Introduction:

This lab is comprised of using a Cisco lightweight access point (LAP) in standalone mode. Setting up two WPA2 personal SSIDs and one WPA2 Enterprise. Then without a Wireless LAN Controller (WLC) we need to use a RADIUS server to authenticate users that connect onto the WPA2 Enterprise network. All this traffic from these SSIDs is then sent to another private network before being sent out to the internet. This lab was a testament to show our abilities of setting up APs and wireless networks, fluency in Linux, and working within limitations, in this case not having a WLC.

Background Information:

Cisco LAP is a piece of the Cisco Unified Wireless Network architecture. Cisco LAPs are meant to be connected directly to Cisco WLCs. Being lightweight APs, they cannot independently act without a WLC which manage the AP's configurations and firmware. They are also only able to handle real-time MAC functionality. The AP uses to WLC to process all non-real-time MAC functionality. LAPs use the CAPWAP (Control and Provisioning of Wireless Access Point) protocol in order to communicate with the WLC it connects to. Based off the LWAPP (Lightweight Access Point Protocol), it is used to control and manage multiple APs from one controller.

WPA2 Personal also known as WPA2 PSK (Pre-share Key) is designed for basic uses such as at home. Users connecting to the network use a passphrase that gets encrypted to authorize their connection to the network. However security of WPA2 Personal is based off how strong the PSK (Wi-Fi password) is. Being both secure and user friendly, most networks use a form of WPA Personal to as their security protocol.

WPA2 Enterprise differs from WPA2 Personal as it uses a radius server to set up user IDs. These unique user IDs require a Username and Password when initially signing into the network. This ensures everyone on a network running WPA Enterprise uses a different login credential. The network can be set up to only

allow a certain number of sessions per user ID on the network ensuring that users can't share their login with coworkers or friends. This allows for a more secure and safter network, specifically design for business environment.

FreeRADIUS is an open source RADIUS (Remote Authentication Dial-In User Service) which can be run on a computer or server for network authentication, authorization and accounting (AAA) services. Being the most used RADIUS server in the world, FreeRADIUS is used on many by many Internet Service Providers and Telecommunication companies. Its popularity stems from its scalability, security, and extensive support both from the developers and community. This lab used FreeRADIUS as we lacked WLCs which normally run the RADIUS server is for Cisco LAPs.

EAP-PEAP (Protected Extendable Authentication Protocol) is an authentication method used for wireless networks and point-to-point connections. In this lab's use case, EAP-PEAP was used to create a secure encrypted tunnel to exchange authentication information for WPA2 Enterprise users over Wi-Fi. This encryption protects the authentication information from man in the middle attacks and eavesdropping as Wi-Fi is an insecure network.

TFTP (Trivial File Transfer Protocol) server is a simple file transferring protocol that allows for users to get or put files from a remote server. Being very lightweight and easy to implement it can only read and write files, it cannot delete and edit files. Due to these limitations, today TFTP is often only used in local area networks (LANs).

Lab Summary:

When we received the AP, it was initially running k9w8. In order to run the APs in standalone mode, we first would have to change the OS version to k9w7. The first step was delete the old k9w8 flash files as well as some config and CAPWAP files on the AP, then after deleting the necessary files, we need to set up a TFTP server, here we used Tftpd64. Using the TFTP server we uploaded a new flash image onto the AP that had k9w7.

On the AP, we set up the SSIDs, VLANs, encryption type and set up server manager to communicate with the RADIUS server. The first step is to set up VLANs 2-4 to use radio 5ghz. Then set up cipher encryption with AES CCMP on VLAN 2-4 via the encryption manager. Setting up the server manager with a shared secret and the IP address of the FreeRADIUS server this allows for the AP to communicate with the RADIUS server for WPA2 Enterprise user authentication. Lastly, we set up the two WPA2 Personal SSIDs set up on VLAN 2 and 3. WPA2 Enterprise was set up similarly however instead of a PSK, select the server set up in the server manger under EAP authentication.

