

UNIT 3

Infrastructure

(16 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 They may contain errors, omissions or outdated details.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.

3.1 Network Architecture

Network architecture is the overall design of a network: its physical layout, logical structure, devices, addressing, protocols and security. A good architecture is **simple, scalable, reliable, secure and easy to manage**. Poor architecture leads to slow performance, frequent outages and expensive redesign.

3.1.1 Goals of a Good Network Design

- **Clean, simple topology:** easy to understand, document and troubleshoot.
- **Redundancy:** no single point of failure for critical links and devices.
- **Scalability:** new users, floors or sites can be added without redesign.
- **Performance:** enough bandwidth, low latency, controlled broadcast traffic.
- **Security:** segmentation, access control, firewalls, monitoring.
- **Manageability:** consistent naming, addressing and configuration; remote management.
- **Cost-effectiveness:** meet requirements without over-spending.

3.1.2 Physical Topologies

Topology	Description	Advantage	Disadvantage
Bus	All devices share one cable	Cheap, simple	Single cable failure stops all; poor performance
Star	Every device connects to a central switch	Easy to manage; one failure affects one node	Central switch is a single point of failure
Ring	Each device connects to two neighbours in a loop	Orderly access	A break can stop the ring (unless dual ring)

Topology	Description	Advantage	Disadvantage
Mesh (full/partial)	Devices connected to many others	Very reliable, redundant paths	Costly, complex cabling
Tree / hierarchical	Star networks arranged in levels	Scalable, structured	Upper levels are critical
Hybrid	Combination of the above	Flexible	More complex to design

Note: Modern LANs are almost always physical star or hierarchical star (tree) built with switches, with partial mesh at core and distribution for redundancy.

3.1.3 Hierarchical (Three-Tier) Model

The most widely used design model divides the enterprise network into three layers, each with a clear job:

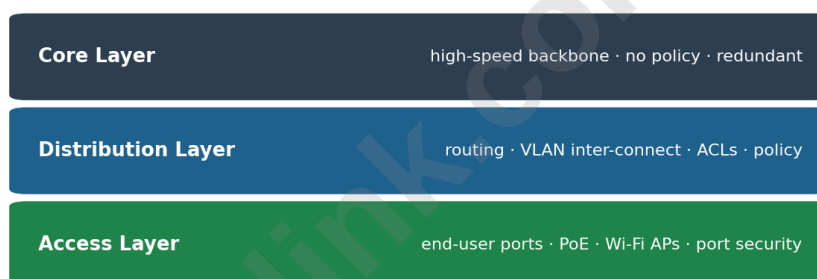


Figure 3.1 — Three-tier hierarchical network model

Layer	Function	Typical devices
Core	Fast, reliable transport between distribution blocks and to data center/WAN. Avoid slow services like heavy filtering.	High-speed Layer 3 switches, core routers
Distribution	Aggregates access switches; inter-VLAN routing; access lists, QoS, route summarization; policy boundary.	Layer 3 switches, routers, firewalls
Access	Connects end devices (PCs, printers, phones, APs); VLAN assignment; port security, PoE.	Layer 2 access switches, wireless APs

In **small networks** the core and distribution layers are combined into a **collapsed-core (two-tier)** design. In modern data centers a **spine-leaf** architecture is used instead: every leaf switch connects to every spine switch, giving predictable, low-latency east-west traffic.

Example 3.1 — Choosing a model

A college has three buildings, each with about 200 computers, and one server room. Which design is suitable?

Solution

A collapsed-core design: access switches in each floor/building connect to a pair of Layer 3 core/distribution switches in the server room (redundant links). VLANs separate students, staff, labs and servers; a firewall connects the college to the ISP.

3.1.4 Logical Design: Addressing, VLANs and Routing

- **IP address plan:** allocate subnets by department/function/location, keep room for growth, use summarizable blocks. Private ranges: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 with NAT for the Internet. Plan IPv6 too.
- **VLANs (Virtual LANs):** split one physical switch network into separate logical broadcast domains (e.g., Staff, Students, Servers, Guest, Management). Benefits: security, smaller broadcast domains, flexible grouping. Traffic between VLANs passes through a router/L3 switch.
- **Trunks (802.1Q):** carry multiple VLANs between switches over one link.
- **Routing:** static routes for small stable networks; dynamic protocols (OSPF, EIGRP, BGP for ISPs) for larger ones.
- **Spanning Tree Protocol (STP/RSTP):** prevents Layer 2 loops when redundant links exist.
- **Link aggregation (LACP/EtherChannel):** bundles several links for bandwidth and redundancy.
- **First-hop redundancy (HSRP/VRRP):** a virtual gateway address that survives router failure.
- **Core services:** DHCP (automatic addressing), DNS (names), NTP (time), directory/authentication (RADIUS/AD).

