

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.



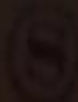
Net-44 (AmprNet)

- 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

NOW
HAM RADIO

John Hays – K7VE john@hays.org


Sheraton
Gateway Hotel
ATLANTA, GA

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.

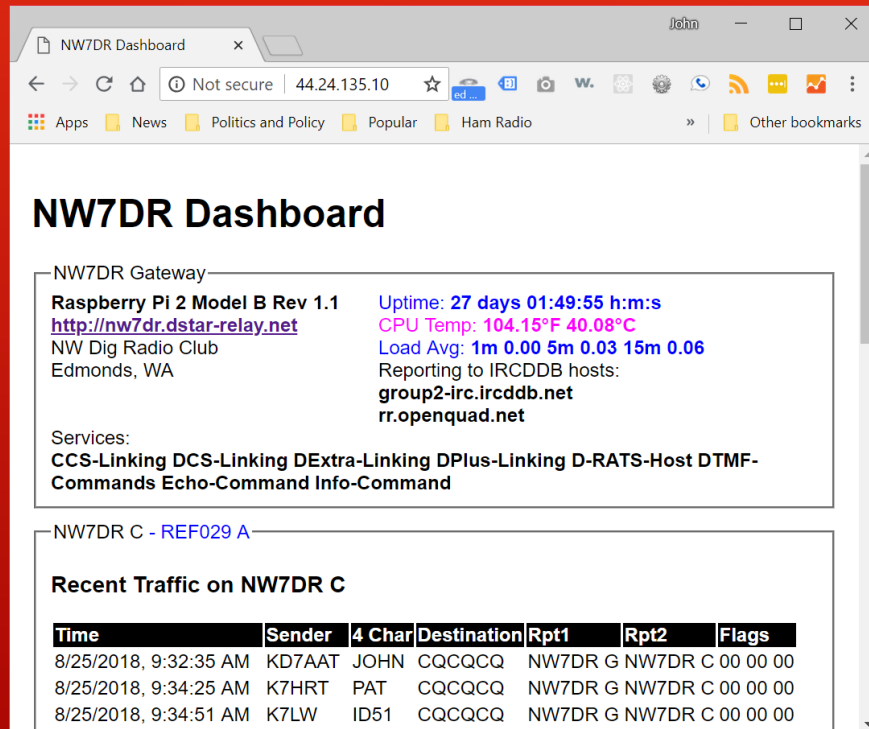
IPv6 Addresses may be used for any legal purpose.

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



NW7DR Dashboard

NW7DR Gateway

Raspberry Pi 2 Model B Rev 1.1
<http://nw7dr.dstar-relay.net>
NW Dig Radio Club
Edmonds, WA