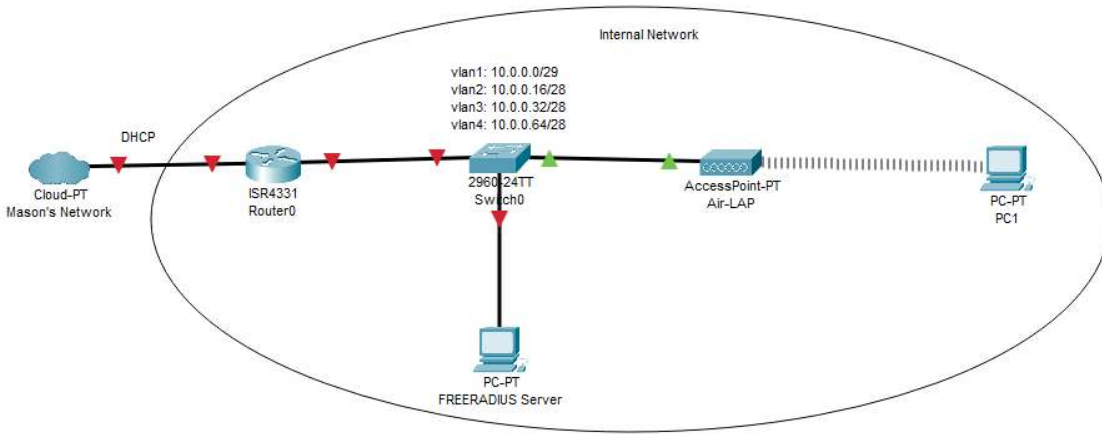
Router was relatively simple, set up the outside interface towards the other private network as a DHCP IP address. For the inside interface, we set up sub interfaces that each corelate to a VLAN. Entering the first address of each subnet, those will be the default gateway of each VLAN. NAT was done with an access-list of "any any" and setting all the IPs of the external interface, using overload, we are able to use one external IP for multiple internal IPs. DHCP can be set up on the switch, however we decided to do it on the router. Each VLAN uses its own DHCP pool.

The Switch we used had nearly zero configurations. It only required enabling the required VLANs (1-4), putting IP addresses on the VLANs, we used the 2nd available address of each subnet. Lastly we enabled trunking on the two interfaces allowing connected to the AP and the router, allow VLANs 1-4.

Linux was set up on a blank hard drive on the computer and run as a normal computer OS. We chose Ubuntu desktop as it is one of the most popular versions of Linux. Downloading Ubuntu is very similar to Windows, involving the use of a media installation key.

FreeRADIUS was downloaded using the terminal CLI within Ubuntu. We followed a guide online to download the FreeRADIUS server and to configure the IP address of the AP, shared secret, and users on the radius server. The IP address of the RADIUS server itself is the same IP address set on the computer, via Linux.

Topology:



Issues:

Many issues were encountered over the course of this lab due to its complexity and limitations (such as not having a WLC for a LAP). Out of all these issues, two stuck out the most, one being the SSIDs having a command preconfigured that wouldn't allow them to be able to be connected to. This was due to the mobility network-id which is normally meant for when the AP participates in a wireless domain service (WDS). However, when used not in this way, this command will mess with the SSID which will not allow for client to be unable to get a DHCP address or not be able to associate with the AP. The fix was to do the "no" command on each SSID for this command and remove it.

The second issue we ran into was when using Docker to run FreeRADIUS as a container. We got messages that all modules failed, and that access was rejected. We then tried using FreeRADIUS on a bare metal installation of Ubuntu (Linux), this was able to authenticate users on the WPA2 Enterprise SSID. We don't know what the issue was on Docker that didn't allow for authentication between the FreeRADIUS server and the Cisco LAP, we believe it was an issue with either something wrong with Docker or Windows that didn't allow for communication

between the RADIUS and LAP.

Conclusion:

Complexity was a major factor of this lab. Due to using many devices and software we aren't used to or completely new to us, like Linux, FreeRADIUS, TFTP and Cisco APs GUI/CLI, the lab was very confusing at first. However, groups working together and the help of tutorials on the internet eventually got us through the lab, though it took longer then expected.