Example 3.2 — Simple subnet plan

Organization block 192.168.10.0/24 must be split into 4 equal subnets for Admin, Lab, Wi-Fi, and Servers.

Solution

Borrow 2 bits: new mask /26 (255.255.255.192), 64 addresses per subnet, 62 usable hosts.

Admin 192.168.10.0/26 (hosts .1–.62), Lab 192.168.10.64/26 (.65–.126), Wi-Fi

192.168.10.128/26 (.129–.190), Servers 192.168.10.192/26 (.193–.254).

3.1.5 Network Security Architecture

- **Perimeter firewall** between the internal network and the Internet; next-generation firewalls add application awareness and intrusion prevention.
- **DMZ (Demilitarized Zone):** a separate network segment for public servers (web, mail relay) so a compromised server cannot reach the internal LAN directly.
- **Segmentation:** VLANs and ACLs/firewall rules between user, server, guest and management networks; zero-trust thinking (verify every request).
- **Remote access:** VPN (IPsec/SSL) with strong authentication (MFA).
- **Wireless security:** WPA2/WPA3, 802.1X authentication, separate guest SSID.
- **Network Access Control (NAC) and port security:** allow only authorized devices.
- **IDS/IPS and logging:** detect and log attacks; central SIEM.
- **Out-of-band management network:** separate network for device administration.

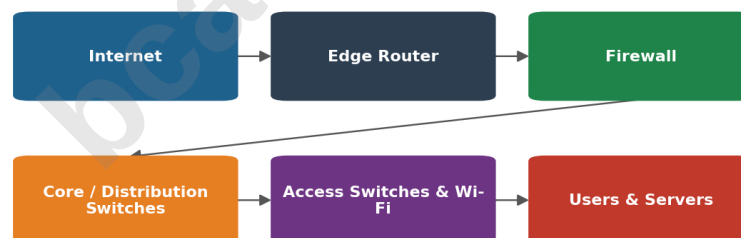


Figure 3.2 — Simplified enterprise network path (DMZ attaches to the firewall)

3.1.6 WAN, Internet Connectivity and Redundancy

- **Connection choices:** leased line, fibre Internet, MPLS/VPN service, broadband, wireless/microwave, LTE/5G, satellite (remote sites).
- **Redundancy:** two ISPs (multihoming) with automatic failover; different physical routes into the building.
- **Branch connectivity:** site-to-site VPN or SD-WAN over the Internet, replacing costly private circuits.

- **Bandwidth management:** QoS to prioritize voice/critical traffic; traffic shaping and caching.

3.1.7 Structured Cabling and Physical Layer

- **Standards:** TIA/EIA-568 (structured cabling), ISO/IEC 11801.
- **Subsystems:** work-area cabling, horizontal cabling (max 90 m permanent link + patch cords = 100 m channel for twisted pair), telecom room/IDF, backbone (vertical) cabling, main distribution frame (MDF), entrance facility.
- **Media:** UTP Cat5e/Cat6/Cat6A for horizontal runs; multimode or single-mode fibre for backbone and long distances.
- **Good practice:** label every cable and port, use patch panels and cable managers, test and certify links, keep spare capacity, separate power and data cables.

Medium	Typical speed / distance	Use
Cat5e UTP	1 Gbps up to 100 m	Basic desktop connections
Cat6 / Cat6A UTP	1–10 Gbps (10 Gbps: Cat6 ≈ 55 m, Cat6A 100 m)	Modern desktops, Wi-Fi AP uplinks
Multimode fibre	10 Gbps up to a few hundred metres	Building backbone, data center
Single-mode fibre	10 Gbps and higher, many kilometres	Campus links, ISP, long distance

3.2 Network Operations

Network operations is the day-to-day work of keeping the network running well after it is built: monitoring, managing changes, fixing faults, securing, documenting and improving. The commonly used framework is **FCAPS** from ISO.

