Ubuntu WiFi 핫스팟
완전 설정 가이드

새로운 컴퓨터에 설치하기 위한 단계별 가이드

네트워크 구성 예시

유선 인터페이스: enp109s0 (인터넷 연결)

무선 인터페이스: wlp0s20f3 (핫스팟)

핫스팟 IP 대역: 10.0.0.0/24

목차

1. 필수 패키지 설치

WiFi 핫스팟을 구축하기 위해 두 가지 필수 패키지가 필요합니다. hostapd는 WiFi 액세스 포인트 역할을 수행하며, dnsmasq는 DHCP 서버와 DNS 포워더 역할을 담당합니다. iptables-persistent는 방화벽 규칙을 영구 저장하기 위해 필요합니다.

설치 명령어:

```
sudo apt update
sudo apt install hostapd dnsmasq iptables-persistent -y
```

설치 후 서비스 중지 (설정 완료 전까지):

```
sudo systemctl stop hostapd
sudo systemctl stop dnsmasq
```

2. hostapd 설정 (WiFi AP)

hostapd는 무선 인터페이스를 액세스 포인트로 동작시키는 데몬입니다. SSID, 비밀번호, 채널, 보안 모드 등을 설정합니다. 보안을 위해 TKIP 대신 CCMP(AES)를 사용하는 것이 권장됩니다.

설정 파일 생성:

```
sudo nano /etc/hostapd/hostapd.conf
```

파일 내용:

```
interface=wlp0s20f3
driver=nl80211
ssid=YourSSID
hw_mode=g
channel=6
wmm_enabled=0
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
rsn_pairwise=CCMP
wpa_passphrase=YourPassword
```

주요 설정 항목 설명:

- interface: 무선 인터페이스 이름 (iwconfig로 확인)
- ssid: WiFi 네트워크 이름
- hw_mode=g: 2.4GHz 대역 (a: 5GHz)

- channel: 사용할 채널 (자동 선택은 hw_mode=g와 channel=0)
- wpa=2: WPA2 보안
- wpa_pairwise=CCMP: AES 암호화 (TKIP는 취약하므로 사용 지양)
- wpa_passphrase: WiFi 비밀번호 (8자 이상)

3. dnsmasq 설정 (DHCP/DNS)

dnsmasq는 가벼운 DHCP 및 DNS 서버입니다. 핫스팟에 연결된 클라이언트에게 IP 주소를 할당하고 DNS 쿼리를 처리합니다. 게이트웨이와 DNS 서버 주소를 클라이언트에 전달하는 것이 중요합니다.

설정 파일 편집:

```
sudo nano /etc/dnsmasq.conf
```

파일 내용 (기존 내용은 주석 처리 후 추가):

```
interface=wlp0s20f3
dhcp-range=10.0.0.50,10.0.0.150,12h
dhcp-option=3,10.0.0.1
dhcp-option=6,10.0.0.1,8.8.8.8
bind-interfaces
server=8.8.8.8
```

설정 항목 설명:

- interface: DHCP를 제공할 인터페이스
- dhcp-range: 할당할 IP 범위와 임대 시간
- dhcp-option=3: 게이트웨이 주소 (클라이언트가 인터넷으로 나가는 경로)
- dhcp-option=6: DNS 서버 주소
- bind-interfaces: 지정된 인터페이스에만 바인딩
- server: 업스트림 DNS 서버

4. 네트워크 인터페이스 정적 IP 설정

무선 인터페이스에 고정 IP 주소를 할당해야 합니다. Ubuntu는 Netplan 또는 /etc/network/interfaces를 사용합니다. 이미 Netplan을 사용 중이면 interfaces 파일을, 그렇지 않으면 Netplan을 사용하는 것이 좋습니다.

방법 A: /etc/network/interfaces 사용

```
sudo nano /etc/network/interfaces
```

추가할 내용:

```
auto wlp0s20f3
iface wlp0s20f3 inet static
```

```
address 10.0.0.1
netmask 255.255.255.0
```

방법 B: Netplan 사용 (기존 Netplan이 있는 경우)

```
sudo nano /etc/netplan/01-network-manager-all.yaml
```

기존 내용에 추가:

```
wlp0s20f3:
 dhcp4: no
 addresses: [10.0.0.1/24]
```

```
sudo netplan apply
```

NetworkManager 충돌 방지:

NetworkManager가 무선 인터페이스를 관리하지 않도록 설정합니다:

```
sudo nano /etc/NetworkManager/NetworkManager.conf
```

```
[keyfile]
unmanaged-devices=interface-name:wlp0s20f3
```

5. IP 포워딩 활성화

핫스팟 클라이언트가 인터넷에 접속하려면 IP 포워딩이 활성화되어야 합니다. 이를 통해 무선 인터페이스와 유선 인터페이스 간에 패킷이 전달됩니다.