Lab Commands:

AP:

```
Building configuration...



Current configuration : 4848 bytes



version 15.3

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption
```

```
hostname ap


logging rate-limit console 9

enable secret 5 $1$fENt$/2GTfkRUVWzSNNT5SU4YM/


aaa new-model


aaa group server radius my-radius-image

 server name my-radius-image


aaa group server radius rad_eap

 server name Docker


aaa group server radius rad_mac


aaa group server radius rad_acct
```

```
aaa group server radius rad_admin

aaa group server tacacs+ tac_admin

aaa group server radius rad_pmip

aaa group server radius dummy

aaa group server radius rad_eap3
 server name Docker

aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login eap_methods3 group rad_eap3
aaa authorization exec default local
aaa accounting network acct_methods start-stop group
rad_acct
```

```
aaa session-id common
no ip source-route
no ip cef


dot11 pause-time 100
dot11 syslog
dot11 vlan-name CCNP-0802-2 vlan 2
dot11 vlan-name CCNP-0802-3 vlan 3
dot11 vlan-name CCNP-0802-4 vlan 4
dot11 vlan-name VLAN1 vlan 1


dot11 ssid CCNP-12-0802-SSID-2
   vlan 2
   authentication open
   authentication key-management wpa version 2
   mbssid guest-mode
```

```
   wpa-psk ascii 7 03145A1815182E5E4A


dot11 ssid CCNP-12-0802-SSID-3
   vlan 3
   authentication open
   authentication key-management wpa version 2
   guest-mode
   mbssid guest-mode
   wpa-psk ascii 7 051B071C325B411B1D


dot11 ssid CCNP-12-0802-SSID-4
   vlan 4
   authentication open eap eap_methods3
   authentication network-eap eap_methods3
   authentication key-management wpa
   mbssid guest-mode
```

```
eap profile trest
 method md5

no ipv6 cef

username Cisco password 7 01300F175804

bridge irb

interface Dot11Radio0
 no ip address
 shutdown
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
```

```
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding

interface Dot11Radio1
 no ip address

 encryption vlan 2 mode ciphers aes-ccm

 encryption vlan 3 mode ciphers aes-ccm

 encryption vlan 4 mode ciphers aes-ccm

 encryption vlan 1 mode ciphers wep128

 ssid CCNP-12-0802-SSID-2
```

```
 ssid CCNP-12-0802-SSID-3


 ssid CCNP-12-0802-SSID-4


 antenna gain 0
 peakdetect
 dfs band 3 block
 mbssid
 channel dfs
 station-role root


interface Dot11Radio1.1
 encapsulation dot1Q 1 native
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
```

```
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1.2
 encapsulation dot1Q 2
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 spanning-disabled
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding


interface Dot11Radio1.3
 encapsulation dot1Q 3
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 spanning-disabled
```

```
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding


interface Dot11Radio1.4
 encapsulation dot1Q 4
 bridge-group 4
 bridge-group 4 subscriber-loop-control
 bridge-group 4 spanning-disabled
 bridge-group 4 block-unknown-source
 no bridge-group 4 source-learning
 no bridge-group 4 unicast-flooding


interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
```

```
interface GigabitEthernet0.1
 encapsulation dot1Q 1 native
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning


interface GigabitEthernet0.2
 encapsulation dot1Q 2
 bridge-group 2
 bridge-group 2 spanning-disabled
 no bridge-group 2 source-learning


interface GigabitEthernet0.3
 encapsulation dot1Q 3
 bridge-group 3
 bridge-group 3 spanning-disabled
```

```
 no bridge-group 3 source-learning


interface GigabitEthernet0.4
 encapsulation dot1Q 4
 bridge-group 4
 bridge-group 4 spanning-disabled
 no bridge-group 4 source-learning


interface BVI1
 mac-address 44d3.ca5a.86bb
 ip address 10.0.0.2 255.255.255.0
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable


ip forward-protocol nd
ip http server
```

```
no ip http secure-server

ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag

ip radius source-interface BVI1



radius-server local

  no authentication eapfast

  no authentication mac

  nas 10.0.0.67 key 7 03105E1812062F4B1F5B4A

  user CCNP nthash 7
12415D43442D5B210B0E017015177342503727510 07B7C770C5D533A410C
000170



radius-server attribute 32 include-in-access-req format %h



radius server Docker

 address ipv4 10.0.0.4 auth-port 1812 acct-port 1813

 key 7 131112011F050A2D7A767B
```

```
bridge 1 route ip


line con 0

line vty 0 4

 transport input all


End
```

