MAKERERE UNIVERSTY BUSINESS SCHOOL

FACULTY OF COMPUTING & INFORMATICS

Systems and Network Administration - Course Outline

Course Code: BUC3129

Credit Units: 4

Credit Hours: 60

Facilitators: Abdallah Ibrahim Nyero, Hajarah Ali Namuwaya, Dr. Ali Mwase, and Charles Kikwanga

Course Description

This course provides students with the skills to design, implement, secure, and maintain modern IT infrastructures in on-premises, cloud, and hybrid environments. Emphasis is placed on automation, virtualization, cloud integration, security hardening, monitoring, and troubleshooting. Learners will gain hands-on experience configuring servers, networks, virtualization platforms, and cloud services, as well as developing administration scripts and security policies that meet industry compliance standards.

Course Objectives

- Design and implement secure, scalable, and fault-tolerant networks.

- Deploy, manage, and integrate systems in on-premises, cloud, and hybrid environments.

- Implement automation and scripting for system provisioning, monitoring, and maintenance.

- Apply security best practices, compliance requirements, and disaster recovery strategies.

- Monitor and optimize IT infrastructure using modern tools and frameworks.

Learning Outcomes

- Configure and administer servers, virtualization platforms, and cloud resources.

- Implement user and access management with identity services.

- Secure systems and networks through firewalls, patching, and endpoint protection.

- Automate routine administrative tasks using PowerShell, Bash, or automation frameworks.

- Monitor performance and detect incidents using modern observability and SIEM tools.

- Plan and implement disaster recovery and business continuity strategies.

Detailed Course Content

Week	Topic	Lesson Details	Hours
1	Introduction to Modern Systems & Network Administration	Evolution of the role; cloud vs. on-prem; hybrid infrastructures; current industry demands	4
2	Core System Components	Hardware fundamentals; OS architecture; virtualization platforms; containerization basics	8
3	Networking Fundamentals & Modern Architectures	IPv4 & IPv6, VLANs, VPNs, firewalls, SDN, Zero Trust	6
4	Cloud Integration	AWS, Azure, GCP basics; deploying virtual networks; hybrid connectivity	8
5	Host & Server Management	OS installation & configuration; Active Directory/Azure AD; Linux server administration	6
6	Automation & Scripting	PowerShell, Bash, Ansible basics; Infrastructure as Code concepts	6

7	User, Access & Identity Management	RBAC, MFA, SSO; IAM in cloud platforms; security policies	6
8	Monitoring & Troubleshooting	Monitoring tools; incident response workflows	6
9	Security & Compliance	Endpoint protection, patch management; SIEM; compliance frameworks	6
10	Disaster Recovery & Business Continuity	Backup strategies, failover, redundancy, DR planning	4

Mode of Delivery

- Face-to-face and online lectures

- Hands-on labs in physical and virtualized environments

- Tutorials & guided projects

Mode of Assessment

Coursework: 40% (Labs, projects, quizzes)

Final Examination: 60% (Written & Practical)

Reading List

- Burgess, M. (2014). Principles of Network and System Administration (5th ed.). John Wiley & Sons.

Systems and Network Administration - Practical Lab Schedule

This practical lab schedule is designed to complement the Systems and Network Administration course, providing hands-on experience in configuring, managing, troubleshooting, and securing systems and networks. The labs progressively build skills from basic concepts to advanced administration tasks.

Week	Lab Topic	Objectives	Key Activities / Tools
1	Introduction to Lab Environment	Familiarize with lab infrastructure, tools, and safety procedures.	Tour of lab; Introduction to virtualization tools (VMware/VirtualBox); Lab safety guidelines.
2	Installing and Configuring Operating Systems	Install client and server OS; configure basic settings.	Install Windows Server, Ubuntu Server; Configure hostname, IP settings.
3	Active Directory Setup	Deploy and configure Active Directory Domain Services.	Install AD DS; Create OUs; Add and manage user accounts.
4	Network Configuration and IP Addressing	Configure static and dynamic IP addressing; Subnetting.	Configure DHCP; Perform subnetting; Assign static IP addresses.
5	File and Print Services	Set up shared folders and network printers.	Configure shared folder permissions; Install and share a printer.
6	User and Group Management	Manage roles, permissions, and group policies.	Create security groups; Configure GPOs for password policies.

7	System Backup and Restore	Perform backups and system recovery.	Use Windows Server Backup; Restore from backup.
8	Linux User and File Management	Create and manage Linux users and file permissions.	Use useradd, passwd, chmod, chown; Configure sudo access.
9	Network Services	Configure DNS, DHCP, and web server services.	Set up BIND DNS; Configure Apache/Nginx; DHCP scope setup.
10	Monitoring and Diagnostics	Use tools to monitor network/system performance.	Wireshark packet capture; Use netstat, ping, traceroute.
11	Security Hardening	Apply security best practices to systems and networks.	Configure firewalls (ufw/Windows Firewall); Disable unused services.
12	Troubleshooting Scenarios	Diagnose and resolve simulated system/network issues.	Identify IP conflicts; Resolve AD replication errors.
13	Capstone Lab Project	Integrate all skills to deploy a small-scale enterprise network.	Design topology; Configure AD, DNS, DHCP; Test connectivity.
14	Final Practical Assessment	Evaluate students' practical skills in system/network administration.	Perform assigned tasks under timed conditions.

