WiFi Lab Setup & Security Protocols Quick Reference

Router Access & Setup

Finding Your Router IP

```bash
# Linux/Mac
ip route | grep default

# Windows
ipconfig /all
```

Common Router IPs

```
192.168.1.1
192.168.0.1
192.168.2.1
10.0.0.1
```

Default Login Credentials

- admin / admin
- admin / password
- admin / (blank)
- admin / 1234
- Check router sticker for defaults

WiFi Security Protocols Comparison

WEP (1997) - BROKEN

- Static encryption key shared by all devices
- Initialization vector reuse vulnerability
- Can be cracked in 5-10 minutes
- Status: Obsolete, avoid completely

WPA (2003) - DEPRECATED

- TKIP generates dynamic keys
- Message integrity checks
- Still has exploitable weaknesses
- Status: Upgrade to WPA2/WPA3 immediately

WPA2 (2004) - CURRENT STANDARD

- AES encryption (much stronger)
- 4-way handshake authentication
- Personal (PSK) and Enterprise modes
- Vulnerable to offline dictionary attacks
- KRACK attack (2017) showed handshake flaws

WPA3 (2018) - MODERN STANDARD

- SAE replaces vulnerable handshake
- Forward secrecy protection
- Protection against offline dictionary attacks
- Individual device encryption
- Not all devices support yet

Guest Network Lab Configuration

Step-by-Step Setup

1. Access router admin interface
2. Navigate to WiFi/Wireless settings
3. Find "Guest Network" section
4. Enable guest network
5. Configure test parameters

Recommended Lab Settings

```
Network Name: TestLab-Guest
```

```
Security: WPA2-Personal
Password: password123 (intentionally weak)
Network Isolation: Enabled
Active Time: Unlimited
```

Multiple Test Networks (if supported)

- TestLab-Open: No security
- TestLab-WEP: WEP security (if available)
- TestLab-WPA2: WPA2 with weak password
- TestLab-Strong: WPA3 with strong password

Lab Documentation Template

```
WiFi Testing Lab Configuration
==============================
Router Model: [Your router model]
Admin IP: 192.168.1.1
Main Network: [Your main SSID]
Guest Network: TestLab-Guest
Guest Password: password123
Guest Security: WPA2-PSK
Channel: [Note the channel]
Test Device MAC: [Your device MAC]
```

Security Best Practices

Router Hardening

- Change default admin credentials
- Disable WPS (WiFi Protected Setup)
- Use WPA3 when available
- Enable network isolation for guests
- Regular firmware updates
- Strong admin passwords

Testing Safety Guidelines

- Only test your own networks
- Document all lab configurations
- Keep main network separate from test networks
- Use intentionally weak passwords for testing only
- Monitor for unauthorized access attempts

Common Router Interface Locations

Guest Network Settings Found In:

- "Wi-Fi network" (main section)
- "Wireless Settings"
- "WiFi Setup"
- "Network Settings"
- "Advanced" → "Guest Access"

Important Features to Configure:

- QR Code generation (auto-created)
- Network isolation (recommended: enabled)
- Bandwidth control (optional)
- Access scheduling (set to unlimited for testing)

Real-World Security Impact

Major WiFi Breaches:

- **Marriott (2018)**: 500M records via WiFi infrastructure
- **Equifax (2017)**: WiFi reconnaissance enabled larger breach
- **Average breach cost**: $4.5 million
- **Detection time**: Often months before discovery

Why WiFi Attacks Succeed:

- Weak passwords (password123, company2024)

- Outdated encryption (WEP still exists)
- Poor network segmentation
- Unmonitored guest networks
- IoT device vulnerabilities