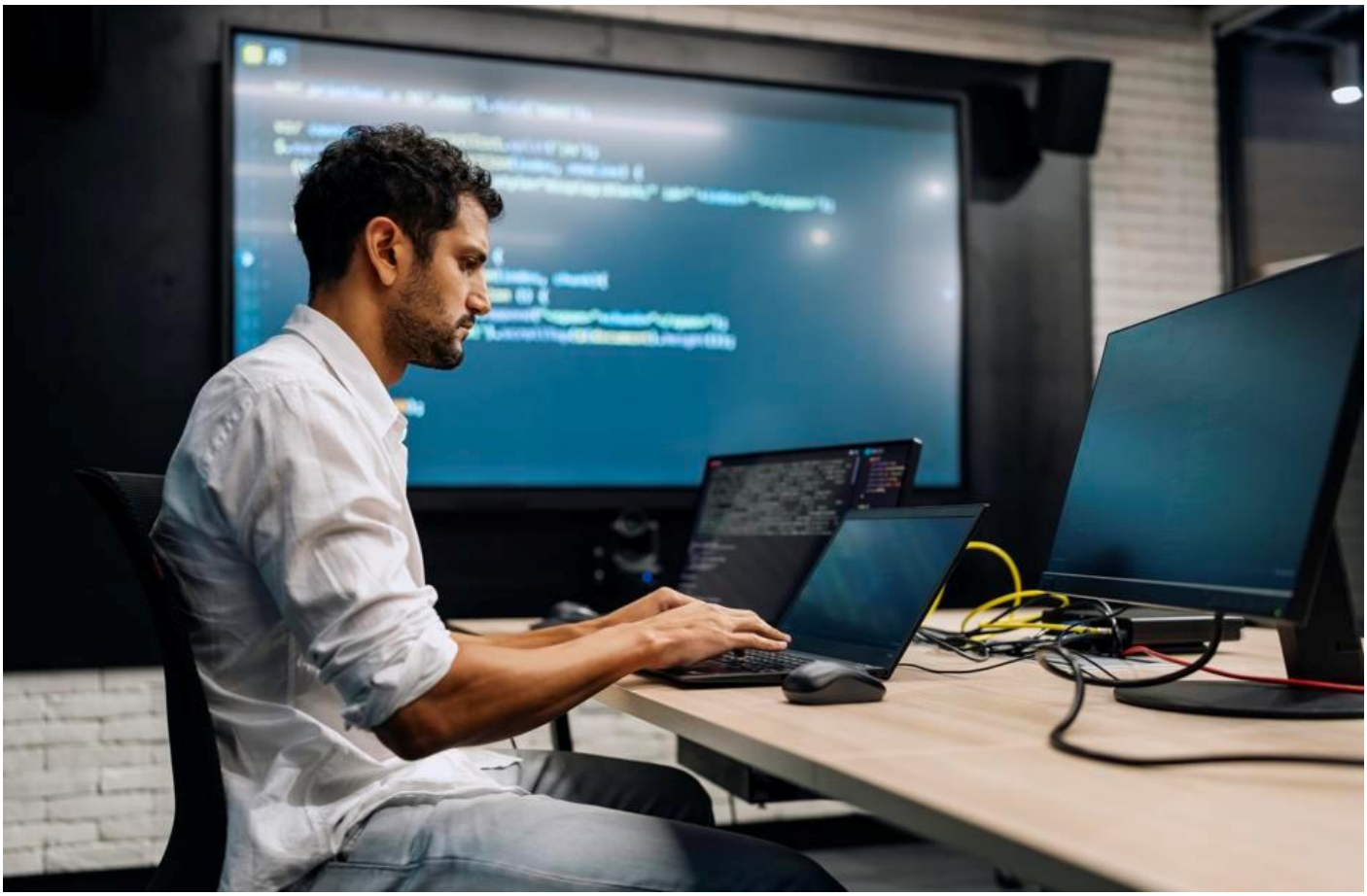

IT Network Systems Administration

QP Code: TEL/Nxxxx

QP Version: 1.0

NSQF Level: 4.5

Model Curriculum Version: 1.0

Telecom Sector Skill Council || 3rd Floor, Plot No. 126, Sector – 44

Gurgaon – 122003

Table of Contents

Training Parameters

Sector	Telecom
Sub-Sector	Network Managed Services
Occupation	Network Operation and Maintenance
Country	India
NSQF Level	4.5
Aligned to NCO/ISCO/ISIC Code	
Minimum Educational Qualification and Experience	NA
Pre-Requisite License or Training	NA
Age Limit	16 to 25 Years
Last Reviewed On	
Next Review Date	
NSQC Approval Date	
QP Version	1.0
Model Curriculum Creation Date	
Model Curriculum Valid Up to Date	
Model Curriculum Version	1.0
Minimum Duration of the Course	450
Maximum Duration of the Course	450

Program Overview

This section summarises the end objectives of the program along with its duration.

Training Outcomes

At the end of the program, the learner should have acquired the listed knowledge and skills to:

- Install, configure, and upgrade operating systems, network devices, servers, and related IT infrastructure as per organisational standards and security policies.
- Monitor system performance, identify faults, diagnose issues, and troubleshoot hardware, software, and network problems to minimise downtime and ensure continuity of services.
- Deliver timely technical support, interact professionally with users, provide clear guidance, document issues, and ensure user satisfaction while maintaining service levels.
- Apply security best practices, configure access control, perform regular updates/patching, and support disaster recovery processes to safeguard systems and organisational data.
- Plan and design network architectures, analyse performance data, recommend improvements, and support the development of scalable and efficient IT systems.