임시 활성화:

```
sudo sysctl -w net.ipv4.ip_forward=1
```

영구 설정:

```
sudo nano /etc/sysctl.conf
```

파일 끝에 추가:

```
net.ipv4.ip_forward=1
```

설정 적용:

```
sudo sysctl -p
```

6. firewalld 설정

이 가이드에서는 firewalld를 사용합니다. ufw를 사용하는 경우 다른 설정이 필요합니다. 핵심은 무선 인터페이스가 속한 영역의 target을 ACCEPT로 설정하고, NAT를 활성화하는 것입니다.

무선 인터페이스 영역 확인:

```
sudo firewall-cmd --get-active-zones
```

무선 인터페이스를 internal 영역에 추가 (없는 경우):

```
sudo firewall-cmd --zone=internal --add-interface=wlp0s20f3 --permanent
sudo firewall-cmd --reload
```

internal 영역 target을 ACCEPT로 변경 (필수!):

```
sudo firewall-cmd --zone=internal --set-target=ACCEPT --permanent
sudo firewall-cmd --reload
```

public 영역에 masquerade 활성화:

```
sudo firewall-cmd --zone=public --add-masquerade --permanent
sudo firewall-cmd --reload
```

설정 확인:

```
sudo firewall-cmd --zone=internal --list-all
```

target: ACCEPT로 표시되어야 합니다. target이 default인 경우 패킷이 차단됩니다.

7. 서비스 활성화 및 시작

모든 설정이 완료되면 서비스를 활성화하고 시작합니다. 부팅 시 자동으로 시작되도록 enable 명령을 실행합니다.

서비스 활성화:

```
sudo systemctl unmask hostapd
sudo systemctl enable hostapd
sudo systemctl enable dnsmasq
```

서비스 시작:

```
sudo systemctl start hostapd
sudo systemctl start dnsmasq
```

서비스 상태 확인:

```
sudo systemctl status hostapd
sudo systemctl status dnsmasq
```

8. 재부팅 후 확인

시스템을 재부팅하여 모든 설정이 영구적으로 적용되는지 확인합니다.

재부팅:

```
sudo reboot
```

재부팅 후 확인 항목:

1. 서비스 상태: systemctl status hostapd dnsmasq
2. IP 주소: ip addr show wlp0s20f3
3. IP 포워딩: cat /proc/sys/net/ipv4/ip_forward
4. 방화벽: sudo firewall-cmd --zone=internal --list-all
5. 클라이언트 연결 테스트

9. 문제 해결 가이드

문제: 클라이언트가 인터넷에 연결되지 않음

가장 흔한 원인은 방화벽 설정입니다. 다음을 확인하세요:

1. firewalld internal 영역의 target이 ACCEPT인지 확인
2. IP 포워딩이 활성화되어 있는지 확인
3. iptables 규칙이 올바른지 확인

진단 명령어:

```
# 패킷 모니터링
sudo tcpdump -i wlp0s20f3 -n

# NAT 패킷 확인
sudo tcpdump -i enp109s0 -n icmp

# 방화벽 로그
sudo journalctl -u firewalld -f
```

문제: hostapd 시작 실패

1. 무선 인터페이스가 올바른지 확인: iwconfig
2. 드라이버가 nl80211을 지원하는지 확인
3. 다른 프로세스가 인터페이스를 사용 중인지 확인

문제: DHCP 할당 안 됨

1. dnsmasq 로그 확인: journalctl -u dnsmasq
2. 인터페이스 IP가 설정되어 있는지 확인
3. 포트 67/udp가 열려 있는지 확인

문제: 연결은 되지만 인터넷 불가

admin prohibited filter 오류가 발생하면 방화벽이 차단하는 것입니다:

```
# internal 영역 target 확인
sudo firewall-cmd --zone=internal --list-all

# ACCEPT로 변경
sudo firewall-cmd --zone=internal --set-target=ACCEPT --permanent
sudo firewall-cmd --reload
```

부록: 설정 파일 위치 요약

파일 경로	용도
/etc/hostapd/hostapd.conf	WiFi AP 설정
/etc/dnsmasq.conf	DHCP/DNS 서버 설정
/etc/network/interfaces	정적 IP 설정 (legacy)
/etc/netplan/*.yaml	정적 IP 설정 (Netplan)
/etc/sysctl.conf	IP 포워딩 설정
/etc/NetworkManager/NetworkManager.conf	NM 인터페이스 제외 설정