Router:

```
Building configuration...



Current configuration : 2357 bytes


 Last configuration change at 22:18:12 UTC Fri May 24 2024
```

```
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core

hostname root

boot-start-marker
boot-end-marker

vrf definition Mgmt-intf

 address-family ipv4
 exit-address-family

 address-family ipv6
 exit-address-family
```

```
no aaa new-model


ip dhcp excluded-address 10.0.0.0 10.0.0.15
ip dhcp excluded-address 10.0.0.17
ip dhcp excluded-address 10.0.0.33
ip dhcp excluded-address 10.0.0.65
ip dhcp excluded-address 10.0.0.18
ip dhcp excluded-address 10.0.0.34
ip dhcp excluded-address 10.0.0.66


ip dhcp pool vlan2
 network 10.0.0.16 255.255.255.240
 default-router 10.0.0.17
 dns-server 1.1.1.1


ip dhcp pool vlan3
```

```
 network 10.0.0.32 255.255.255.240
 dns-server 1.1.1.1
 default-router 10.0.0.33


ip dhcp pool vlan4
 network 10.0.0.64 255.255.255.240
 dns-server 1.1.1.1
 default-router 10.0.0.65


subscriber templating
multilink bundle-name authenticated


license udi pid ISR4321/K9 sn FDO214421CF


spanning-tree extend system-id


redundancy
```

```
 mode none


vlan internal allocation policy ascending


interface GigabitEthernet0/0/0
 no ip address
 ip nat inside
 negotiation auto


interface GigabitEthernet0/0/0.1
 encapsulation dot1Q 1 native
 ip address 10.0.0.6 255.255.255.248


interface GigabitEthernet0/0/0.2
 encapsulation dot1Q 2
 ip address 10.0.0.17 255.255.255.240
 ip nat inside
```

```
interface GigabitEthernet0/0/0.3
 encapsulation dot1Q 3
 ip address 10.0.0.33 255.255.255.240
 ip nat inside

interface GigabitEthernet0/0/0.4
 encapsulation dot1Q 4
 ip address 10.0.0.65 255.255.255.240
 ip nat inside

interface GigabitEthernet0/0/1
 ip address dhcp
 ip nat outside
 negotiation auto

interface Serial0/1/0
```

```
 no ip address


interface Serial0/1/1

 no ip address


interface GigabitEthernet0

 vrf forwarding Mgmt-intf

 no ip address

 negotiation auto


interface Vlan1

 no ip address


ip nat inside source list 101 interface GigabitEthernet0/0/1
overload

ip forward-protocol nd

no ip http server
```

```
no ip http secure-server

ip tftp source-interface GigabitEthernet0


access-list 101 permit ip 10.0.0.0 0.0.0.255 any


control-plane


line con 0

 stopbits 1

line aux 0

 stopbits 1

line vty 0 4

 login


End
```

Switch:

```
Building configuration...


Current configuration : 4247 bytes


version 12.2
service config
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption


hostname swat


boot-start-marker
boot-end-marker


no aaa new-model
```

```
system mtu routing 1500

vtp domain CCNP

vtp mode transparent

authentication mac-move permit

ip subnet-zero



crypto pki trustpoint TP-self-signed-1177695488

 enrollment selfsigned

 subject-name cn=IOS-Self-Signed-Certificate-1177695488

 revocation-check none

 rsakeypair TP-self-signed-1177695488



crypto pki certificate chain TP-self-signed-1177695488

 certificate self-signed 01

  3082023D 308201A6 A0030201 02020101 300D0609 2A864886
F70D0101 04050030

  31312F30 2D060355 04031326 494F532D 53656C66 2D536967
6E65642D 43657274
```