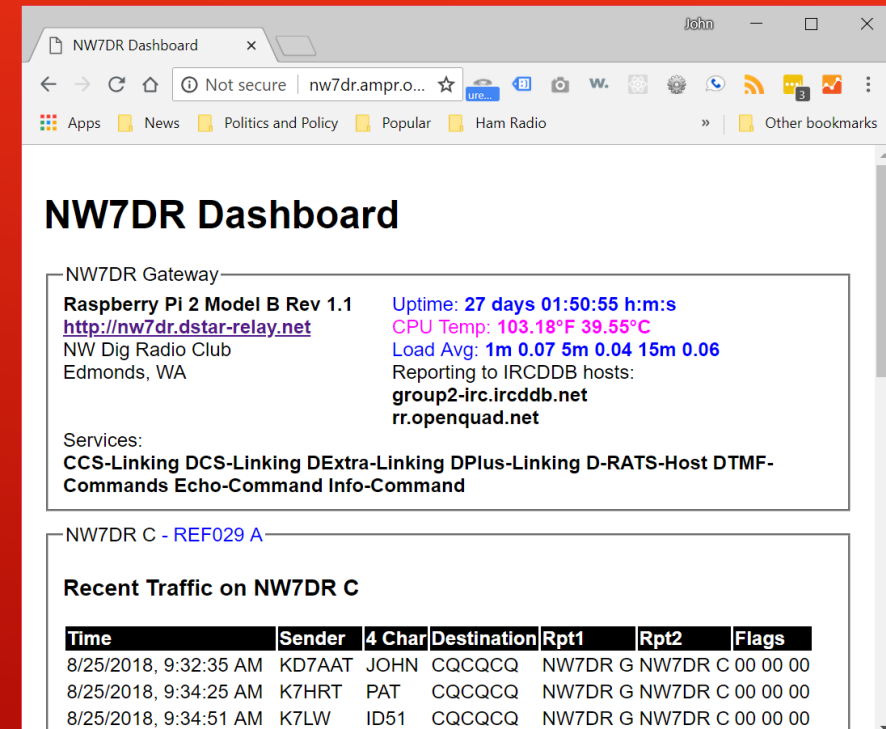
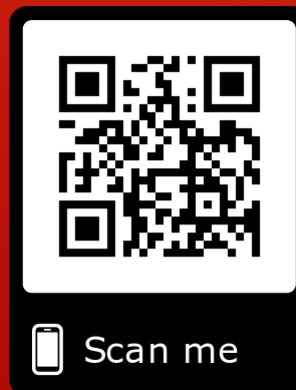
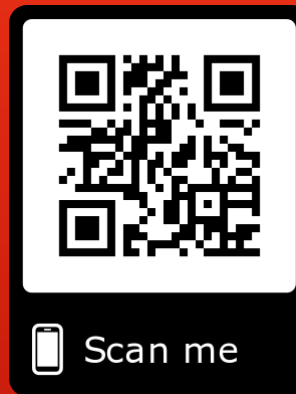
Uptime: 27 days 01:49:55 h:m:s
CPU Temp: 104.15°F 40.08°C
Load Avg: 1m 0.00 5m 0.03 15m 0.06
Reporting to IRCDB hosts:
group2-irc.ircddb.net
rr.openquad.net

Services:
CCS-Linking DCS-Linking DExtra-Linking DPlus-Linking D-RATS-Host DTMF-Commands Echo-Command Info-Command

NW7DR C - REF029 A

Recent Traffic on NW7DR C

Time	Sender	4 Char	Destination	Rpt1	Rpt2	Flags
8/25/2018, 9:32:35 AM	KD7AAT	JOHN	CQCQCQ	NW7DR G	NW7DR C	00 00 00
8/25/2018, 9:34:25 AM	K7HRT	PAT	CQCQCQ	NW7DR G	NW7DR C	00 00 00
8/25/2018, 9:34:51 AM	K7LW	ID51	CQCQCQ	NW7DR G	NW7DR C	00 00 00



NW7DR Dashboard

NW7DR Gateway

Raspberry Pi 2 Model B Rev 1.1
<http://nw7dr.dstar-relay.net>
NW Dig Radio Club
Edmonds, WA

Uptime: 27 days 01:50:55 h:m:s
CPU Temp: 103.18°F 39.55°C
Load Avg: 1m 0.07 5m 0.04 15m 0.06
Reporting to IRCDB hosts:
group2-irc.ircddb.net
rr.openquad.net

Services:
CCS-Linking DCS-Linking DExtra-Linking DPlus-Linking D-RATS-Host DTMF-Commands Echo-Command Info-Command

NW7DR C - REF029 A

Recent Traffic on NW7DR C

Time	Sender	4 Char	Destination	Rpt1	Rpt2	Flags
8/25/2018, 9:32:35 AM	KD7AAT	JOHN	CQCQCQ	NW7DR G	NW7DR C	00 00 00
8/25/2018, 9:34:25 AM	K7HRT	PAT	CQCQCQ	NW7DR G	NW7DR C	00 00 00
8/25/2018, 9:34:51 AM	K7LW	ID51	CQCQCQ	NW7DR G	NW7DR C	00 00 00

