Setting up Vlans on an Asus Rt-N16

Big credit to **80sguitartist** for this

Here is what will be accomplished:

- The physical Port 1 on the back of router called LAN1 will broadcast an IP address on the 192.168.1.X subnet.
- Physical Port 2 (LAN2) will broadcast an IP address on the 192.168.2.X subnet.
- Physical Port 3 (LAN3) will broadcast an IP address on the 192.168.3.X subnet.
- Physical Port 4 (LAN4) will broadcast an IP address on the 192.168.4.X subnet.
- NO Firewall scripts have been put into place to prevent anyone from talking to each other on other subnets. (a firewall example is shown in the next section)

This is a tutorial on getting VLAN's working NOT restricting Access. If everything looks good to those on the board I will update this with Firewall scripts but for now I just want to make sure what I have is correct and there are no major flaws.

- Everyone should be able to get out to the Internet. (Obviously, you need a working Internet connection going into the WAN port.)

- 1. First and Foremost. I have only tested these instructions on the following build?s of DD-WRT. Others could work but your mileage may vary.

```
DD-WRT v24-18024_NEWD-2_K2.6_mega.bin
DD-WRT v24-14896_NEWD-2_K2.6_mini.bin
```

- 2. Freshly install one of the builds above and reset to factory defaults. I have found the easiest way to do this is to log in to the router via telnet command and type in ?erase nvram?. Hit the Enter key and then type in ?reboot?. The Factory defaults will be restored. After you have reset everything wait a couple of minutes before you proceed. Go take a piss or something.

- 3. Plug your computer into **LAN1** on the back of the router.

- 4. Open a browser (IE or Firefox, not sure about Chrome) and go to 192.168.1.1.

- 5. Change the username and password when prompted. I used the typical username ?root? and password ?admin?.

- 6. Once you changed the username and password and you know they work Close Internet Explorer.

- 7. Open a Command prompt and Telnet into the router 192.168.1.1, log in, and then input these commands below. After each line, hit the Enter key.

```
nvram set vlan1ports="4 8"
nvram set vlan3ports="2 8"
nvram set vlan4ports=?1 8?
```

```
nvram set vlan5ports=?3 8?
nvram commit
reboot
```

- 8. Gonna have to wait a few minutes for it to reboot. Get a cup of coffee or something.
- 9. Login into web interface 192.168.1.1 and then go to **Setup-->Vlans.**

```
Uncheck Port 1 and put a checkmark for VLAN 4 for Port 1.
Uncheck Port 2 and put a checkmark for VLAN 3 for Port 2.
Uncheck Port 3 and put a checkmark for VLAN5 for Port 3.
```

- 10. Click **Save**
- 11. Go to the **Administration** tab and then click Reboot Router. You must do this to get the Vlan 2, 3 and 4 options to show up in the next steps.
- 12. Yep, you?re waiting a few minutes for it to reboot again. Just think about how happy you?ll be when this works. But make sure to think for a couple minutes.
- 13. Log back in to the router and go to **Setup-->Networking**.
- 14. Go down to **Port Setup** and for each of the Network Configurations for vlan3, vlan4, and vlan5 click on Unbridged. This will let you enter in the values below (enter those values)

```
Network Configuration vlan3 = Unbridged
IP address: 192.168.3.1
Subnet Mask: 255.255.255.0

Network Configuration vlan4 = Unbridged
IP address: 192.168.4.1
Subnet Mask: 255.255.255.0

Network Configuration vlan5 = Unbridged
IP address: 192.168.2.1
Subnet Mask: 255.255.255.0
```

- 15. After all the above have been entered click on **Save**
- 16. You should still be in the **Setup-->Networking** Page. Go to the bottom and for the section on DHCPD click on **Add** under **Multiple DHCP Server.**

- 17. Click on the Dropdown where it currently says **eth0** and choose vlan3. Then click on **Save.**

- 18. Again, click on the Add button in the DHCP section like you just did. This time we want to change the DHCP 1 entry to vlan 4. Then click on **Save.**

- 19. One more time, click on the **Add** button and change it to vlan5. Then click on **Save.**

- 20. Now click on **Apply Settings.**

- 21. Go to the **Administration** tab and then click **Reboot Router.**

- 22. This should be the last time you have to wait. So get ready for some ultimate VLAN?ing fun. Oh Yeah!

- 23. Moment of Truth! Here is what your results should be below. **VERY IMPORTANT!** If you are quickly unplugging and plugging into the various ports on the router you need to release and renew your IP address on your computer. Otherwise, your NIC will cache the old IP address it just got. So, when plugging into different ports, do a release and renew of your IP address. Results should be:

Tests:

- Plugging into LAN4 (Actual port on the router itself) should give you a **192.168.4.X** address.
- Plugging into LAN3 should give you a **192.168.3.X** address.
- Plugging into LAN2 should give you a **192.168.2.X** address.
- Plugging into LAN1 give you **192.168.1.X** addresses.
- Any port should be able to get out to the Internet.

- 24. Now, You?ve got some VLANs but everyone can talk to everyone else. You need to setup firewall scripts to prevent that. Continue on to the Firewall Scripts.

