

UNIT 1

Introduction

(4 Hours) — Network Administration (CACS406)

⚠ Please Note

These notes were prepared with the help of AI from the TU BCA syllabus and general knowledge. They may contain errors, omissions or outdated details. Please verify important points against your textbook, class notes and the latest TU syllabus before relying on them in an exam.

1.1 Network Administrator as a Profession

A **network administrator** is the person responsible for planning, installing, configuring, securing, monitoring and maintaining an organization's computer network so that users and services can rely on it every day. The network may include LANs, WANs, wireless networks, servers, switches, routers, firewalls and the services that run on them (DNS, DHCP, e-mail, web, file and print).

Roles and Responsibilities

- **Design and installation:** planning network layout, choosing hardware and software, cabling, and rolling out new sites or services.
- **Configuration and maintenance:** setting up routers, switches, servers, user accounts, IP addressing and applying patches and upgrades.
- **Monitoring and troubleshooting:** watching performance and availability, finding the root cause of faults and restoring service quickly.
- **Security:** managing firewalls, access control, antivirus, updates and responding to incidents.
- **Backup and disaster recovery:** taking regular backups, testing restores and maintaining a recovery plan.
- **User support:** helping users (help desk), creating and removing accounts, training users.
- **Documentation:** keeping network diagrams, IP plans, configuration records and procedures up to date.
- **Planning and budgeting:** capacity planning, purchase recommendations and vendor coordination.

Skills Required

Type of Skill	Examples
Technical	TCP/IP, routing and switching, Windows/Linux server administration, virtualization, scripting, security, cloud basics
Analytical	Troubleshooting methodology, log analysis, capacity planning
Soft skills	Communication, patience with users, teamwork, time management, documentation writing
Business	Understanding organization goals, cost–benefit analysis, vendor and contract handling

Types of Administrators and Career Path

Depending on the size of the organization, the work may be shared among specialists: **system administrator** (servers and OS), **network engineer** (routing/switching), **security administrator**, **database administrator**, **cloud administrator** and **help-desk/support technician**. A typical career path is: Help-desk technician → Junior network administrator → Network administrator → Senior administrator / Network engineer → Network architect or IT manager.

Certifications

Industry certifications help prove skills. Common examples are CompTIA Network+ and Security+, Cisco CCNA/CCNP, Microsoft Windows Server certifications, Red Hat RHCSA/RHCE, Linux Professional Institute (LPIC) and cloud certifications from AWS, Azure or Google.

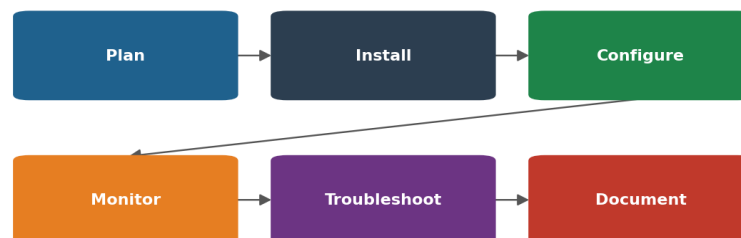


Figure 1.1 — Typical work cycle of a network administrator

Example 1.1 — A day in the life

Morning: check monitoring dashboard and overnight backup reports. A user cannot access the shared drive.

Midday: create accounts for three new staff, apply a security patch on the file server during a maintenance window.

Evening: update the network diagram after adding a new switch and document the change.

What this shows

The job mixes routine maintenance (backups, accounts), reactive work (troubleshooting) and proactive work (patching, documentation).

1.2 Network Administrator Professional Ethics

Administrators have privileged access to systems and data such as e-mail, files and passwords. This trust must be matched with strong professional ethics. Guidelines are given by bodies such as the **SAGE/LOPSA Code of Ethics** (system administrators) and the **ACM / IEEE Code of Ethics**.

Core Ethical Principles

- **Integrity and honesty:** be truthful about mistakes, outages and capabilities; do not hide problems.
- **Privacy and confidentiality:** do not read users' private files or e-mail unless required by authorized duty; protect sensitive data.
- **Professionalism:** perform work competently, keep skills current, follow procedures and change-management rules.
- **Responsible use of power:** use admin privileges only for legitimate work; never abuse access for curiosity, profit or revenge.
- **Legal compliance:** obey laws, licences and policies (for Nepal, the Electronic Transactions Act, 2063 and related cyber rules).
- **Respect for users and colleagues:** treat everyone fairly, without discrimination; support and share knowledge.
- **Security responsibility:** report vulnerabilities and breaches promptly and act to protect the organization and the public.
- **Fairness with resources:** apply quotas, policies and access rules equally.