Applications

Remote Station Management and Operation



44.x.x.100

VPN – Internet - VPN



44.x.x.25

Applications

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

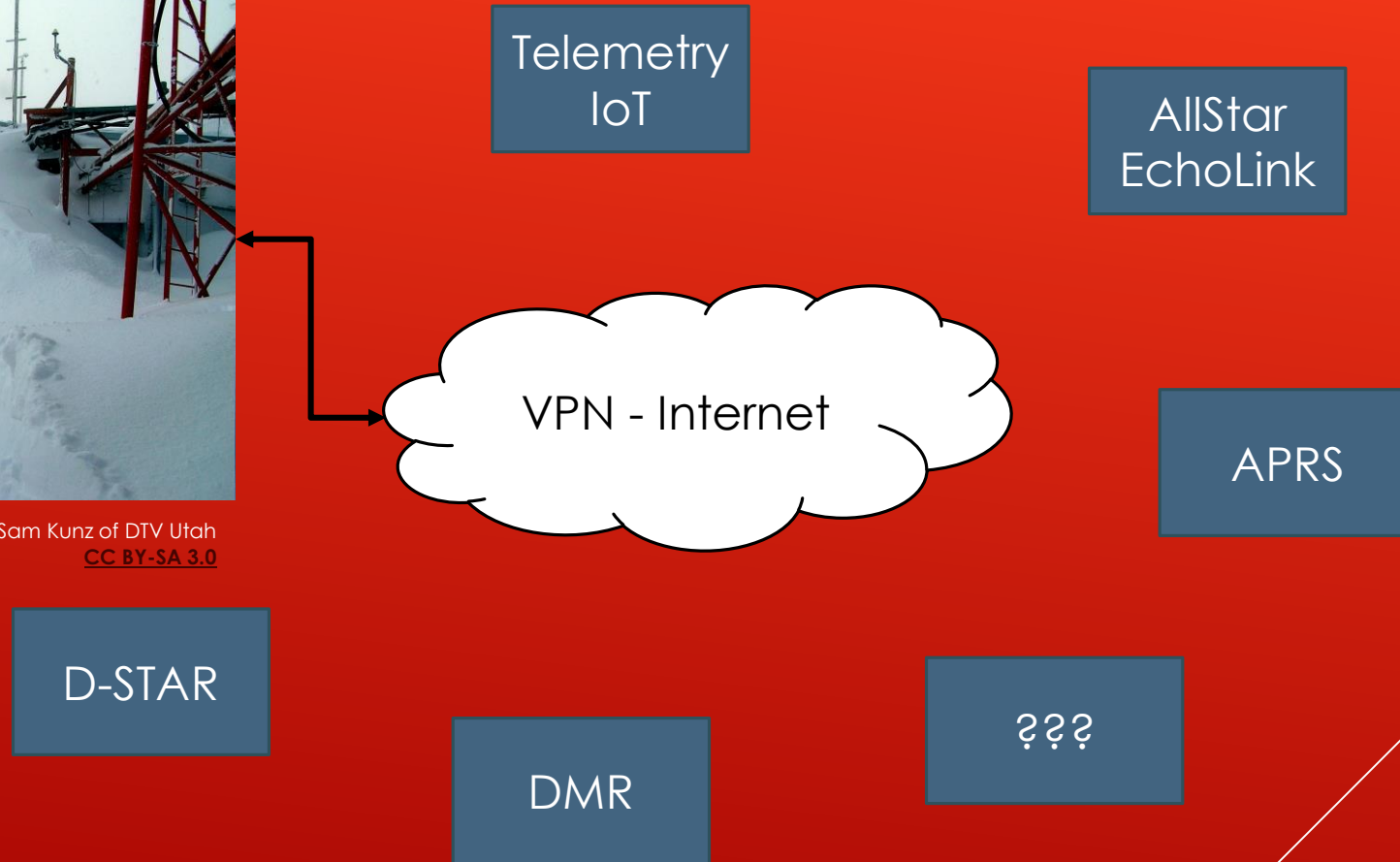