69666963 6174652D 31313737 36393534 3838301E 170D3933
30333031 30313330

35385A17 0D323030 31303130 30303030 305A3031 312F302D
06035504 03132649

4F532D53 656C662D 5369676E 65642D43 65727469 66696361
74652D31 31373736

39353438 3830819F 300D0609 2A864886 F70D0101 01050003
818D0030 81890281

8100A6E5 67F16507 541FAA8A 24390EEF D50BC644 F5156F79
8922F09A DB36C3F1

5477482D 07853625 71E151C7 E0ABEE90 471AC9C5 141D0D8D
DDB908D4 742F67E8

043A6FC7 06D499B4 DCF33995 7CFBDF05 A85B65BA 24FB7C0D
E3EB61D5 78A48F1A

6DFA81A4 0516B3CF 1F67715B D200899A CA83B8E7 B16CDACC
6C29BFFE EC07A9CA

96B50203 010001A3 65306330 0F060355 1D130101 FF040530
030101FF 30100603

551D1104 09300782 05737761 742E301F 0603551D 23041830
16801421 7300C95A

4C83C28E 6AB44241 23BC39F9 40863130 1D060355 1D0E0416
04142173 00C95A4C

83C28E6A B4424123 BC39F940 8631300D 06092A86 4886F70D
01010405 00038181

```
  0019D385 BF74AA07 BDA0F9B1 E0290766 4042C746 C742C3F9
B53F3970 11A91861

  193A3B09 5CBA0583 1E5E26BE 57DFE12A DD277040 F77DEB1D
CEB764BF DB4064C3

  7EDEE037 C0FBFC98 AC3795E2 E6F1D9B2 8311A76C 3BF958D5
C3353325 BAD16A2F

  2A3F8FA4 22054C45 B910AA5D EB3E5B62 1F49CB47 04ED546F
6614BD42 5C652819 4E

  quit



spanning-tree mode pvst

spanning-tree etherchannel guard misconfig

spanning-tree extend system-id



vlan internal allocation policy ascending



vlan 2-5,7



vlan 10
```

```
 name DATA


vlan 11-12


vlan 20
 name VOICE


vlan 29


vlan 30
 name MGT


vlan 40
 name MISC


vlan 50
 name NATIVE
```

```
vlan 99
 name MANAGEMENT

vlan 100,192,400,999

interface FastEthernet0/1

interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk

interface FastEthernet0/3

interface FastEthernet0/4
```

```
interface FastEthernet0/5

interface FastEthernet0/6

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13
```

```
interface FastEthernet0/14

interface FastEthernet0/15

interface FastEthernet0/16

interface FastEthernet0/17

interface FastEthernet0/18

interface FastEthernet0/19

interface FastEthernet0/20

interface FastEthernet0/21
```

```
interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface FastEthernet0/25

interface FastEthernet0/26

interface FastEthernet0/27

interface FastEthernet0/28

interface FastEthernet0/29

interface FastEthernet0/30
```

```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk

interface FastEthernet0/31

interface FastEthernet0/32

interface FastEthernet0/33

interface FastEthernet0/34

interface FastEthernet0/35

interface FastEthernet0/36

interface FastEthernet0/37
```

```
interface FastEthernet0/38

interface FastEthernet0/39

interface FastEthernet0/40

interface FastEthernet0/41

interface FastEthernet0/42

interface FastEthernet0/43

interface FastEthernet0/44

interface FastEthernet0/45
```

```
interface FastEthernet0/46

interface FastEthernet0/47

interface FastEthernet0/48

interface GigabitEthernet0/1

interface GigabitEthernet0/2

interface GigabitEthernet0/3

interface GigabitEthernet0/4

interface Vlan1
 ip address dhcp
```

```
interface Vlan2
 no ip address

ip classless
ip http server
ip http secure-server

ip sla enable reaction-alerts

line con 0
line vty 0 4
 login
line vty 5 15
 login

end
```

