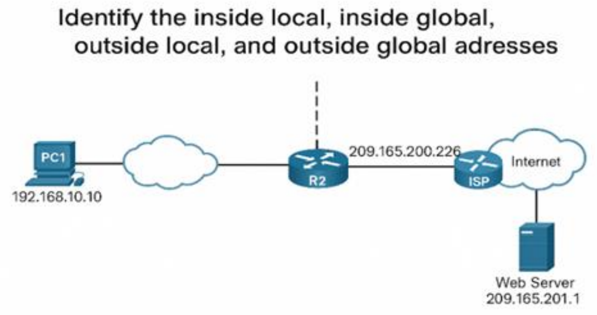
10 x 2 = 20 Marks

			CO	**KL**	**M**
1.	a).	Summarize the advantages of link state routing over distance vector routing.	1	2	2
	b).	For the given subnet mask, calculate the wild card mask: i) 255.255.255.0 ii) 255.255.255.192 iii) 255.240.0.0 iv) 255.255.252.0	1	2	2
	c).	Identify the four types of NAT addresses.	2	1	2
	d).	Differentiate single-carrier and dual-carrier WAN connection.	2	2	2
	e).	State the benefits of VPN.	3	1	2
	f).	Name the four possible destinations of syslog messages.	3	2	2
	g).	Identify any four business considerations for switch selection.	4	2	2
	h).	Differentiate physical topology and logical topology.	4	2	2
	i).	Define Type-2 hypervisor.	5	1	2
	j).	Identify the RESTful Operations for the HTTP Methods POST, GET, PUT, and DELETE.	5	2	2

5 x 10 = 50 Marks

		UNIT-1			
2.	a).	Explain the OSPF packet types.	1	2	5
	b).	Discuss placement strategies of ACLs.	1	3	5
		OR			
3.	a).	Refer to the exhibit. Configure OSPF on three routers R1, R2, and R3	1	3	6

		 R1 10.0.12.0/30 10.0.13.0/30 10.0.12.1 OSPF 10.0.13.1 R2 192.168.2.1 192.168.3.1 R3 192.168.2.0/24 192.168.3.0/24			
	b).	 R1 10.0.12.0/30 10.0.13.0/30 R3 192.168.1.10 192.168.2.20 Refer to the exhibit and configure the commands for standard ACL. i) On **R2**, deny access to the network from the host 192.168.1.10 (connected to R2), and allow all other traffic. Apply the ACL inbound on the LAN interface. ii) On **R3**, allow only the host 192.168.2.20 (connected to R3) to access the router and deny all others. Apply the ACL inbound on the LAN interface. iii) On **R2**, block all traffic from the network 192.168.1.0/24 to any destination. Apply the ACL on the interface closest to the source (LAN interface). iv) On **R3**, deny access only to host 192.168.2.20 and permit all other traffic. Apply the ACL inbound on the LAN interface.	1	3	4
		UNIT-2			
4.	**a).**	Refer to the exhibit. The edge router R2's global ip address is 209.165.200.226. Explain the NAT table of R2.	**2**	**2**	**5**

		 Identify the inside local, inside global, outside local, and outside global adresses PC1 192.168.10.10 R2 209.165.200.226 ISP Internet Web Server 209.165.201.1			
	b).	Explain PAT with an example.	**2**	**2**	**5**
		OR			
5.	**a).**	Discuss the advantages and disadvantages of NAT.	**2**	**2**	**5**
	b).	Differentiate static and dynamic NAT with examples.	**2**	**2**	**5**
		UNIT-3			
6.	**a).**	Explain IPSec. How is confidentiality, integrity, and authentication provided in IPSec?	**3**	**3**	**5**
	b).	Explain remote access and site-to-site VPN.	**3**	**2**	**5**
		OR			
7.	**a).**	Differentiate Weighted Fair Queuing (WFQ) and Class-Based Weighted Fair Queuing (CBWFQ).	**3**	**3**	**5**
	b).	Tabulate the syslog message levels and severity levels	**3**	**2**	**5**
		UNIT-4			
8.	**a).**	Explain two-tier and three-tier campus networks, and in what case you will use them.	**4**	**3**	**5**
	b).	Recommend any four ways scalable networks can be built.	**4**	**3**	**5**
		OR			
9.		Explain the seven-step trouble shooting process with a neat flow diagram.	**4**	**3**	**10**
		UNIT-5			
10.	**a).**	Explain the difference between Type-1 and Type-2 hypervisors with a neat diagram and example.	**5**	**3**	**5**
	b).	Explain RESTful API with an example.	**5**	**3**	**5**
		OR			
11.	**a).**	Explain DNS attacks.	**5**	**3**	**5**
	b).	Explain DHCP attacks.	**5**	**3**	**5**

CO-COURSE OUTCOME KL-KNOWLEDGE LEVEL M-MARKS

NOTE: Questions can be given as A, B splits or as a single Question for 10 marks