



802.1X LAB

LAB MATERIALS

- HaPeplink Router with Docker Support
- Firmware 8.5.0
- Access Point (Internal or External), Switch (optional)
- Laptop/Phone/Client Device
- USB Stick
- Ethernet Cable(s)

**A limited number of lab kits will be provided for attendees to share.
Recommended for attendees to bring their own materials, but not necessary.*

802.1X LAB

STEP 1: PREPARE DOCKER

- 1.1. Insert USB stick and setup external storage if necessary
- 2.2. Go to Advanced > Docker > Install essential package
3. Go to Docker Management in InControl2 and create a script with following:
`docker run -d --name freeradius -p 1812:1812/udp -p 1813:1813/udp westnetdocker/freeradtest(-arm for Peplink w/ ARM architecture)`
4. Apply script to Peplink Router

STEP 2: RADIUS/802.1X CONFIGURATION

1. Access Web Admin and note FreeRADIUS IP address
2. [Advanced Tab > RADIUS Server]
 - a. Click New Profile
 - b. Create a name
 - c. Leave port default 1812
 - d. Secret is "testing123"
3. [Advanced Tab > 802.1X Authentication]
 - a. Enable
 - b. Confirm RADIUS server settings
 - c. Save and Apply Changes
4. [Network Tab > Port Settings]
 - a. Edit LAN port(s) to enable 802.1X
 - b. Port type = Access
 - c. Authentication Method = Port-based 802.1X
 - d. Save and Apply Changes

STEP 3: CLIENT CONFIGURATION (WINDOWS)

1. Autostart Services Wired AutoConfig/WLAN AutoConfig
2. Open View Network Connections
3. Right click ethernet adapter > Properties
4. Click Authentication Tab > Choose PEAP > Settings > Uncheck "Verify the server's identity.." > Choose MSCHAP v2 > OK
5. Click Additional settings > Specify user authentication > replace credentials > User name = testuser > Password = testpass

STEP 4: TEST PORT-BASED 802.1X

1. Connect client to port configured for 802.1X
2. Confirm network access is granted
3. Connect unauthorized client
4. Confirm network access is denied

STEP 5: CONFIGURE WI-FI AUTHENTICATION

1. Create SSID in Web Admin AP Tab or InControl Wi-Fi AP Tab
2. Security Policy = WPA2 - Enterprise
3. 802.1X Version = V2
4. Select RADIUS server profile from dropdown
5. Save/Apply

STEP 6: TEST WI-FI AUTHENTICATION

1. Connect client to Wi-Fi
2. User name = testuser > Password = testpass
3. Confirm network access is granted
4. Test invalid password = denied access

802.1X LAB

BEST PRACTICES & TIPS

- Set static IP or DHCP reservation for RADIUS server
- Create secondary RADIUS server for backup
- Use strong RADIUS shared secrets (not "testing123" in production).
- Test with multiple client OS types (Windows, macOS, Android, iOS).
- Create guest VLAN network for unauthenticated traffic.
- Use additional flags for Docker run command
 - Run container with static IP: `--ip 192.168.1.9`
 - Run container on VLAN: `--network vlan100`
 - Run container to auto-restart: `--restart unless-stopped`
- Configure RADIUS server for EAP-TLS certificate based authentication for gold standard of security
- Utilize external RADIUS server or Peplink KVM for production

TROUBLESHOOTING

- Client cannot authenticate: Check RADIUS IP, shared secret, client configuration, Docker container logs
- Unauthorized clients granted access: Check 802.1X port settings, ensure correct Wi-Fi SSID configuration.
- RADIUS container not starting: Remove all Docker containers, reboot Peplink, and start over
- 802.1X port settings unavailable: Ensure firmware is 8.5.0 or above, RADIUS and 802.1X are configured in Advanced Tab of Web Admin.