Compulsory Modules

The table lists the modules and their duration corresponding to the Compulsory NOS of the QP.

NOS and Module Details	Theory Duration	Practical Duration	On-the-Job Training Duration (Mandatory)	On-the-Job Training Duration (Recommended)	Total Duration
TEL/Nxxxx: Maintain work organisation and management NOS Version- 1.0 NSQF Level- 4	**20:00**	**30:00**	**10:00**	**-**	**60:00**
Module 1 Introduction and Overview of WorldSkills (Bridge Module)	05:00	00:00	00:00	-	05:00
Module 2: Work organisation and management	15:00	30:00	10:00		55:00
TEL/Nxxxx: Communicate Effectively and Demonstrate Interpersonal Skills NOS Version- 1.0 NSQF Level- 4	**20:00**	**30:00**	**10:00**	**-**	**60:00**
Module 3: Communication and Interpersonal Skills	20:00	30:00	10:00	-	60:00
TEL/Nxxxx: Configure and Maintain Data Transfer Networks	**30:00**	**40:00**	**20:00**	**-**	**90:00**

NOS Version- 1.0 NSQF Level- 4					
Module 4: Data Transfer Networks	30:00	40:00	20:00	-	90:00
TEL/Nxxxx: Perform Network and System Operations NOS Version- 1.0 NSQF Level- 4	**30:00**	**40:00**	**20:00**	**-**	**90:00**
Module 5: Network and System Operations	30:00	40:00	20:00	-	90:00
TEL/Nxxxx: Implement Infrastructure Automation and Configuration Management NOS Version- 1.0 NSQF Level- 4	**30:00**	**20:00**	**40:00**	**-**	**90:00**
Module 6: Infrastructure Automation	30:00	20:00	40:00	-	90:00
TEL/Nxxxx: Troubleshoot IT Systems, Networks, and Services NOS Version- 1.0 NSQF Level- 4	**20:00**	**20:00**	**20:00**	**-**	**60:00**
Module 8: Troubleshooting	20:00	20:00	20:00	-	60:00
Total Duration	**150:00**	**180:00**	**120:00**	**-**	**450:00**

Module Details

Module 1: Introduction and Overview of WorldSkills

Bridge Module

Terminal Outcomes:

- Outline the overview of the WorldSkills Competition.

