Practical Exam Part 1 - Complete Study Guide

45 Minutes Total | 10 Marks

EXAM OBJECTIVE

1. **Cable through to data center and ping 100.64.0.1 from Linux VM**
2. **Set up RADIUS server for WiFi user authentication (username/password)**

TIME ALLOCATION STRATEGY

Task	Time	Cumulative
Physical cabling to data center	3 min	3 min
Configure MikroTik hEX PoE with PPPoE	8 min	11 min
Verify ping to 100.64.0.1	2 min	13 min
Configure Linksys as AP	5 min	18 min
Install & configure FreeRADIUS	12 min	30 min
Configure WAP for WPA Enterprise	8 min	38 min
Test smartphone authentication	5 min	43 min
Buffer time	2 min	45 min

PART 1: PHYSICAL SETUP & CONNECTIVITY (13 minutes)

Step 1: Identify Your Pod Assignment (1 min)

Critical Information Table:

Pod	PPPoE Username	PPPoE Password	Data Center Port	ONU Label
A	alpha	alpha	17 (or A)	alpha
B	beta	beta	18 (or B)	beta
C	charlie	charlie	19 (or C)	charlie
D	delta	delta	20 (or D)	delta
E	echo	echo	21 (or E)	echo
F	foxtrot	foxtrot	22 (or F)	foxtrot
G	golf	golf	23 (or G)	golf
H	hotel	hotel	24 (or H)	hotel

⚠️ **CRITICAL:** Your credentials and port number are determined by your pod assignment!

Step 2: Physical Cabling (2 min)

Connection Path:

> Desk → Patch Panel (at desk) → Data Center Patch Panel → Cloud Core Switch Port

Physical Steps:

1. Locate your desk patch panel port
2. Run Ethernet cable from desk to data center
3. Connect to the **numbered port matching your pod** on Cloud Core Switch
4. This connection provides **Power over Ethernet (PoE)** to your MikroTik hEX PoE
5. **Verify:** MikroTik should power on automatically

🔍 **Troubleshooting:**

- Check link lights on both ends
- Ensure cable is fully seated in both jacks
- Verify you're using the correct port number

Step 3: Configure MikroTik hEX PoE for PPPoE (8 min)

A. Initial Connection:

1. Connect your PC/Linux VM to **LAN port** (ports 2-5) on MikroTik
2. Your PC should get IP: `192.168.88.x` (DHCP)
3. Verify with: `ip addr show`

B. Reset Configuration (if needed):

- Open browser: `http://192.168.88.1`
- If you can't login or wrong settings exist:
    - **Unplug power**
    - **Hold reset button while plugging back in**
    - **Hold for 5 seconds** until USER LED flashes
    - Release button

C. Configure PPPoE:

1. Browser to: `http://192.168.88.1`
2. Login: **username:** `admin` **password:** (blank)
3. Click **QuickSet** page
4. Configure:
    - **WAN Connection Type:** `PPPoE`
    - **PPPoE Username:** (from table above - e.g., `alpha`)
    - **PPPoE Password:** (from table above - e.g., `alpha`)
    - ✅ **Enable DHCP Server** (check box)
    - ✅ **Enable NAT** (check box)
5. Click **Apply** and wait ~30 seconds

D. Verify PPPoE Connection:

1. Click **WebFig** → **Interfaces**
2. Click on **pppoe-out1** interface
3. Status should show: **connected** or **running**
4. Note your WAN IP: `100.64.0.x`

Step 4: Test Connectivity to Data Center (2 min)

From Linux VM terminal:

bash

```bash
# Verify you have IP in 192.168.88.0/24 range
ip addr show

# Check default gateway
ip route show
# Should show: default via 192.168.88.1

# Ping the MikroTik gateway
ping -c 3 192.168.88.1

# Ping your WAN interface (check WebFig for your IP)
ping -c 3 100.64.0.x

# ⭐ CRITICAL TEST - Ping data center server
ping -c 3 100.64.0.1
```

✅ **SUCCESS CRITERIA:** You must successfully ping `100.64.0.1`

🔍 **Troubleshooting:**

- If you have multiple network interfaces, disconnect from Murdoch network
- Verify PPPoE shows "connected" in WebFig
- Check NAT is enabled on MikroTik
- Verify firewall isn't blocking ICMP

PART 2: RADIUS SERVER & WiFi AUTHENTICATION (32 minutes)

Step 5: Configure Linksys as Access Point (5 min)

A. Connect to Linksys:

1. Physically connect PC to Linksys **LAN port** (not Internet port!)
2. Browser to: `http://192.168.1.1`
3. Login: **username:** `root` **password:** `admin`
4. If can't login: **Hold reset button 10+ seconds**

B. Convert to Access Point Mode:

1. **Setup → Basic Setup:**
   - **WAN Connection Type:** `Disabled`
   - **Router IP Address:** `192.168.88.2`
   - **Subnet Mask:** `255.255.255.0`

    - **Gateway:** `192.168.88.1`
    - **Local DNS:** `192.168.88.1`
    - ❌ **Disable DHCP Server** (uncheck)
2. Click **Save Settings**
3. Click **Apply**