Firewall Scripts

I had a lot of trouble getting my Firewall Scripts working. Initially, what I found on the web for setting the Asus RT-N16 did not work. I found that every page that referenced the VLAN firewall scripts appeared to be with the use of the command INPUT versus the command FORWARD. Once I got this correct the following

results should occur when following the instructions below.

End traffic results:

- Routing will work like any common network on the LAN (192.168.1.1)
- Clients on VLAN3 (192.168.3.1), VLAN4 (192.168.4.1), and VLAN5 (192.168.2.1) will not be able to Access the router?s IP at 192.168.1.1 via telnet, web, etc. They will be able to ping the IP.
- Each VLAN cannot access each other or the clients that are connected through a different VLAN. For example, Clients on VLAN3 cannot access anything but other clients on VLAN3 and the Internet.
- If a client tries to ping anyone on a different VLAN there is no response.

- 1. Plug your computer in **LAN1** on the back of the router.

- 2. Open a browser (IE or Firefox, not sure about Chrome) and go to 192.168.1.1.

- 3. Go to **Administration-->Commands.**

- 4. Input the commands below into the Command window. You should be able to copy and paste.

```
# Accept traffic into vlan5
iptables -I INPUT -i vlan5 -j ACCEPT
# Allow traffic outbound to forward from vlan5 to vlan2 (WAN)
iptables -I FORWARD -i vlan5 -o vlan2 -m state --state NEW -j ACCEPT
# Disallow access to the router on vlan5 through the typical ports for management (telnet,ftp,ssh
iptables -I INPUT -i vlan5 -p tcp -m multiport --dports 21,22,23,80,443 -j DROP
# Disallow anything on 192.168.2.X (vlan5) to communicate to the other networks
iptables -I FORWARD -s 192.168.2.0/255.255.255.0 -d 192.168.1.0/255.255.255.0 -j DROP
iptables -I FORWARD -s 192.168.2.0/255.255.255.0 -d 192.168.3.0/255.255.255.0 -j DROP
iptables -I FORWARD -s 192.168.2.0/255.255.255.0 -d 192.168.4.0/255.255.255.0 -j DROP
iptables -I FORWARD -s 192.168.2.0/255.255.255.0 -d 192.168.5.0/255.255.255.0 -j DROP
# Disallow anything on the bridge interface to communicate to vlan5
iptables -I FORWARD -i br0 -o vlan5 -j logdrop
```

```
# Accept traffic into vlan3
iptables -I INPUT -i vlan3 -j ACCEPT
# Allow traffic outbound to forward from vlan3 to vlan2 (WAN)
iptables -I FORWARD -i vlan3 -o vlan2 -m state --state NEW -j ACCEPT
# Disallow access to the router on vlan3 through the typical ports for management (telnet,ftp,ssh
iptables -I INPUT -i vlan3 -p tcp -m multiport --dports 21,22,23,80,443 -j DROP
iptables -I FORWARD -s 192.168.3.0/255.255.255.0 -d 192.168.1.0/255.255.255.0 -j DROP
iptables -I FORWARD -s 192.168.3.0/255.255.255.0 -d 192.168.2.0/255.255.255.0 -j DROP
iptables -I FORWARD -s 192.168.3.0/255.255.255.0 -d 192.168.4.0/255.255.255.0 -j DROP
iptables -I FORWARD -s 192.168.3.0/255.255.255.0 -d 192.168.5.0/255.255.255.0 -j DROP
```

```
# Disallow anything on the bridge interface to communicate to vlan3
iptables -I FORWARD -i br0 -o vlan3 -j logdrop



# Accept traffic into vlan4
iptables -I INPUT -i vlan4 -j ACCEPT
# Allow traffic outbound to forward from vlan4 to vlan2 (WAN)
iptables -I FORWARD -i vlan4 -o vlan2 -m state --state NEW -j ACCEPT
# Disallow access to the router on vlan4 through the typical ports for management (telnet,ftp,ssh
iptables -I INPUT -i vlan4 -p tcp -m multiport --dports 21,22,23,80,443 -j DROP
iptables -I FORWARD -s 192.168.4.0/255.255.255.0 -d 192.168.1.0/255.255.255.0 -j DROP
iptables -I FORWARD -s 192.168.4.0/255.255.255.0 -d 192.168.2.0/255.255.255.0 -j DROP
iptables -I FORWARD -s 192.168.4.0/255.255.255.0 -d 192.168.3.0/255.255.255.0 -j DROP
iptables -I FORWARD -s 192.168.4.0/255.255.255.0 -d 192.168.5.0/255.255.255.0 -j DROP
# Disallow anything on the bridge interface to communicate to vlan4
iptables -I FORWARD -i br0 -o vlan4 -j logdropic into vlan5
iptables -I INPUT -i vlan5 -j ACCEPT
```

- 5. Click on **Save Firewall.**

- 6. Go to **Administration-->Management**

- 7. Click on **Reboot Router.**

You should now have an Asus RT-N16 with Firewall scripts to prevent VLANs from accessing other VLANs.