Duration: 5:00	**Duration: 00:00**
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Discuss the objectives and benefits of the WorldSkills Competitions. • Explain about the network systems.	
Classroom Aids	
Whiteboard, Markers, Notebooks, Pens, Audio-visual training materials, laptop with an Internet connection, projector or large screen.	
Tools, Equipment and Other Requirements	

Module 2: Work organisation and management

Mapped to NOS: TEL/Nxxxx, v1.0

Terminal Outcomes:

- Apply health and safety principles, professional integrity, and secure work practices while handling IT equipment, data, and workplace resources.
- Demonstrate safe and efficient use of PPE, tools, and equipment while performing IT hardware and network-related tasks.
- Apply effective work organisation practices by planning, arranging, and maintaining a clean, safe, and productive work environment.

Duration: 15:00	**Duration: 30:00**
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Discuss health and safety legislation, obligations, regulations, and documentation. • Identify situations when personal protective equipment (PPE) must be used, e.g. for ESD (electrostatic discharge). • Explain how and why to seek assistance from peers when lacking in experience or knowledge in a particular area. • Explain the importance of integrity and security when dealing with user equipment and information. • State the importance of safe and secure disposal of waste for recycling. • Elaborate on the techniques of planning, scheduling, and prioritising. • Illuminate the significance of accuracy, checking, and attention to detail in all working practices. • State the importance of methodical working practices. • Discuss various collaboration and research methods and techniques. • Identify the value of managing one's own continuing professional development. • Discuss about speed of IT systems change and the need to maintain currency.	• Follow organisational health and safety standards, rules, and regulations during all IT network operations. • Maintain a safe and organised working environment by applying safety protocols and housekeeping practices. • Identify and use appropriate Personal Protective Equipment (PPE), including ESD protection devices, while handling electronic components. • Select, operate, clean, maintain, and store tools and equipment safely and securely as per manufacturer guidelines. • Plan the work area to maximise efficiency and maintain the discipline of regular tidying. • Schedule, reschedule, and prioritise multiple tasks effectively based on changing work requirements. • Work efficiently and check progress and outcomes regularly. • Undergo various certification requirements, such as Cisco, Microsoft, and Linux, specialising in at least one specific area. • Use thorough and efficient research methods to support knowledge growth. • Experiment with new methods, tools, and systems to adapt to emerging technologies and improve work practices. • Collaborate effectively with work colleagues to

	maximise efficiency and learning. • Work effectively as a member of a project team.
Classroom Aids:	
Training Kit (Trainer Guide, Presentations), Whiteboard, Markers, Notebooks, Pens, Audio-visual training materials, laptop with an Internet connection, projector or large screen	
Tools, Equipment and Other Requirements	
Personal Protective Equipment (ESD straps, Safety shoes, Safety goggles, Dust masks), Screwdrivers, Crimping tool, Tweezers, Pliers, Punch-down tool, Surge protectors, Cable organisers, Fire extinguisher (CO_2), Ethernet cables (Cat5e, Cat6), Cable testers, Loopback plugs, Network switches, Routers, Patch panels, Keystone jacks, Desktop PCs or laptops, cleaning materials (microfiber cloth & brushes).	

Module 3: Communication and interpersonal Skills

Mapped to NOS: TEL/Nxxxx, v1.0

Terminal Outcomes:

- Demonstrate effective listening and questioning skills to understand workplace situations and respond appropriately.
- Apply clear, accurate, and professional verbal and written communication while interacting with colleagues and stakeholders.
- Work collaboratively with colleagues by adapting communication style, supporting team activities, and maintaining productive workplace relationships.
- Manage workplace conflicts, misunderstandings, and emotional responses to maintain a positive and professional work environment.