C. Physical Reconnection:

1. **Cable LAN port of MikroTik → LAN port of Linksys** (NOT Internet port!)
2. Reconnect your Linux VM to network
3. Should get new IP: `192.168.88.x` from MikroTik DHCP

D. Verify Dual Access:

bash

```bash
# Test MikroTik access
ping 192.168.88.1

# Test Linksys access
ping 192.168.88.2

# Browse to both:
# http://192.168.88.1 (MikroTik)
# http://192.168.88.2 (Linksys)
```

E. Configure Basic Wireless Settings:

1. Access Linksys: `http://192.168.88.2`
2. **Wireless → Basic Settings:**
    - **SSID:** `YourUniqueName-Lab` (NOT dd-wrt!)
    - **Wireless Channel:** Choose 6 or 11 (avoid 1)
    - **Save**
3. **Wireless → Advanced Settings:**
    - **TX Power:** `5 mW` (reduce interference)
    - **Save & Apply**

Step 6: Install FreeRADIUS on Linux VM (5 min)

A. Install FreeRADIUS:

bash

```bash
sudo apt update
sudo apt install freeradius
```

B. Stop FreeRADIUS (before configuration):

bash

```bash
sudo service freeradius stop
```

C. Verify Installation:

bash

```bash
# Check if installed
dpkg -l | grep freeradius

# Verify config directory exists
ls -la /etc/freeradius/3.0/
```

Step 7: Configure FreeRADIUS (12 min)

A. Configure RADIUS Clients (7 min):

The RADIUS client is your **Linksys AP** at `192.168.88.2`

bash

```bash
sudo nano /etc/freeradius/3.0/clients.conf
```

Scroll to bottom of file and add:

```
# Linksys Access Point
client linksys-ap {
    ipaddr = 192.168.88.2
    secret = MySecretKey123
    shortname = linksys
    nastype = other
}
```

📝 Key Points:

- `ipaddr`: IP address of Linksys AP
- `secret`: Shared secret (you'll enter this on AP too)

- Use a memorable secret like: `MySecretKey123` or `RadiusTest2024`

Save: `Ctrl+O`, `Enter`, `Ctrl+X`

B. Configure RADIUS Users (5 min):

bash

```bash
sudo nano /etc/freeradius/3.0/users
```

Scroll down and find the commented example like:

```
#bob    Cleartext-Password := "hello"
```

Add your test users at the top of the file:

```
# Test users for WiFi authentication
testuser Cleartext-Password := "testpass"
student1 Cleartext-Password := "password123"
admin1 Cleartext-Password := "admin123"
```

📝 Format is critical:

- Username (no quotes)
- Space
- `Cleartext-Password`
- Space
- `:=`
- Space
- `"password"` (in quotes)

Save: `Ctrl+O`, `Enter`, `Ctrl+X`

C. Verify Configuration:

bash

```
# Check configuration syntax
sudo freeradius -C

# Should output: "Configuration appears to be OK"
```

If errors appear:

- Check for typos in clients.conf
- Verify user format in users file
- Ensure proper spacing and quotes

D. Start FreeRADIUS in Debug Mode:

bash

```
# Start in foreground/debug mode
sudo freeradius -X
```

If you get "Address already in use" error:

bash

```
# Find and kill existing process
ps -e | grep radius
sudo kill [PID_number]

# Try again
sudo freeradius -X
```

✅ **SUCCESS:** Should see output ending with:

```
Ready to process requests
```

⚠️ **KEEP THIS TERMINAL OPEN** - You'll see authentication attempts here

---

Step 8: Configure Linksys for WPA Enterprise (8 min)

A. Access Linksys Configuration:

- Browser: `http://192.168.88.2`
- Login: `root` / `admin`

B. Configure WPA Enterprise:

1. Click **Wireless → Wireless Security**
2. Configure:
   - **Security Mode:** `WPA2 Enterprise`
   - **WPA Algorithms:** `AES` (or `TKIP+AES`)
   - **RADIUS Server:** `[Your Linux VM IP]`
     - Find with: `ip addr show` (e.g., `192.168.88.10`)
   - **RADIUS Port:** `1812`
   - **Shared Secret:** `MySecretKey123` (MUST match clients.conf!)
3. Click **Save Settings**
4. Click **Apply Settings**

📝 Critical Points:

- RADIUS Server IP must be your Linux VM IP (not 192.168.88.1!)
- Shared Secret must EXACTLY match what you put in clients.conf
- Port is standard: 1812

Step 9: Test Authentication with Smartphone (5 min)

A. Connect Smartphone to WiFi:

1. Open WiFi settings on phone
2. Select your SSID: `YourUniqueName-Lab`
3. Should prompt for enterprise credentials

B. Enter Credentials:

- **EAP Method:** `PEAP` or `TTLS`
- **Phase 2 Authentication:** `MSCHAPv2` or `PAP`
- **CA Certificate:** `Don't validate` or `Use system certificates`
- **Identity/Username:** `testuser`
- **Anonymous Identity:** (leave blank or same as username)
- **Password:** `testpass`

