BRINGING NET-44 AND IPV6 TO YOUR STATION VIA VPN

A brief presentation on creating your own Internet connected network for Amateur Radio using a VPN tunnel and BGP advertised static IP address space.
Net-44 (AmpRNet)

- What is it?
  - Net-44 is a Class-A CIDR /8 IPv4 Network
  - 16 million IP addresses
  - We've had it for 20-30 years
  - It's a valuable, largely unused resource
  - Exclusively for Amateur Radio

DCC – 2012 ATLANTA
What Will Be Covered

This presentation will examine the steps and resources to create a VPN connected static IP address space in Net-44 and IPv6 to:

• Enable Amateur Radio services such as websites and databases
• Enable access to station resources over the Internet
• Add Amateur Radio IoT (WX station, Remote Control, …)

Ground rules:
Net-44 addresses may only be used for Amateur Radio experimentation and infrastructure. IPv6 Addresses may be used for any legal purpose.

Transmissions on amateur frequencies must conform to Amateur Radio Service rules.
Applications

Self hosted Amateur Radio Websites and Services

• Fixed (static) IP addresses and domain names (Reuse well known ports, e.g. 80/443)
  • nw7dr.ampr.org
  • 44.24.135.10
Applications

Remote Station Management and Operation

44.x.x.100

VPN – Internet - VPN

44.x.x.25

John Hays – K7VE
john@hays.org
Applications

Fixed IP While Traveling / Mobile (Tunnel through LTE Example)

LAN – 44.x.x.x

Wifi/Wired with DHCP/Static
Applications

Repeater/Node/Gateway Site Linking with Static IP Addresses

Telemetry
IoT

AllStar
EchoLink

APRS

VPN - Internet

D-STAR

DMR

???
Obtaining Net-44 Addresses

Create an account on https://portal.ampr.org
Obtaining Net-44 Addresses
Obtaining Net-44 Addresses

Select ‘Networks’ and navigate to your regional network
Obtaining Net-44 Addresses

When you reach your regional network, you will be presented with existing allocations.

At the bottom of the list, you can request an allocation by clicking on the link, e.g. 44.24.0.0/16

<table>
<thead>
<tr>
<th>Address Range</th>
<th>Description</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.24.200.0 / 22</td>
<td>San Juan County KD7KAB</td>
<td>KD7KAB</td>
</tr>
<tr>
<td>44.24.221.0 / 24</td>
<td>HamWAN PSDL Anycast</td>
<td>K7WAN</td>
</tr>
<tr>
<td>44.24.240.0 / 20</td>
<td>HamWAN PSDL</td>
<td>K7WAN</td>
</tr>
</tbody>
</table>

If the address range you want is not within any of the subnets above, or the region you are located in is not listed above, you may request an allocation from the parent network by clicking here: 44.24.0.0/16

You need to be logged in to request an allocation. If you are not logged in when you make a request, you will be re-directed to the login page.

Go back to parent network
Obtaining Net-44 Addresses

Fill in the form, select a /24 netmask, end user, and direct(BGP). In the notes, let the coordinator know your plans for the network.

Send and await the allocation. BGP allocations will pass through ARDC and require additional paperwork.

ARDC will generate a letter for your network provider to permit routing and advertisement of your subnet.

If you need to request a specific IP or range of IP’s, for example, because you already have an allocation and need to get it registered on this portal, please let the coordinator know by specifying the IP(s) in the “Notes” box. If this is a new request, the coordinator will allocate your IP(s) from the available space within the subnet above. Please ensure that you select the netmask based on the size of the allocation you are requesting.
When your ‘direct (BGP)’ allocation is processed, you will be assigned the block of addresses for your subnet.

In order to have a network service provider route your subnet, additional information will be required by the ARDC.

Example information from Spartan Host <sales@spartanhost.net> – verify with provider before submitting.

- ASN that will advertise the subnet: 201106
- Network Service Provider name: Spartan Host Ltd
- NSP postal address: 280 Comber Road, Dundonald, Belfast, BT16 1UR, United Kingdom
- NSP telephone: +446029105858
Spartan Host Provisioning Example

Order at https://spartanhost.org/vps
Spartan Host Provisioning Example

Select your plan and configure on next screen.

I use Ubuntu 64-bit 16.04, select defaults on the rest.
Spartan Host Provisioning Example

Check out

Shortly thereafter the host will be setup and ready to use.