Duration: 20:00	**Duration: 30:00**
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the importance of active listening as a key component of effective communication. • Describe the roles, responsibilities, and communication needs of colleagues within the workplace. • Discuss strategies for building and maintaining productive working relationships with colleagues and managers. • Identify techniques for effective teamwork in IT networks and support environments. • Explain methods for resolving misunderstandings and managing conflicting demands professionally. • Describe the process for managing tension and anger to handle difficult situations constructively.	• Apply strong listening and questioning techniques to accurately understand complex work situations. • Demonstrate effective verbal and written communication while interacting with colleagues in routine and non-routine tasks. • Adapt communication style and support methods to meet the changing needs of colleagues. • Contribute proactively to building and maintaining a strong, effective, and collaborative team environment. • Share knowledge, skills, and work insights with colleagues to promote a supportive learning culture. • Manage tension and anger professionally to reassure colleagues and facilitate constructive problem resolution.
Classroom Aids:	
Training Kit (Trainer Guide, Presentations), Whiteboard, Markers, Notebooks, Pens, Audio-visual training materials, laptop with an Internet connection, projector or large screen	
Tools, Equipment and Other Requirements	
Feedback forms, Sticky notes, Flip charts or chart paper.	

Module 4: Data Transfer Networks

Mapped to NOS: TEL/Nxxxx, v1.0

Terminal Outcomes:

- Explain fundamental networking concepts, protocols, architectures, and components used in modern data transfer networks.
- Configure switching, routing, network segmentation, and addressing schemes to enable efficient and secure data communication across enterprise networks.
- Implement network security, load balancing, VPN connectivity, and fault-tolerance mechanisms to ensure reliable and protected data transfer.
- Use network monitoring, traffic analysis, and device management tools to analyse performance, detect issues, and troubleshoot network problems effectively.

Duration: 30:00	**Duration: 40:00**
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the structure and functions of the OSI model and the TCP/IP protocol stack. • Describe the operational principles of data-link, network, and transport layer protocols. • Identify and explain the roles and functions of various network components used in IT infrastructures. • Differentiate between common network topology types and interpret their appropriate usage scenarios. • Explain the concept of network segmentation and the use of VLANs for traffic separation. • Describe security protocols used to safeguard local and wide area networks. • Explain IPv4 and IPv6 addressing concepts. • Illustrate the fundamental concepts of routing and switching in enterprise networks. • Explain the principles of load balancing. • Identify common types of network protocol attacks and describe suitable mitigation methods. • Explain methods for actively managing network equipment. • Describe the concepts and principles of Network Function Virtualization (NFV).	• Initialise active network equipment by performing basic setup, configuration, and verification tasks. • Implement enterprise-wide connectivity by configuring and verifying internal and external gateway routing protocols, such as OSPF, BGP, and EIGRP. • Set up network load balancing and fault-tolerance mechanisms using technologies such as GLBP, HSRP, VRRP, LACP, and PAgP. • Apply basic security configurations to protect the control and data plane of network devices. • Establish secure connectivity between remote branches using VPN technologies such as IPSec, SSL VPN, Direct Access, OpenVPN, DMVPN, and GRE. • Use network discovery and traffic analysis tools (CDP, NetFlow, Syslog, SNMP, tcpdump) to monitor, analyse, and troubleshoot network performance.

• Explain controller-based and software-defined network (SDN) management approaches and their applications.	
Classroom Aids:	
Training Kit (Trainer Guide, Presentations), Whiteboard, Markers, Notebooks, Pens, Audio-visual training materials, laptop with an Internet connection, projector or large screen	
Tools, Equipment and Other Requirements	
Managed Layer 2/3 Switches, Routers, Patch Panels, serial cables, Network Interface Cards (NICs), Cisco Packet Tracer, GNS3 / EVE-NG / NetSim / FortiSim, Linux VMs (Ubuntu/CentOS/Debian), Ethernet cables (Cat5e/Cat6), Cable crimping tools, RJ45 connectors, Cable testers, Loopback plugs, Cable organisers, Wireshark, tcpdump, NetFlow analysers, SNMP tools, OpenFlow controllers, Power supply, Fire extinguisher (CO_2), Toolkits (screwdrivers, pliers, cutters), ESD mats.	