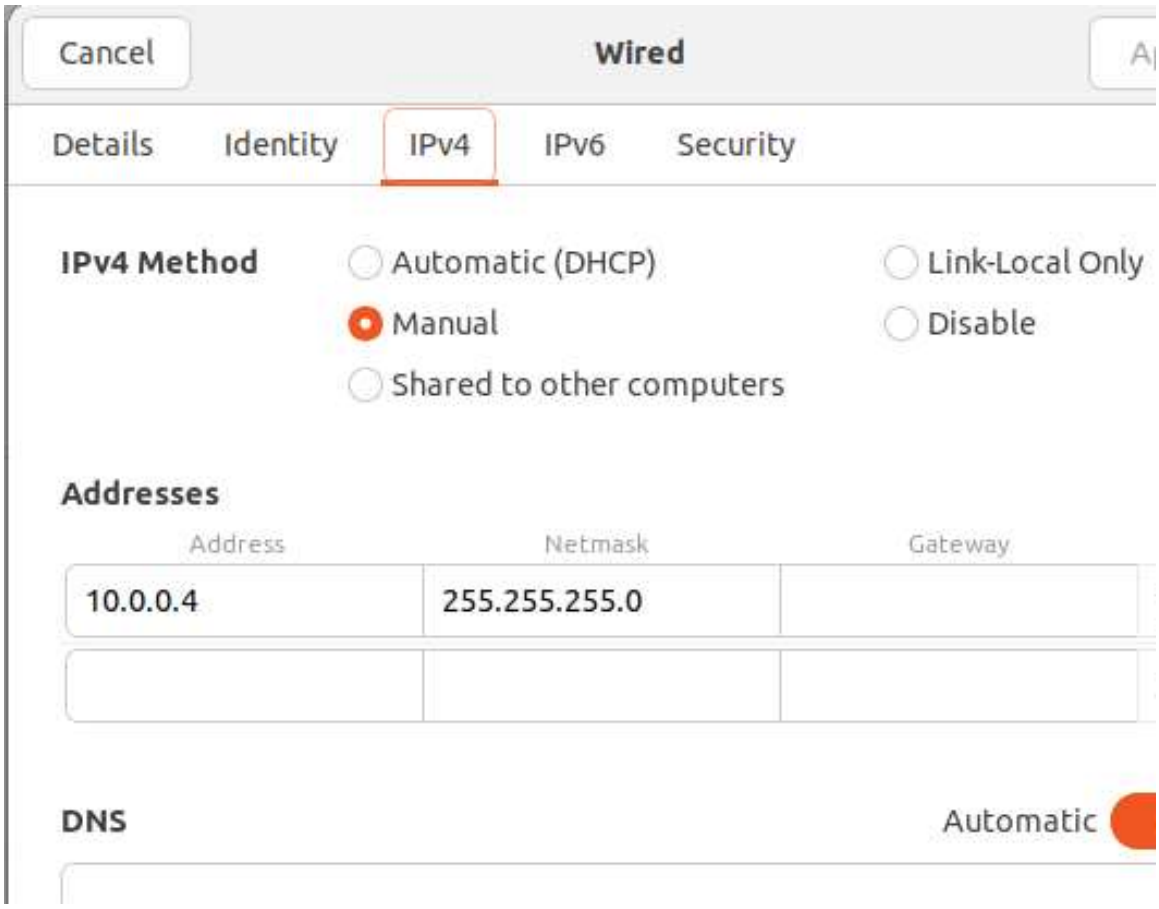
FreeRADIUS install Commands:

- sudo apt update
- sudo apt install freeradius freeradius-utils
- sudo nano /etc/freeradius/3.0/clients.conf
- clients kevinAP {

  ipaddr = 10.0.0.2

  secret = testing123
- sudo nano /etc/freeradius/3.0/users
- bob Cleartext-Password := “testing”
- sudo freeradius -X

IP on Linux:


Cancel
Wired
Details
Identity
IPv4
IPv6
Security
IPv4 Method
Automatic (DHCP)
Link-Local Only
Manual
Disable
Shared to other computers
Addresses
Address
Netmask
Gateway
10.0.0.4
255.255.255.0
DNS
Automatic