Applications

Repeater/Node/Gateway Site Linking with Static IP Addresses

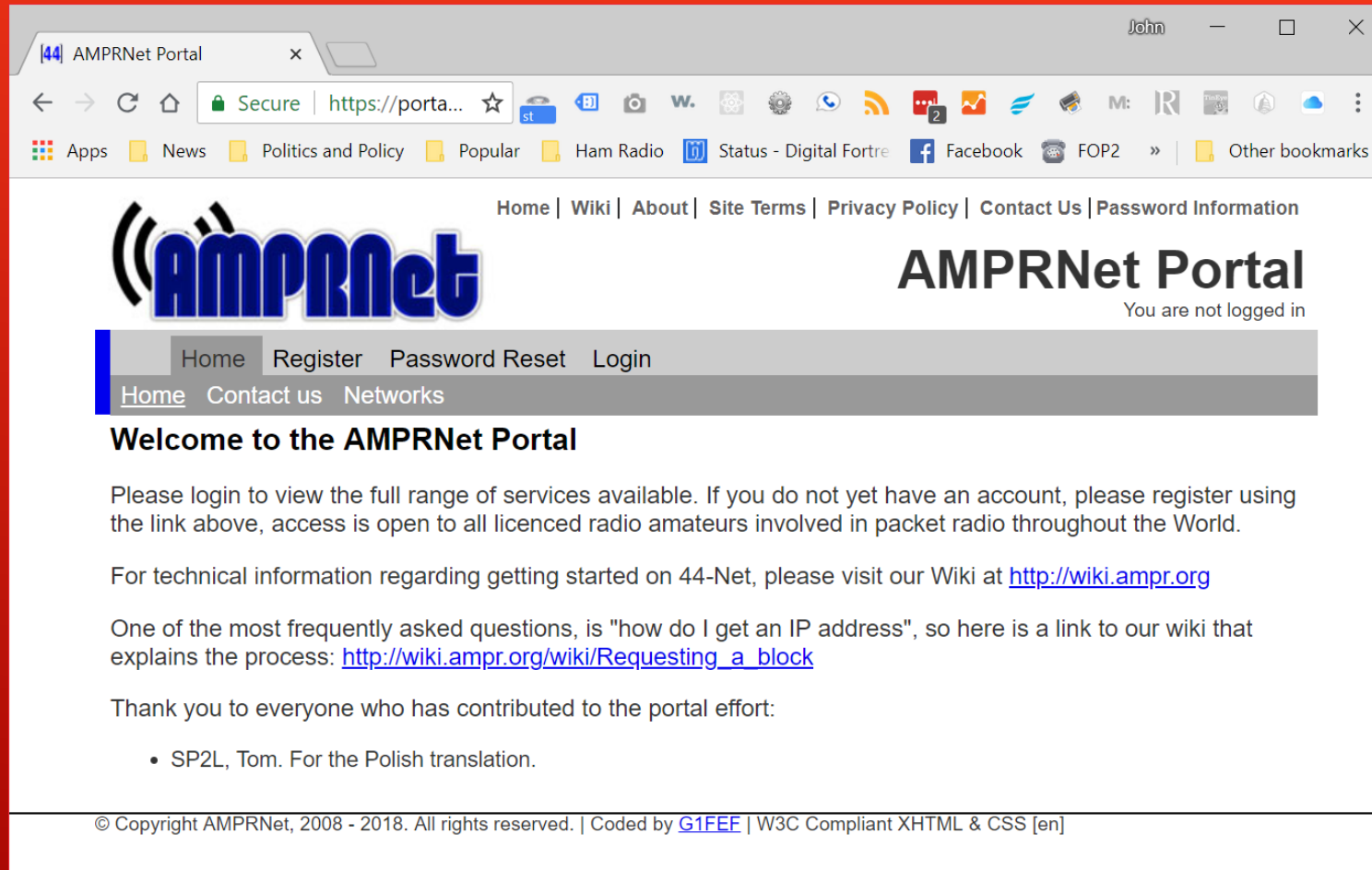


Farnsworth Peak - Photo by Sam Kunz of DTV Utah
[CC BY-SA 3.0](#)