Optionally, and recommended, as part of the setup you can enable 2 factor authentication for the VPS control panel. It uses the Google Authenticator application.
Spartan Host Provisioning Example (Control Panel)
Spartan Host Provisioning Example (Report)
Spartan Host Provisioning Example

**ssh** or **vnc** into your host
Update the VPS Server

See [https://groups.io/g/net-44-vpn/wiki/](https://groups.io/g/net-44-vpn/wiki/)

**Update Ubuntu**
Issue the following commands

```
apt-get update
apt-get upgrade
```

Change the ssh port number by editing `/etc/ssh/sshd_config`

Note the new ssh port for future logins

Change the timezone using:

```
dpkg-reconfigure tzdata
```

reboot
Turn on router capabilities for the VPS

Edit the file `/etc/sysctl.conf` and uncomment, update, or add the following lines:

```
net.ipv4.ip_forward=1
net.ipv6.conf.all.forwarding=1
net.ipv6.conf.all.proxy_ndp=1
net.ipv4.conf.all.accept_redirects=0
net.ipv6.conf.all.accept_redirects=0
net.ipv4.conf.all.send_redirects=0
```

Save the file and then reload it with the command

```
sysctl -p
```
Install and Prepare OpenVPN

`apt-get install openvpn easy-rsa`

Adding a special new account, allows OpenVPN to run under non-root privileges, which is a good security enhancement.

`useradd vpn`

Edit and add the account to `/etc/sudoers`

```
# OpenVPN
Defaults:vpn env_keep += "ifconfig_pool_remote_ip common_name"
vpn ALL=NOPASSWD: /etc/openvpn/server-clientconnect.sh
vpn ALL=NOPASSWD: /etc/openvpn/server-clientdisconnect.sh
```

Make these changes active with a reboot

`reboot`
Create your Certificate Authority (CA)

cd /usr/share/easy-rsa

Edit and save a file named **vars** using your preferred editor. Update these variables:

```bash
export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_OU="MyOrganizationalUnit"
export KEY_NAME="server"
```

Run: `source ./vars`
Create your Certificate Authority (CA)

Generate server and Diffie Hellman parameters, then copy to /etc/openvpn:

```
./clean-all
./build-dh
./build-ca
./build-key-server server
openvpn --genkey --secret keys/ta.key
cd keys
cp ca.crt server.crt server.key ta.key dh2048.pem /etc/openvpn
```
Download Scripts and Support Files

Get allfiles.tgz from https://groups.io/g/net-44-vpn/files and save to /tmp

```
  cd /tmp
  tar -xzf allfiles.tgz
  cd /tmp/etc/openvpn
  cp * /etc/openvpn
  cd /tmp/usr/share/easy-rsa
  cp * /usr/share/easy-rsa
```

Make sure the scripts are executable and create the "Client Configuration Directory"

```
  cd /usr/share/easy-rsa
  chmod +x *.sh
  cd /etc/openvpn
  chmod +x *.sh
  mkdir ccd
```
Update Network Variables and Make server.conf

With your net-44 subnet and netmask in hand, along with the IPv6 prefix from your Spartan Host account, edit the file `/etc/openvpn/network-variables`.

Replace values marked in yellow below with your network values.

```
LOCALIPV4=127.0.0.1
IPV6PRE=2006:f00d:beef:4e
IPV4NETWORK=44.1.0.0
IPV4NETMASK=255.255.255.0
```

Run the script to build the server.conf file.

```
cd /etc/openvpn
./server.config.sh
```

This will create a file named `server.conf.new`, review it's contents and if it looks right copy it to `server.conf`.

John Hays – K7VE
john@hays.org
Set Tunnel Value and Start OpenVPN

Define the Tunnel
Edit the file `/etc/openvpn/variables` it will contain two lines

```plaintext
prefix=aaaa:bbbb:cccc:dddd:80::
prefixlen=112
```

`aaaa:bbbb:cccc:dddd` should be the IPv6 prefix from your Spartan Host account.

Startup and Enable the VPN server
Start the server, look at its status, and if OK, then enable it.

```bash
systemctl start openvpn@server
systemctl status openvpn@server
systemctl enable openvpn@server
```

If you followed all of the steps correctly, you should have a working VPN Server!
Setup Clients – Update Template

Run build-template.sh, It will create a file config.openvpng.tpl.new which should be copied to config.openvpng.tpl

cd /usr/share/easy-rsa
./build-template.sh
cp config.ovpn.tpl.new config.ovpn.tpl

Note: This configuration file uses the public IP address of the VPS, you may want to change it to a domain name, if you have given one to your VPS.

