

COMP 012 - Network Administration

Project Development Phase

SESSION 14: PROJECT SPRINT 2 - CORE FEATURES

ACTIVITY 14.1: NETWORK SERVICES IMPLEMENTATION

Topic: Configuring core network services

Description: Implement DNS, DHCP, and other network services

INSTRUCTIONS:

Configure DNS services:

- All servers resolvable by name
- A records for all hosts
- Reverse DNS zones
- DNS forwarding for external resolution

Configure DHCP (if applicable):

- DHCP scope for client network
- Reservations for critical devices
- Scope options (gateway, DNS)

Configure file sharing:

- Windows shared folders with permissions
- Linux Samba shares (if cross-platform)
- Map drives or mount points

Configure web services:

- Deploy sample web application
- Configure virtual hosts
- Test from client machines

Create service documentation:

- Service inventory
- Configuration details
- Access instructions

Deliverables: Submit service configurations and test results

30 Points

ACTIVITY 14.2: ROUTING AND SWITCHING CONFIGURATION

Topic: Implementing network infrastructure in Packet Tracer

Description: Build the routing and switching infrastructure

INSTRUCTIONS:

Build network in Packet Tracer:

- Implement your network design
- Configure all VLANs

- Set up trunk links
- Configure router interfaces

Implement routing:

- Choose: Static or OSPF
- Configure routes between all segments
- Verify routing tables
- Test inter-VLAN routing

Configure ACLs:

- Implement security policy
- Block unauthorized traffic
- Allow required services
- Document all ACL rules

Connect Packet Tracer to concept:

- Document how PT network maps to VMs
- Explain routing between segments

Verify all connectivity

Deliverables: Submit .pkt file and routing/ACL documentation

35 Points

ACTIVITY 14.3: SECURITY IMPLEMENTATION

Topic: Implementing comprehensive security

Description: Apply security measures across your infrastructure

INSTRUCTIONS:

Server security:

- Windows Firewall rules
- Linux UFW rules
- Service hardening
- Strong password policies

Network security:

- ACLs on routers/switches
- Port security on switches
- Disable unused ports

Access control:

- Proper user permissions
- Group-based access
- Principle of least privilege

Monitoring and logging:

- Enable audit logging
- Configure event forwarding (optional)
- Set up fail2ban on Linux

Create security documentation:

- Security policy document
 - Firewall rule documentation
 - Access control matrix
- Milestone: 50% complete

Deliverables: Submit security configurations and documentation
(50% milestone)

40 Points

TOTAL POINTS: 105