3.2.1 FCAPS Network Management Model

Area	Meaning	Examples
F – Fault management	Detect, isolate and correct faults	Alarms, ticketing, troubleshooting
C – Configuration management	Track and control device configuration	Config backup, version control, change approval
A – Accounting / Administration	Track usage and users	Usage reports, quotas, billing/charge-back, user accounts

Area	Meaning	Examples
P – Performance management	Measure and improve network performance	Bandwidth, latency, utilization, capacity trends
S – Security management	Protect network resources	Access control, log review, patching, audits

3.2.2 Monitoring and Management Tools

- **SNMP (Simple Network Management Protocol):** a manager polls agents on devices (using MIBs and OIDs) and receives traps. SNMPv3 adds authentication and encryption — use it instead of v1/v2c.
- **Syslog:** devices send log messages to a central log server for analysis and retention.
- **NetFlow / sFlow / IPFIX:** traffic flow statistics to see who is using the bandwidth.
- **Ping, traceroute, packet capture (Wireshark, tcpdump):** basic diagnostic tools.
- **Monitoring platforms:** Nagios, Zabbix, PRTG, Icinga, Prometheus + Grafana, SolarWinds.
- **Thresholds and alerts:** alert on real problems (link down, high CPU, disk 90% full) and avoid too many false alarms.
- **Dashboards and reports:** visual overview for staff and management.



Figure 3.3 — Monitoring loop

3.2.3 Troubleshooting Methodology

Good administrators follow a structured method rather than guessing:

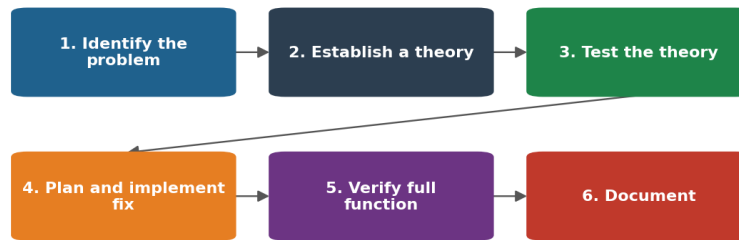


Figure 3.4 — Troubleshooting steps (CompTIA style)

- **Approaches:** top-down (start at application layer), bottom-up (start at physical layer), divide-and-conquer (start at middle layer such as IP ping).
- **Ask:** What changed? Who is affected? Since when? Can it be reproduced?
- **Use OSI layers:** Layer 1 cable/port lights, Layer 2 VLAN/MAC/STP, Layer 3 IP/route/gateway, Layer 4 firewall/ports, Layer 7 application/DNS.

Example 3.3 — A user cannot open websites

A user's PC shows 'connected' but no website opens, though others are fine.

Solution (divide and conquer)

1) Check link light and IP address (ipconfig / ip a). 2) Ping the default gateway. 3) Ping an outside IP such as 8.8.8.8. 4) If IP works but names fail, the DNS setting is wrong: check DNS server address or DHCP scope. 5) Fix, test the browser, record the cause.

3.2.4 Change, Configuration and Documentation Management

- **Change management:** request → review/risk assessment → approval → schedule in a maintenance window → implement → verify → close. Always include a rollback plan.
- **Configuration backup and version control:** automatically back up router/switch configs (RANCID, Oxidized, Git) so a failed device can be replaced quickly.
- **Documentation:** network diagrams (physical and logical), IP address and VLAN tables, cable/port maps, device inventory, procedures, contact lists.
- **Asset management:** serial numbers, warranty, firmware versions, owners.
- **Patch and firmware management:** test then deploy security updates on schedule.
- **Standard naming conventions:** for example, *bkt-core-sw01* (site-role-type-number).

3.2.5 Capacity Planning, Performance and QoS

- Measure link utilization over time; plan an upgrade when sustained use exceeds about 70–80%.
- Find bottlenecks (WAN link, uplink oversubscription, slow server, wireless congestion).
- **QoS (Quality of Service):** classify and prioritize traffic (voice, video conferencing above bulk downloads).
- Use caching proxies, load balancers and CDNs to reduce load.

3.2.6 Operations Management Practices

- **Help desk and ticketing:** single point of contact; track requests and incidents; escalation levels (L1, L2, L3).
- **SLA and priorities:** respond first to incidents that affect many users or critical services.
- **ITIL concepts:** incident, problem (root cause) and change management, service catalogue, continual improvement.
- **On-call rota and runbooks:** known procedures for common failures.
- **Security operations:** log review, vulnerability scans, regular audits and user awareness.
- **Automation:** scripts and tools (Python, Ansible) for repetitive tasks and consistent configuration.
- **Post-incident review:** analyse causes without blame and improve.