Laptop Specification Sheet

The following specifications are recommended for student laptops to ensure they can successfully complete all hands-on lab activities, including the virtualization-heavy Capstone Lab Project.

Operating System: A 64-bit operating system such as Windows 10/11 Professional or a modern Linux distribution is required to run virtualization software.

1. Processor (CPU): A multi-core processor that supports hardware virtualization technology (Intel VT-x or AMD-V).

Minimum: Intel Core i5 or AMD Ryzen 5 (8th generation or newer)

Recommended: Intel Core i7 or AMD Ryzen 7 (10th generation or newer)

2. Memory (RAM): This is the most critical component for running multiple virtual machines simultaneously.

Minimum: 16 GB

Recommended: 32 GB for optimal performance, especially during the Capstone Lab Project.

3. Storage: A Solid-State Drive (SSD) is mandatory for performance, as it will significantly reduce load times for virtual machines.

Minimum: 512 GB SSD

Recommended: 1 TB SSD or larger.

4. Networking:

Wireless: Standard Wi-Fi (802.11ac or ax).

Wired: An Ethernet port is highly recommended. If the laptop does not have one, a USB-to-Ethernet adapter is required for certain labs.

5. Peripherals: Standard keyboard, mouse or trackpad, and a functional webcam are expected.

6. Virtualization Software: Students will need to install and use a desktop virtualization tool.

Recommended: VMware Workstation Player (free for personal use) or Oracle VM VirtualBox.

Capstone Project: Deploy and Secure a Hybrid Network Infrastructure for a Medium-Sized Organization

Project Overview

Students will design, implement, secure, and document a **hybrid IT infrastructure** for a fictional company, **TechLink Solutions**, which has:

- A head office with 100 staff
- A branch office with 30 staff
- Several remote employees working from home
- Business-critical applications hosted both **on-premises** and **in the cloud**

The solution must provide **secure, scalable, and reliable** access for all users, while ensuring compliance with security standards and enabling future growth.

Project Objectives

By completing this project, students will:

- Apply **network design principles** to build a logical, segmented infrastructure.
- Deploy **Active Directory** and integrate with **Azure AD**.
- Configure **secure remote access** using VPN or Zero Trust Network Access.
- Automate basic administrative tasks with **PowerShell or Bash scripts**.
- Implement **monitoring and alerting** for proactive infrastructure management.
- Develop a **backup and disaster recovery plan**.
- Demonstrate understanding of **security hardening** and **compliance requirements**.

Project Requirements

1. Network & Systems Design

- Create a network topology showing:
    - VLAN segmentation for different departments (e.g., HR, Finance, IT)
    - Branch connectivity (site-to-site VPN or dedicated link)
    - Internet and firewall placement
- Assign **IP address schemes** and justify choices.

2. Server Deployment

- Install and configure:
    - **Windows Server** with **Active Directory Domain Services** (AD DS)
    - **Azure AD** tenant and configure hybrid identity

    - File server with departmental shared folders & permissions

3. Cloud Integration

- Deploy a **cloud-based application server** (Azure or AWS)
- Configure **secure access** from the on-premises network

4. Security Implementation

- Configure **MFA** for all cloud accounts
- Apply **group policies** for password complexity, account lockout, and workstation security
- Enable **Windows Defender or endpoint protection** on all systems

5. Automation

- Write a PowerShell or Bash script to:
    - Create user accounts in bulk
    - Assign users to correct groups based on department

6. Monitoring & Maintenance

- Set up **Nagios/Zabbix** to monitor:
    - Server uptime
    - CPU & memory usage
    - Network bandwidth
- Create an **alert policy** for system failures

7. Backup & Disaster Recovery

- Configure **daily backups** for:
    - Active Directory
    - File server data
- Document recovery procedures

8. Documentation & Presentation

- Provide a **detailed report** covering:
    - Design diagrams
    - Configurations used
    - Scripts written
    - Security measures
    - Backup/DR plan

- Present the project to the class as if pitching to a company's IT director.

Project Deliverables

1. **Network topology diagram**
2. **Server and network configuration details**
3. **Automation script file**
4. **Monitoring system screenshots**
5. **Backup configuration evidence**
6. **Security policy document**
7. **Final presentation (PowerPoint or similar)**

Evaluation Criteria

Area	**Weight**
Design & Planning	15%
Implementation & Configuration	25%
Security Measures	15%
Automation	10%
Monitoring & Maintenance	10%
Documentation	15%
Presentation	10%