Module 5: Network and System Operations

Mapped to NOS: TEL/Nxxxx, v1.0

Terminal Outcomes:

- Install, configure, and manage core enterprise network and system services to support reliable IT infrastructure operations.
- Deploy and administer application hosting, file sharing, web services, terminal services, and email systems across different operating systems.
- Implement infrastructure monitoring, backup solutions, and workstation deployment systems to ensure system availability and continuity.
- Configure and manage storage and file system structures to support secure, scalable, and efficient data management

Duration: 30:00	**Duration: 40:00**
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the principles of operation of common application protocols. • Describe client–server interaction models and their role in application communication. • Explain modern application delivery models used in enterprise environments. • Identify and describe operating system–level functionalities that support application deployment. • Explain dependency structures between different groups of services, applications, and systems. • Discuss various options for implementing enterprise services using different operating systems.	• Install and manage enterprise directory services such as ADDS and LDAP. • Configure and maintain domain name services using Windows DNS and BIND. • Deploy and administer dynamic host configuration services (DHCP). • Set up and manage network address translation (NAT) services. • Configure network time services to synchronise system clocks across devices. • Install and manage remote network access services such as SSH and Remote Desktop Services. • Implement and administer authentication, authorisation, and accounting (AAA) services. • Set up and manage IT infrastructure monitoring systems such as Icinga2, Nagios, Cacti, and Windows Resource Monitor. • Configure and operate email exchange systems using SMTP, IMAP, and POP with or without encryption. • Deploy public key infrastructure (PKI) services using Active Directory Certificate Services and OpenSSL. • Install and manage file sharing services such

	as SMB, DFS, NFS, and FTP. • Configure and maintain web hosting services using Apache, Nginx, or IIS. • Install and manage terminal access services, including SSH, Remote Desktop Services, and Telnet. • Configure and administer backup systems such as Windows Server Backup, rsync, and script-based backup tools (Bash, Batch, PowerShell). • Deploy and manage client workstation installation systems using Windows Deployment Services and Group Policy. • Configure and manage file systems, including software RAID, mdadm, LVM/dynamic disks, and file systems such as NTFS, ReFS, and EXT4.
Classroom Aids:	
Training Kit (Trainer Guide, Presentations), Whiteboard, Markers, Notebooks, Pens, Audio-visual training materials, laptop with an Internet connection, projector or large screen	
Tools, Equipment and Other Requirements	
Physical or virtual Windows Server machines, Physical or virtual Linux servers (Ubuntu/CentOS/Debian), Directory Services-enabled system (ADDS), DNS/DHCP servers, NAT/firewall device, Email server environment (Exchange / Postfix / Dovecot), Web servers (Apache, Nginx, IIS), RDP-enabled systems, PKI server (Active Directory Certificate Services or OpenSSL), Managed Layer 2/Layer 3 switches, Routers, Patch panels, Ethernet LAN cables (Cat5e/Cat6), Console cables, Network interfaces (single/dual NICs), Monitoring software (Nagios, Icinga2, Cacti, Windows Resource Monitor), Log collection tools (Syslog server), Packet sniffers (Wireshark, tcpdump), AAA/Radius/TACACS servers (FreeRADIUS or Windows NPS), rsync, Script-based backup tools (Bash, PowerShell, Batch), Windows Deployment Services (WDS), Group Policy Management Console (GPMC), mdadm environment in Linux, LVM tools, Disk management utilities, Cable testers, Crimping devices, RJ45 connectors, Patch cords, Screwdrivers, pliers, ESD wrist straps, Fire extinguisher (CO_2 type).	

Module 6: Infrastructure Automation

Mapped to NOS: TEL/Nxxxx, v1.0

Terminal Outcomes:

- Implement infrastructure automation workflows to streamline system deployment and maintenance.
- Execute routine infrastructure tasks through automated scripts and tools, ensuring consistency, efficiency, and reliability in IT system operations.