Common Ethical Dilemmas

Situation	Ethical action
Manager asks to read an employee's e-mail	Do it only with written authorization and a legitimate reason under company policy; keep it confidential
You find illegal or inappropriate content on a server	Do not copy or spread it; report through the proper channel (management/legal)
You make a mistake that causes data loss	Admit it, restore from backup, record the cause and prevent recurrence
A friend asks for free access to the company network	Refuse; follow access policy
Pirated software is requested on office machines	Refuse; recommend licensed or open-source alternatives

Policies that Support Ethics

- **Acceptable Use Policy (AUP)** — what users may and may not do on the network.
- **Privacy / monitoring policy** — informs users what is logged and who may see it.
- **Access-control and least-privilege rules** — give only the access required for the job.
- **Incident response and disclosure procedure** — how security events are reported and handled.

Note: In exams, mention at least: confidentiality, integrity, legal compliance, responsible use of privilege, and continuous learning.

1.3 Recent Trends in Network Administration

Major Trends

Trend	Meaning	Effect on administration
Cloud computing	Renting servers, storage and services (IaaS, PaaS, SaaS) from providers such as AWS, Azure, Google Cloud	Less physical hardware; need cloud, cost and security skills
Virtualization and containers	Many virtual machines or containers on one host (VMware, KVM, Hyper-V, Docker, Kubernetes)	Faster deployment, better hardware use, new orchestration tools
Software-Defined Networking (SDN)	Separates control plane from data plane; network managed centrally by software	Central policy, automation, programmable networks

Trend	Meaning	Effect on administration
Network automation / DevOps / IaC	Using scripts and tools (Ansible, Python, Terraform) to configure devices	Fewer manual errors, consistent configuration
Network security trends	Zero-trust, next-gen firewalls, MFA, SIEM, endpoint protection	Continuous verification, faster threat detection
IPv6 adoption	128-bit addressing to replace exhausted IPv4	Dual-stack networks, new addressing plans
Wireless: Wi-Fi 6/6E/7 and 5G	Faster, denser wireless access and cellular networks	More wireless management, mobility support
Internet of Things (IoT)	Many small connected devices (sensors, cameras)	Larger network, segmentation and security challenges
Remote work and BYOD	Staff working from home or with personal devices; VPN and VDI	Remote access security, device management (MDM)
AI and AIOps	Machine learning for monitoring, anomaly detection and prediction	Proactive fault prediction and automated response
Edge computing	Processing data near where it is produced	Distributed small sites to manage
SD-WAN	Software-managed WAN using multiple links (MPLS, broadband, LTE)	Cheaper, flexible branch connectivity
Observability and monitoring	Metrics, logs and traces collected centrally (Prometheus, Grafana, ELK)	Faster root-cause analysis

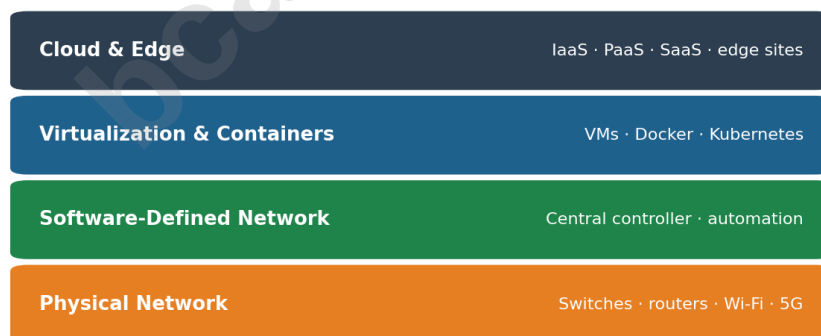


Figure 1.2 — How modern trends stack on top of the physical network

Example 1.2 — Traditional vs. modern administration

Traditional: an administrator logs in to each of 50 switches and types the same VLAN commands one by one.

Modern: the administrator writes one Ansible playbook (or uses an SDN controller) and pushes the change to all 50 switches in minutes.

Benefit

Automation is faster, repeatable, less error-prone and leaves an auditable record of changes.

Key Takeaways — Unit I

- ✓ A network administrator plans, installs, configures, secures, monitors and documents the network.
- ✓ Skills needed: technical, analytical, communication and business awareness; certifications like CCNA, Network+, RHCSA help.
- ✓ Ethics: confidentiality, integrity, legal compliance, responsible use of privileges, honesty and continuous learning.
- ✓ Policies (AUP, privacy, least privilege, incident response) support ethical practice.
- ✓ Recent trends: cloud, virtualization/containers, SDN, automation/IaC, zero-trust security, IPv6, Wi-Fi 6/5G, IoT, remote work, AIOps.

— *End of Unit I* —