JADAVPUR UNIVERSITY

COMPUTER AIDED DESIGN CENTRE

Faculty Council of Engineering and Technology

Kolkata - 700 032

Certificate Course on

Network Security

Scope

Large Scale network comprising firewall, server, router, switches, access points, servers, etc; is now an absolute must for any mid-size company. Organizations require system admins to configure, maintain and secure such network infrastructure. This course focuses on building the technical skills to become a system administrator.

The topics include connecting to a WAN, implementing network security, network types, network media, routing and switching fundamentals, the TCP/IP and OSI models, IP addressing, WAN technologies, operating and configuring IOS devices, extending switched networks with VLANs, determining IP routes, managing IP traffic with access lists, and establishing point-to-point connections.

Course Duration: 32 hrs.

Eligibility: Higher Secondary passed with basic knowledge of computer hardware
Participants must have mobile devices running Android 4.0.3 or above; laptop/desktop computer with Windows; and stable internet connectivity. Google Meet should be preinstalled the mobile device.

Course Content

Sl. No.	Topic	Theory hours	Practical hours	Total No. of hours
1	• Compare and contrast OSI and TCP/IP models • Compare and contrast TCP and UDP protocols • Compare and contrast network topologies 1. Star 2. Mesh 3. Hybrid • Configure, verify, and troubleshoot IPv4 addressing and subnetting • Compare and contrast IPv4 address types 1. Unicast 2. Multicast 3. Broadcast • Describe and verify switching concepts 1. MAC learning and aging 2. Frame switching 3. Frame flooding 4. MAC address table	1	1	2

	• Interpret Ethernet frame format • Troubleshoot interface and cable issues (collisions, errors, duplex, speed)			
2	• Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches 1. Access ports (data and voice) 2. Default VLAN • Configure, verify, and troubleshoot interswitch connectivity 1. Trunk ports 2. Add and remove VLANs on a trunk 3. DTP, VTP (v1&v2), and 802.1Q 4. Native VLAN • Configure, verify, and troubleshoot STP protocols 1. STP mode (PVST+ and RPVST+) 2. STP root bridge selection • Configure, verify and troubleshoot STP related optional features 1. Port Fast 2. BPDU guard	1	1	2
3	• Configure and verify Layer 2 protocols 1. Cisco Discovery Protocol 2. LLDP • Configure, verify, and troubleshoot (Layer 2/Layer 3) EtherChannel 1. Static 2. PAGP 3. LACP • Describe the routing concepts 1. Packet handling along the path through a network 2. Forwarding decision based on route lookup 3. Frame rewrite • Interpret the components of a routing table 1. Prefix 2. Network mask 3. Next hop 4. Routing protocol code 5. Administrative distance 6. Metric 7. Gateway of last resort • Describe how a routing table is populated by different routing information sources 1. Admin distance • Configure, verify, and troubleshoot inter-VLAN routing 1. Router on a stick 2. SVI	1	1	2
4	• Compare and contrast static routing and dynamic routing • Compare and contrast distance vector and link state routing protocols • Compare and contrast interior and exterior routing protocols • Configure, verify, and troubleshoot IPv4 and IPv6 static routing	1	1	2

	1. Default Route 2. Network Route 3. Host Route 4. Floating Static			
5	• Configure, verify, and troubleshoot single area and multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs) • Configure, verify, and troubleshoot single area and multi-area OSPFv3 for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs	1	1	2
6	• Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub) • Configure, verify, and troubleshoot EIGRP for IPv6 (excluding authentication,filtering, manual summarization, redistribution, stub)	1	1	2
7	• Configure, verify, and troubleshoot RIPv2 for IPv4(excludingauthentication,filtering, manual summarization, redistribution) • Troubleshoot basic Layer 3 end-to-end connectivity issues	1	1	2
8	• Configure and verify PPP and MLPPP on WAN interfaces using local authentication • Configure, verify, and troubleshoot PPPoE client-side interfaces using local authentication • Configure, verify, and troubleshoot GRE tunnel connectivity	1	1	2
9	• Describe WAN topology options 1. Point-to-point 2. Hub and spoke 3. Full mesh 4. Single vs dual-homed • Describe WAN access connectivity options 1. MPLS 2. METRO ETHERNET 3. BROADBAND PPoE 4. Internet VPN (DMVPN, site-to-site VPN,client VPN)	1	1	2
10	• Internet VPN (DMVPN, site-to-site VPN, client VPN) • Describe basic QoS concepts 1. Marking 2. Device trust 3. Prioritization a. voice b. video c. data • Shaping • Policing	1	1	2

	• Congestion Management			
11	• Describe DNS lookup operation • Troubleshoot client connectivity issues involving DNS • Configure and verify DHCP on a router(excluding staticreservations) 1. Server 2. Relay 3. Client 4. TFTP, DNS, and gateway options • Troubleshoot client-and router-based DHCP connectivity issue	1	1	2
12	• Configure, verify, and troubleshoot basic HSRP 1. Priority 2. Pre-emption 3. Version • Configure, verify, and troubleshoot inside source NAT 1. Static 2. Pool 3. PAT • Configure and verify NTP operating in a client/server mode	1	1	2
13	• Configure, verify, and troubleshoot port security 1. Static 2. Dynamic 3. Sticky 4. Max MAC addresses 5. Violation actions 6. Err-disable recovery • Describe common access layer threat mitigation techniques 1. 802.1x 2. DHCP snooping 3. Nondefault native VLAN • Configure, verify, and troubleshoot IPv4 and IPv6 access list for traffic filtering 1. Standard 2. Extended 3. Named	1	1	2
14	• Verify ACLs using the APIC-EM Path Trace ACL Analysis tool • Configure, verify, and troubleshoot basic device hardening 1. Local authentication 2. Secure password 3. Access to device A. Source address B. Telnet/SSH 4. Login banner • Describe device security using AAA with TACACS+ and RADIUS	1	1	2
15	• Configure and verify device-monitoring protocols 1. SNMPv2 2. SNMPv3 3. Syslog	1	1	2

	• Troubleshoot network connectivity issues using ICMP echo-based IP SLA 1. Backup and restore device configuration 2. Using Cisco Discovery Protocol or LLDP for device discovery 3. Licensing 4. Logging 5. Timezone 6. Loopback • Configure and verify initial device configuration			
16	• Perform device maintenance 1. Cisco IOS upgrades and recovery (SCP, FTP, TFTP, and MD5 verify) 2. Password recovery and configuration register 3. File system management • Use Cisco IOS tools to troubleshoot and resolve problems 1. Ping and traceroute with extended option 2. Terminal monitor 3. Log events 4. Local SPAN • Describe network programmability in enterprise network architecture 1. Function of a controller 2. Separation of control plane and data plane 3. Northbound and southbound APIs	1	1	2
	Total	16	16	32

Doubt Clearing Session: *One extra session for 2 hours at the end of the course.*

Certificate: Completion certificate (in printed form) will be provided at the end of the course.