Obtaining Net-44 Addresses

Create an account on <https://portal.ampr.org>

A screenshot of a web browser displaying the AMPRNet Portal. The browser's address bar shows "https://porta...". The page features a navigation menu with links like Home, Wiki, About, Site Terms, Privacy Policy, Contact Us, and Password Information. The AMPRNet logo is prominently displayed on the left, and the text "AMPRNet Portal" is on the right, with a note "You are not logged in". Below this is a secondary navigation bar with links for Home, Register, Password Reset, Login, Contact us, and Networks. The main content area welcomes users and provides instructions on how to log in or register, including a link to the wiki for technical information. A list of contributors is also shown, mentioning SP2L and Tom for a Polish translation. The footer contains copyright information for AMPRNet from 2008 to 2018 and credits the coding to G1FEF.

Obtaining Net-44 Addresses

[Home](#) [Register](#) [Password Reset](#) [Login](#)

Request a login

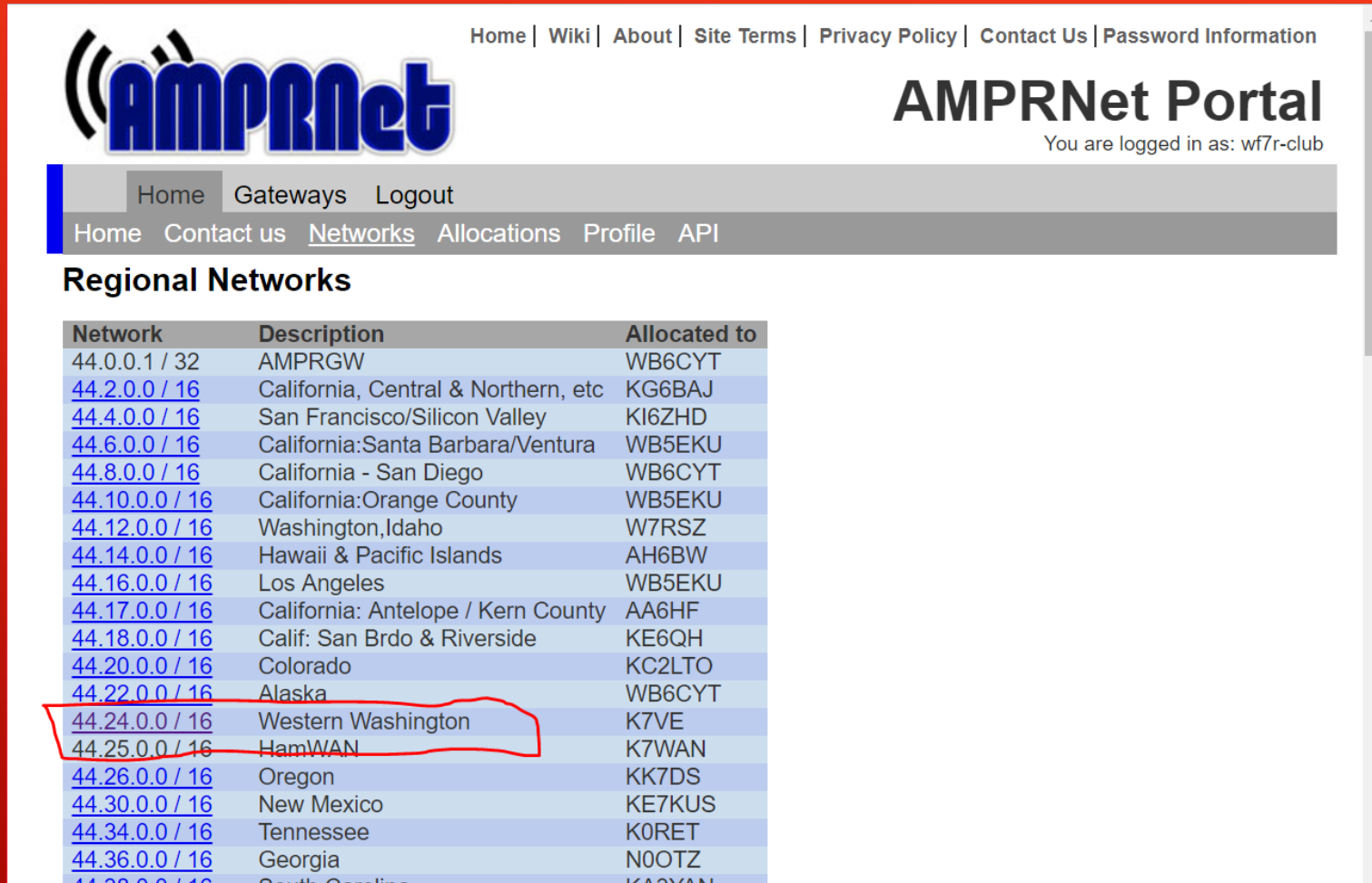
In order to access the portal, you first need to create an account. The first step is to provide us with your details on the form below. When you submit the form, the system will send you an email asking you to verify your email address, please follow the instructions provided in the email in order to continue with the registration process. We strongly advise that you add our email address info@ampr.org to your safe senders list / whitelist this will ensure that our emails are not blocked by your anti-spam software.