3.3 Data Centers Overview

A **data center** is a specially designed facility that houses an organization's critical computing, storage and network equipment along with the power, cooling, security and connectivity systems needed to run them continuously. It may be a small server room, an enterprise data center, a colocation facility, or a huge cloud provider site.

3.3.1 Types of Data Centers

Type	Description
Enterprise (on-premises)	Built and operated by the organization for its own use
Colocation	Rent rack space, power, cooling and connectivity in a provider's facility; you own the equipment
Managed hosting	Provider owns and operates the servers for you

Type	Description
Cloud / hyperscale	Very large facilities offering virtualized, pay-per-use services (AWS, Azure, Google)
Edge data center	Small facility close to users or devices for low latency

3.3.2 Main Components of a Data Center

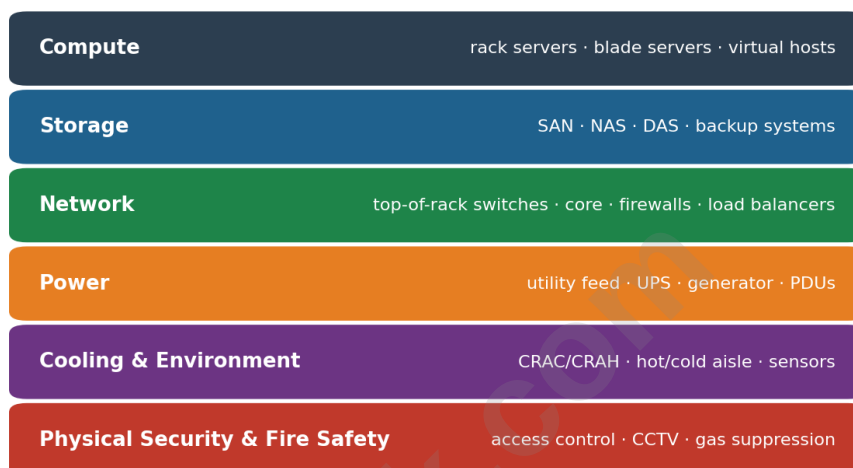


Figure 3.5 — Building blocks of a data center

3.3.3 Data Center Tiers (Uptime Institute)

Tier	Redundancy	Availability	Downtime / year
Tier I – Basic	No redundancy; single path	99.671%	≈ 28.8 hours
Tier II – Redundant components	N+1 components, single path	99.741%	≈ 22 hours
Tier III – Concurrently maintainable	N+1, multiple paths; maintenance without shutdown	99.982%	≈ 1.6 hours
Tier IV – Fault tolerant	2N or 2(N+1); survives any single fault	99.995%	≈ 26 minutes

Note: N = the capacity needed to run the load. N+1 means one spare unit; 2N means a completely duplicated system.

3.3.4 Location and Design Considerations

- Site selection: away from flood zones, fault lines, industrial hazards; stable power, multiple ISPs and fibre routes. (In Nepal, seismic safety and monsoon flooding are important factors.)
- Space planning: standard 19-inch racks (42U typical), clear aisles, raised floor or overhead cable trays, room for growth.
- Floor loading, ceiling height, fire-rated walls, and separation of equipment from office areas.
- Modular design for step-by-step expansion.

3.4 Running Data Centers

Running a data center means keeping the facility and its equipment available, safe, efficient and well organized every day.

3.4.1 Power

- **Sources:** utility power, backed by a **UPS** (battery, bridges the gap of seconds to minutes) and a **diesel generator** (long outages).
- **Redundancy:** two independent power feeds (A/B), dual power supplies in servers, redundant PDUs.
- **UPS types:** offline/standby, line-interactive, online (double-conversion) — online gives cleanest power for critical loads.
- **Monitoring:** track load per circuit; never overload; test generators and batteries regularly.
- **Efficiency – PUE (Power Usage Effectiveness) = Total facility power ÷ IT equipment power.** Ideal value is close to 1.0; 1.5–2.0 is typical for older sites.

Example 3.4 — PUE calculation

A data center draws 300 kW in total, of which the IT equipment uses 200 kW. Calculate PUE.