C. Connect and Verify:

1. Tap **Connect**
2. Should connect successfully
3. Verify IP address (Settings → WiFi → Your network)
4. Should have `192.168.88.x` address

D. Check RADIUS Logs:

In your terminal running `sudo freeradius -X`, you should see:

```
Received Access-Request
  User-Name = "testuser"
  ...
Sending Access-Accept
```

✅ **SUCCESS CRITERIA:**

- Phone connects to WiFi
- Phone gets IP from MikroTik DHCP (192.168.88.x)
- RADIUS shows "Access-Accept" in logs
- Can browse internet from phone

WHAT THE ASSESSOR WILL CHECK

Physical Setup:

- ✅ Correct cable from desk to data center
- ✅ MikroTik powered on via PoE
- ✅ Proper cable between MikroTik LAN and Linksys LAN

Network Connectivity:

- ✅ PPPoE authenticated successfully
- ✅ `ping 100.64.0.1` works from Linux VM
- ✅ Linux VM has IP in 192.168.88.0/24 range

RADIUS Configuration:

- ✅ FreeRADIUS service running
- ✅ Clients.conf has Linksys AP configured
- ✅ Users file has test users
- ✅ Shared secrets match between AP and RADIUS

WiFi Authentication:

- ✅ Linksys configured for WPA2 Enterprise
- ✅ RADIUS server IP correctly set
- ✅ Smartphone can authenticate with username/password
- ✅ Authentication shows in RADIUS logs

COMMON MISTAKES TO AVOID

❌ **Using Internet port on Linksys** → Use LAN port! ❌ **Forgetting to disable Linksys DHCP** → Must be disabled ❌ **Mismatched RADIUS shared secrets** → Must match exactly ❌ **Wrong RADIUS server IP** → Use your Linux

VM IP, not gateway ❌ **RADIUS not running** → Keep `freeradius -X` terminal open ❌ **Typos in usernames/passwords** → Case sensitive! ❌ **Using wrong port number in data center** → Match your pod ❌ **NAT not enabled on MikroTik** → Check the checkbox ❌ **Multiple network connections active** → Unplug Murdoch network

---

QUICK REFERENCE COMMANDS

Network Troubleshooting:

bash

```bash
ip addr show
ip route show
ping 192.168.88.1      # Gateway
ping 192.168.88.2      # Linksys
ping 100.64.0.1        # Data center
```

RADIUS Management:

bash

```bash
# Stop service
sudo service freeradius stop

# Check config
sudo freeradius -C

# Run in debug mode
sudo freeradius -X

# Kill stuck process
ps -e | grep radius
sudo kill [PID]
```

Files to Edit:

bash

```
/etc/freeradius/3.0/clients.conf    # Add AP
/etc/freeradius/3.0/users           # Add users
```

Browser Access:

```
http://192.168.88.1    # MikroTik
http://192.168.88.2    # Linksys
```

PRACTICE CHECKLIST

Before the exam, practice:

- □ Identifying correct data center port
- □ Resetting MikroTik configuration
- □ Configuring PPPoE with QuickSet
- □ Verifying PPPoE connection status
- □ Converting Linksys to AP mode
- □ Editing clients.conf with proper syntax
- □ Editing users file with proper format
- □ Starting FreeRADIUS in debug mode
- □ Configuring WPA2 Enterprise on AP
- □ Connecting smartphone with PEAP/TTLS
- □ Reading RADIUS authentication logs

EXAM DAY TIPS

1. **Read pod assignment carefully** - Wrong port = wrong credentials
2. **Reset both devices first** - Start with clean config
3. **Write down your credentials** - Pod letter, username, password
4. **Keep terminals open** - See RADIUS logs in real-time
5. **Test as you go** - Don't wait until end to test connectivity
6. **Watch for typos** - Copy/paste when possible
7. **Check shared secrets match** - AP and clients.conf must be identical
8. **Stay calm** - You have practiced this!

FINAL VERIFICATION

Before calling the assessor:

bash

```
# 1. Can ping data center
ping -c 3 100.64.0.1

# 2. RADIUS is running
ps -e | grep radius

# 3. Can access both devices
ping 192.168.88.1
ping 192.168.88.2

# 4. Smartphone connected and has IP
# Check phone WiFi settings

# 5. Authentication logs show success
# Check freeradius -X terminal output
```

When all checks pass → Call assessor for grading!

TROUBLESHOOTING FLOWCHART

Can't ping 100.64.0.1: → Check PPPoE status in WebFig → Verify NAT is enabled → Check correct data center port → Unplug from Murdoch network

Can't access Linksys at 192.168.88.2: → Verify cable LAN to LAN → Check DHCP disabled on Linksys → Verify gateway set to 192.168.88.1 → Reset and reconfigure

Phone won't authenticate: → Check RADIUS server IP on AP → Verify shared secrets match → Check user exists in users file → Look at RADIUS debug output → Try different phone/device

RADIUS won't start: → Kill existing process: `sudo killall freeradius` → Check config: `sudo freeradius -C` → Fix syntax errors in config files → Restart: `sudo freeradius -X`

Good luck on your exam! 🎓