Required details

Callsign:	WF7R
Username:	wf7r-club
Password:	
Password:	
First name:	John
Surname:	Hays
Email:	john@hays.org
Organisation:	NW Digital Radio Club
Grid square:	CN87uu
Country:	UNITED STATES
Enter number:	
	
I agree:	☒ To the Terms and Conditions
Register	

Obtaining Net-44 Addresses

Select 'Networks' and navigate to your regional network



Home | Wiki | About | Site Terms | Privacy Policy | Contact Us | Password Information

AMPRNet Portal

You are logged in as: wf7r-club

Home Gateways Logout

Home Contact us Networks Allocations Profile API

Regional Networks

Network	Description	Allocated to
44.0.0.1 / 32	AMPRGW	WB6CYT
44.2.0.0 / 16	California, Central & Northern, etc	KG6BAJ
44.4.0.0 / 16	San Francisco/Silicon Valley	KI6ZHD
44.6.0.0 / 16	California: Santa Barbara/Ventura	WB5EKU
44.8.0.0 / 16	California - San Diego	WB6CYT
44.10.0.0 / 16	California: Orange County	WB5EKU
44.12.0.0 / 16	Washington, Idaho	W7RSZ
44.14.0.0 / 16	Hawaii & Pacific Islands	AH6BW
44.16.0.0 / 16	Los Angeles	WB5EKU
44.17.0.0 / 16	California: Antelope / Kern County	AA6HF
44.18.0.0 / 16	Calif: San Brdo & Riverside	KE6QH
44.20.0.0 / 16	Colorado	KC2LTO
44.22.0.0 / 16	Alaska	WB6CYT
44.24.0.0 / 16	Western Washington	K7VE
44.25.0.0 / 16	HamWAN	K7WAN
44.26.0.0 / 16	Oregon	KK7DS
44.30.0.0 / 16	New Mexico	KE7KUS
44.34.0.0 / 16	Tennessee	K0RET
44.36.0.0 / 16	Georgia	N0OTZ
44.38.0.0 / 16	South Carolina	K42VAN

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](#)

44.24.200.0 / 22	San Juan County KD7KAB	KD7KAB
44.24.221.0 / 24	HamWAN PSDR Anycast	K7WAN
44.24.240.0 / 20	HamWAN PSDR	K7WAN

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



Home | Wiki | About | Site Terms | Privacy Policy | Contact Us | Password Information

AMPRNet Portal

You are logged in as: wf7r-club

Home Gateways Logout

Home Contact us Networks Allocations Profile API

Request Allocation

Network Details

Parent network:

Netmask requested:

Description:

Type:

Connection Details

Radio: ☐

IPIP Tunnel: ☐

Direct (BGP): ☒

Accompanying notes

Notes:

This network will be used by NW Digital Radio Club for remote station operation, linking, VOIP, and websites....