It only needs to be run once, you can edit the resulting config.openvpng.tpl if you need to make changes.
Setup Clients – Create OVPN Files

Repeat for each client:

```
cd /usr/share/easy-rsa
./generate_openvpn_config.sh
```

Pick a user name, you might want to use a callsign or other designation. Since we previously edited the vars file, most values will be populated correctly, so just hit return, except for the following questions:

Please type in user name for the new config: `username-of-client`
Sign the certificate? [y/n]: `y`
1 out of 1 certificate requests certified, commit? [y/n] `y`

This will create a file named `openvpn_username-of-client.ovpn`

This file will be transferred to your client after installing OpenVPN on the client.
Install and Configure OpenVPN on Clients

OpenVPN is available for almost all major modern operating system, including Microsoft Windows, Mac OS, Linux, Unix, Android, Apple IOS, ... see https://openvpn.net/ for many clients.

Raspberry Pi - Raspbian and Similar Linux Devices

Login to your device and do the install

```
sudo apt-get update
sudo-apt-get upgrade
sudo apt-get install openvpn unzip
```
Install and Configure OpenVPN on Clients

Install OVPN Configuration
Copy the .ovpn file you created to the local system. It should be placed in /etc/openvpn - sftp is a good method.

```bash
 cd /etc/openvpn
 # If you have changed the ssh port, use sftp -P <portnumber> root@[VPS Host]
sudo sftp root@[Your VPS IP or Domain Name]
sftp> cd /usr/share/easy-rsa
sftp> get openvpn_username-of-client.ovpn
sftp> exit
sudo mv openvpn_username-of-client.ovpn username-of-client.conf
```

# I like dropping the openvpn_, and on Linux .conf is preferred to .ovpn for the filename

John Hays – K7VE
john@hays.org
Running OpenVPN on Clients

Startup Your Client

```bash
sudo openvpn --config /etc/openvpn/username-of-client.conf --daemon
# wait a short time and
ifconfig tun0
hostname -I
```
Assigning IP Addresses and Subnets to a Client

Login to your VPS as root, then

```
cd /etc/openvpn
./make-ccd.sh
```

Example (Use a netmask of 255.255.255.255 for a single address, see what mask to use for subnets at http://www.rjsmith.com/CIDR-Table.html

Building CCD file ..
Client Name (same as used when building ovpn file)
username-of-client

Host IPv4 address to assign to client (in 44.1.0.0/255.255.255.0)
44.1.0.20

Client subnet mask, eg. 255.255.255.255 or 255.255.255.240
255.255.255.240

Host IPv6 address to assign to client (2006:f00d:beef:4e:80::xxxx)
2006:f00d:beef:4e:80::1001

John Hays – K7VE
john@hays.org
Assigning and Monitoring Client IP Addresses

The `make-ccd.sh` will create a file in `/etc/openvpn/ccd` with the same name as the username, e.g. `username-of-client` that will be used to setup the client addressing and routing.

Example content of `/etc/openvpn/ccd/username-of-client`:

```
ifconfig-push 44.1.0.20 255.255.255.255.0
ifconfig-ipv6-push 2006:f00d:beef:4e:80::1001/112 2006:f00d:beef:4e::1
iroute 44.1.0.20 255.255.255.240
route-ipv6 2006:f00d:beef:4e:80::<
```

If your client doesn’t pick up these values, restart the OpenVPN server, as root on your VPS:

```
systemctl restart openvpn@server
```

You can see the clients that logged in with:

```
cat /etc/openvpn/openvpn-status.log
```
Monitoring Connected Clients

A web based monitoring tool is available.

You can optionally use Let’s Encrypt to provide https for non-radio connections.

https://github.com/furlongm/openvpn-monitor

John Hays — K7VE
john@hays.org
Caveats and Considerations

I encourage sharing an account and subnet, but this comes with special responsibilities:
• Keep up to date contact information on portal.ampr.org
• Periodically make sure that the addresses are not being used inappropriately
  • Revoke certificates of abusers
  • Stop routing subnets that have been compromised or for DMCA takedown requests.

Install and maintain firewalls to help enforce usage standards
A VPN'ed host has access to your LAN, so take proper isolation measures and/or firewall rules.
Q&A – and Help

A support and sharing group is at https://groups.io/g/net-44-vpn

John Hays – K7VE
john@hays.org