Duration: 30:00	**Duration: 20:00**
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the concepts of continuous integration and continuous delivery/deployment (CI/CD) pipelines. • Describe the capabilities and typical use cases of various infrastructure automation tools. • Explain the importance of code version control in managing system configurations and automation scripts. • Discuss the behaviour and functioning of infrastructure automation tools in different deployment environments.	• Set up and run routine infrastructure maintenance operations using scripting and programming languages such as Bash and PowerShell. • Use modern automation tools for system deployment and configuration management through platforms such as Git. • Identify and implement infrastructure as code (IaC) using automation tools such as Ansible.
Classroom Aids:	
Training Kit (Trainer Guide, Presentations), Whiteboard, Markers, Notebooks, Pens, Audio-visual training materials, laptop with an Internet connection, projector or large screen	
Tools, Equipment and Other Requirements	
Server OS VMs (Windows Server, Linux Server: Ubuntu/CentOS/Debian), VMware Workstation / Oracle VirtualBox, Ansible (IaC tool), Git (version control), Shell scripting environments (Bash), PowerShell 5.x or 7.x, YAML editors, GitHub, GitLab, or Bitbucket accounts (cloud or local server), Jenkins / GitLab CI / GitHub Actions demo environment, Local or cloud-based runners/executors, Code editors (VS Code, Sublime Text, Notepad++), Terminal emulators (PuTTY, MobaXterm, GNOME Terminal), JSON/YAML linters, Routers/switches, Shared storage or NAS.	

Module 7: Troubleshooting

Mapped to NOS: TEL/Nxxxx, v1.0

Terminal Outcomes:

- Diagnose hardware, software, and operating system issues using appropriate tools, logs, and manufacturer guidelines to identify the root cause of problems.
- Install, configure, and upgrade operating systems, drivers, and system roles/features according to user requirements, technical specifications, and standard procedures.
- Apply systematic troubleshooting processes to resolve system and network issues, verify solutions, document outcomes, and obtain user acceptance.

Duration: 20:00	**Duration: 20:00**
Theory – Key Learning Outcomes	**Practical – Key Learning Outcomes**
• Explain the range of operating systems and their suitability for different user requirements and budgets. • Describe the process for selecting appropriate drivers for various types of hardware. • Explain the basic functions of computer hardware and the standard procedures for system setup. • Discuss the importance of following installation or upgrade instructions and the potential consequences of not adhering to them. • Identify the precautions required before performing a system installation or upgrade. • Explain the purpose of documenting installation or upgrade activities for future reference and system management. • Describe methods and tools used to troubleshoot computer systems effectively.	• Listen closely to users, interpret their requirements, and identify needs accurately to ensure expectations are met. • Select appropriate operating systems, proprietary or open-source, based on user requirements and total cost of ownership. • Show how to identify accurate hardware components and corresponding software drivers according to user and manufacturer specifications. • Check manufacturer guidance consistently to determine the correct upgrade workflows. • Select the required operating system or server roles/features, such as ADDS or Windows Server Backup. • Discuss proposed technical solutions with relevant stakeholders and confirm agreement before implementation. • Prepare detailed technical documentation outlining the solution for approval and sign-off. • Configure selected roles/features following manufacturer instructions or organisational best practices. • Test implemented configurations, rectify detected issues, and re-test to confirm successful resolution. • Obtain user acceptance for completed configurations and record necessary