Send

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 co-ordinator know by specifying the IP(s) in the "Notes" box. If this is a new request, the co-ordinator 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.

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.

Additional Information for Routing Net-44

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>

E3 KVM VIRTUAL SERVERS

E5 KVM VIRTUAL SERVERS

STORAGE SERVERS

20 GBPS DDOS PROTECTED (TCP)

SEATTLE E5 KVM VIRTUAL SERVERS

RAID 10 SSD

\$2.50 per month	\$5 per month	\$10 per month	\$15 per month
512MB Memory	1024MB Memory	2048MB Memory	3072MB Memory
10GB SSD Disk Space	15GB SSD Disk Space	30GB SSD Disk Space	45GB SSD Disk Space
1000GB Transfer @ 1Gb/s	2000GB Transfer @ 1Gb/s	3000GB Transfer @ 1Gb/s	3500GB Transfer @ 1Gb/s
1 vCore (3.0 GHz) Processor	2 vCore (3.0 GHz) Processor	2 vCore (3.0 GHz) Processor	3 vCore (3.0 GHz) Processor
1 IPv4 + /64 IPv6 Address	1 IPv4 + /64 IPv6 Address	1 IPv4 + /64 IPv6 Address	1 IPv4 + /64 IPv6 Address
ORDER NOW	ORDER NOW	ORDER NOW	ORDER NOW



Spartan Host Provisioning Example

1024MB SEABKVM
RAM: 1024MB CPU: 2 Cores IPv4: 1 Storage: 15GB Raid 10 SSD Bandwidth:
2000GB Port: 1Gb/s DDoS Protection: 20Gb/s TCP Location: Seattle,
Washington Control Panel: Virtualizor Managed: No

Choose Billing Cycle
1 Month Price - \$5.00 USD

Configure Server

Hostname
foo.k7ve.net

Configurable Options

Number of IPs
1

VirtIO
Enable

Virtual Network Type
VirtIO

Operating System
Ubuntu 16.04 64-bit

Location
Seattle, Washington

Additional Required Information

How did you find us?
Example

Order Summary
1024MB SEABKVM
DDoS Protected SSD E5 KVM VPS -
Seattle
1024MB SEABKVM \$5.00 USD
» Number of IPs: 1 \$0.00 USD
» VirtIO: Enable \$0.00 USD
» Virtual Network Type: VirtIO \$0.00 USD
» Operating System: Ubuntu 16.04 64-bit \$0.00 USD
» Location: Seattle, Washington \$0.00 USD
Setup Fees: \$0.00 USD
Monthly: \$5.00 USD
\$5.00 USD
Total Due Today
Continue

Select your plan and configure on next screen

I use Ubuntu 64-bit 16.04, select defaults on the rest

Review & Checkout

Product/Options	Price/Cycle
1024MB SEABKVM Edit	\$5.00 USD ×
DDoS Protected SSD E5 KVM VPS - Seattle foo.k7ve.net » Number of IPs: 1 » VirtIO: Enable » Virtual Network Type: VirtIO » Operating System: Ubuntu 16.04 64-bit » Location: Seattle, Washington	Monthly

Order Summary
Subtotal \$5.00 USD
Totals \$5.00 USD Monthly
\$5.00 USD
Total Due Today
Checkout
Continue Shopping