Solution

$PUE = 300 \div 200 = 1.5$. This means for each 1 watt used by IT equipment, another 0.5 watt goes to cooling, lighting and losses.

3.4.2 Cooling and Environment

- Servers turn nearly all electricity into heat, so cooling is essential. Recommended inlet temperature about 18–27 °C and relative humidity about 40–60% (ASHRAE guidance).
- **Hot-aisle / cold-aisle layout:** racks face each other; cold air enters the front (cold aisle), hot air leaves the back (hot aisle). Containment stops the two from mixing.
- **Cooling equipment:** CRAC (Computer Room Air Conditioner) and CRAH (Air Handler), in-row cooling, liquid cooling for dense loads, free/economizer cooling where climate allows.
- **Airflow management:** blanking panels in empty rack spaces, sealed floor openings, tidy cabling.
- **Sensors:** temperature, humidity and water-leak detection with alarms.

3.4.3 Fire Protection and Physical Security

- **Fire detection:** early smoke detection (VESDA) and heat sensors.
- **Suppression:** clean-agent gas systems (FM-200/Novec/inert gas) that do not damage equipment; water sprinklers are avoided or pre-action type; portable extinguishers (CO₂) available.
- **Access control:** ID cards, biometrics, mantraps, visitor logs, escorts, locked racks.
- **Surveillance:** CCTV, alarms, security guards; restricted zones for critical areas.
- **Safe procedures:** no food or drink, no unnecessary cardboard, equipment unpacked outside the server room.

3.4.4 Racks, Cabling and Asset Management

- Rack unit (U) = 1.75 inch (44.45 mm) height; a standard rack is 42U.
- Place heavy equipment (UPS, big servers) at the bottom; put patch panels and switches at the top (top-of-rack switching) or in end-of-row racks.
- Use labelled, colour-coded cables, cable trays and Velcro ties — not tight plastic ties.
- Keep an up-to-date **inventory (DCIM – Data Center Infrastructure Management)** of rack locations, power, ports, serial numbers and warranty dates.

3.4.5 Operational Procedures

- **Change control:** approval and scheduling for installing/removing equipment.
- **Standard operating procedures (SOPs)** and checklists for start-up, shutdown, maintenance and emergencies.
- **Monitoring 24×7:** a Network Operations Center (NOC) or on-call staff watches power, cooling, network and servers.
- **Preventive maintenance:** test UPS/generator, replace filters, check fire systems, update firmware.
- **Capacity management:** track rack space, power, cooling and network ports; plan before limits are reached.
- **Disaster recovery and backup:** offsite copies, secondary site, regular restore tests.
- **Compliance and audits:** follow standards such as ISO/IEC 27001, TIA-942, and local regulations.
- **Green IT:** improve PUE, virtualize, consolidate underused servers, use efficient equipment and recycle e-waste.

Example 3.5 — UPS runtime idea

A UPS battery bank stores 5 kWh usable energy. The connected IT load is 10 kW. Estimate runtime.

Solution

Runtime $\approx$ energy $\div$ load = 5 kWh $\div$ 10 kW = 0.5 hour = 30 minutes (in practice slightly less because of inverter losses and battery ageing). This is why a generator is needed for long outages.

Key Takeaways — Unit III

- ✓ Good network architecture is simple, redundant, scalable, secure and manageable; document it.
- ✓ Three-tier model: Core (fast transport), Distribution (policy/routing), Access (end devices); small sites use a collapsed core; data centers use spine–leaf.
- ✓ Logical design covers IP plan, VLANs/trunks, routing, STP, link aggregation, HSRP/VRRP, DHCP/DNS/NTP; security uses firewall, DMZ, VPN, segmentation.
- ✓ Structured cabling: 90 m permanent link (100 m channel) for UTP; fibre for backbone; label and certify.
- ✓ Operations follow FCAPS (Fault, Configuration, Accounting, Performance, Security) with SNMP, syslog, flow tools and a troubleshooting method.
- ✓ Change management, configuration backup, documentation, help desk and ITIL practices keep the network stable.
- ✓ Data center = compute, storage, network, power (UPS + generator), cooling, fire and physical security; Tier I–IV describe availability.
- ✓ Running a data center: redundant power, hot/cold aisles, clean-agent fire suppression, access control, DCIM, SOPs, PUE = total power ÷ IT power.

— *End of Unit 3* —