	documentation. • Use system logs to find and identify issues. • Use network package inspection, connectivity checking tools, etc., to troubleshoot and identify problems in a network.
Classroom Aids:	
Training Kit (Trainer Guide, Presentations), Whiteboard, Markers, Notebooks, Pens, Audio-visual training materials, laptop with an Internet connection, projector or large screen	
Tools, Equipment and Other Requirements	
RAM modules, Hard drives / SSDs, Motherboards (spare/demo units), Power supplies, Network Interface Cards (NICs), Cables (power, SATA, data cables), Peripheral devices (keyboard, mouse, USB devices), POST card testers, Power supply testers, Multimeter, Thermal paste and cleaning kit, System logs viewers (Event Viewer, journalctl), Disk management utilities, Linux logs (/var/log), Recovery tools (Windows Recovery Environment, boot repair tools), Wireshark, tcpdump, Ping, tracert, nslookup tools, Connectivity testers, LAN cable tester, Loopback plugs, Screwdriver set (Phillips, flat, Torx), Anti-static wrist straps, Anti-static mats, Cleaning brushes, Cable ties, cable organisers.	

Module 8: On-the-Job Training

Mapped to QP: TEL/Qxxxx, v1.0

Mandatory Duration: 120:00	Recommended Duration: 00:00
Location: On-Site	

Terminal Outcomes

- Apply organisational health & safety practices and use PPE/ESD protection while working with IT hardware and network devices.
- Configure switches and routers with basic initialisation, IP addressing, VLANs, and routing parameters.
- Implement enterprise routing protocols (OSPF, BGP, EIGRP) to enable network connectivity across multiple branches.
- Set up load-balancing and redundancy mechanisms such as HSRP, VRRP, LACP, or PAgP.
- Establish secure VPN connectivity using IPSec, SSL VPN, DMVPN, or GRE tunnels.
- Use network diagnostic tools (CDP, NetFlow, Syslog, SNMP, tcpdump, Wireshark) to analyse traffic and identify issues.
- Install and configure Directory Services (ADDS/LDAP), DNS, DHCP, NAT, and NTP services on enterprise servers.
- Deploy user access services, including SSH, RDP, remote access VPN, and terminal access tools.
- Configure email systems using SMTP, POP, and IMAP with or without encryption.
- Set up file-sharing services such as SMB, NFS, DFS, and FTP in an enterprise environment.
- Configure web hosting services using Apache, Nginx, or IIS.
- Monitor IT systems using infrastructure monitoring tools (Nagios, Icinga2, Cacti, Windows Resource Monitor).
- Implement backup strategies using Windows Server Backup, rsync, and script-based automation.
- Deploy client systems using WDS, imaging tools, and Group Policy settings.
- Manage storage and file systems, including RAID setups, LVM, dynamic disks, and NTFS/EXT4 configurations.
- Use Git for version control of configuration files, scripts, and automation assets.
- Implement Infrastructure as Code (IaC) workflows using Ansible to deploy and manage multi-node configurations.

Annexure

Trainer Requirements

Trainer Prerequisites						
Minimum Educational Qualification	**Specialisation**	**Relevant Industry Experience**		**Training Experience**		**Remarks**
		Years	**Specialisation**	**Years**	**Specialisation**	
Diploma	Computer Science, IT, or related disciplines	3	Network/System Administration, IT Infrastructure, IT Support	2	IT Networking, Systems Administration and troubleshooting	Industry certifications such as CCNA/CCNP, MCSA/MCSE, Linux+, RHCSA, CompTIA Network+ preferred.
B.Sc. / BCA	Information Technology, Computer Science, Computer Applications	2		1		
B.Tech.	Computer Science, IT, or related disciplines	1		1		

Trainer Certification	
Domain Certification	**Platform Certification**
"IT Network System Administration, TEL/Qxxxx, version 1.0". Minimum accepted score is 80%.	"Trainer, MEP/Q2601". Minimum accepted score is 80%.

Assessor Requirements

Assessor Prerequisites						
Minimum Educational Qualification	**Specialisation**	**Relevant Industry Experience**		**Assessment Experience**		**Remarks**
		Years	**Specialisation**	**Years**	**Specialisation**	
Diploma	Computer Science, IT, or related disciplines	4	Network/System Administration, IT Infrastructure, IT Support	3	IT Networking, Systems Administration and troubleshooting	Industry certifications such as CCNA/CCNP, MCSA/MCSE, Linux+, RHCSA, CompTIA Network+ preferred.
B.Sc. / BCA	Information Technology, Computer Science, Computer Applications	3		2		
B.Tech.	Computer Science, IT, or related disciplines	2		2		

Assessor Certification	
Domain Certification	**Platform Certification**
"IT Network System Administration, TEL/Qxxxx, version1.0". Minimum accepted score is 80%.	"Assessor, MEP/Q2701" Minimum accepted score is 80%.

Assessment Strategy

1. Assessment System Overview:

- Batches assigned to the assessment agencies for conducting the assessment on SDSM/SIP or email.
- Assessment agencies send the assessment confirmation to VTP/TC looping SSC.
- The assessment agency deploys the ToA certified Assessor for executing the assessment.
- SSC monitors the assessment process & records.

2. Testing Environment:

- Confirm that the centre is available at the same address as mentioned on SDMS or SIP.
- Check the duration of the training.
- Check the Assessment Start and End time to be as 10 a.m. and 5 p.m.
- If the batch size is more than 30, then there should be 2 Assessors.
- Check that the allotted time to the candidates to complete Theory & Practical Assessment is correct.
- Check the mode of assessment—Online (TAB/Computer) or Offline (OMR/PP).
- Confirm the number of TABs on the ground are correct to execute the Assessment smoothly.
- Check the availability of the Lab Equipment for the particular Job Role.

3. Assessment Quality Assurance levels / Framework:

- Question papers created by the Subject Matter Experts (SME).
- Question papers created by the SME verified by the other subject Matter Experts.
- Questions are mapped with NOS and PC.
- Question papers are prepared considering that level 1 to 3 are for the unskilled & semi- skilled individuals, and level 4 and above are for the skilled, supervisor & higher management.
- An assessor must be ToA certified & the trainer must be ToT Certified.
- The assessment agency must follow the assessment guidelines to conduct the assessment.

4. Types of evidence or evidence-gathering protocol:

- Time-stamped & geotagged reporting of the assessor from assessment location.
- Center photographs with signboards and scheme-specific branding.
- Biometric or manual attendance sheet (stamped by TP) of the trainees during the training period.
- Time-stamped & geotagged assessment (Theory + Viva + Practical) photographs & videos.

5. Method of verification or validation:

- A surprise visit to the assessment location.
- A random audit of the batch.
- Random audit of any candidate.

6. Method for assessment documentation, archiving, and access:

- Hard copies of the documents are stored.
- Soft copies of the documents & photographs of the assessment are uploaded / accessed from Cloud

Storage.

- Soft copies of the documents & photographs of the assessment are stored in the Hard Drives.

References

Glossary

Term	Description
Declarative Knowledge	Declarative knowledge refers to facts, concepts and principles that need to be known and/or understood in order to accomplish a task or to solve a problem.
Key Learning Outcome	A key learning outcome is a statement of what a learner needs to know, understand and be able to do in order to achieve the terminal outcomes. A set of key learning outcomes will make up the training outcomes. Training outcome is specified in terms of knowledge, understanding (theory) and skills (practical application).
OJT (M)	On-the-job training (Mandatory); trainees are mandated to complete specified hours of training on-site
OJT (R)	On-the-job training (Recommended); trainees are recommended the specified hours of training on-site
Procedural Knowledge	Procedural knowledge addresses how to do something, or how to perform a task. It is the ability to work or produce a tangible work output by applying cognitive, affective or psychomotor skills.
Training Outcome	Training outcome is a statement of what a learner will know, understand and be able to do upon the completion of the training.
Terminal Outcome	The terminal outcome is a statement of what a learner will know, understand and be able to do upon the completion of a module. A set of terminal outcomes help to achieve the training outcome.

Acronyms and Abbreviations

Term	Description
NOS	National Occupational Standard (s)
NSQF	National Skills Qualifications Framework
OJT	On-the-job Training
QP	Qualifications Pack
PwD	People with Disability
PPE	Personal Protective Equipment