Empty Cart

Spartan Host Provisioning Example

Check out

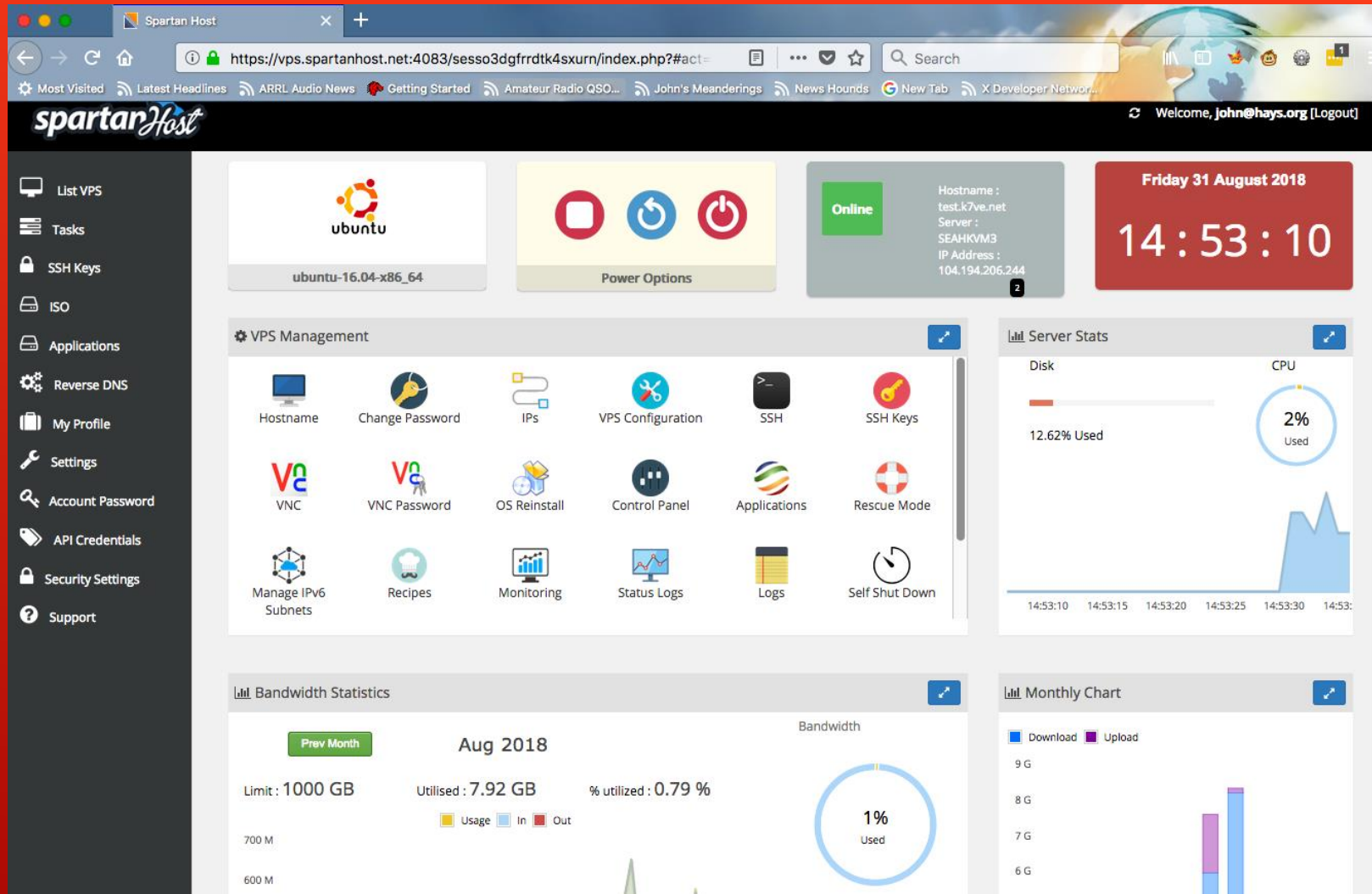
Shortly thereafter the host will be setup and ready to use.

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.

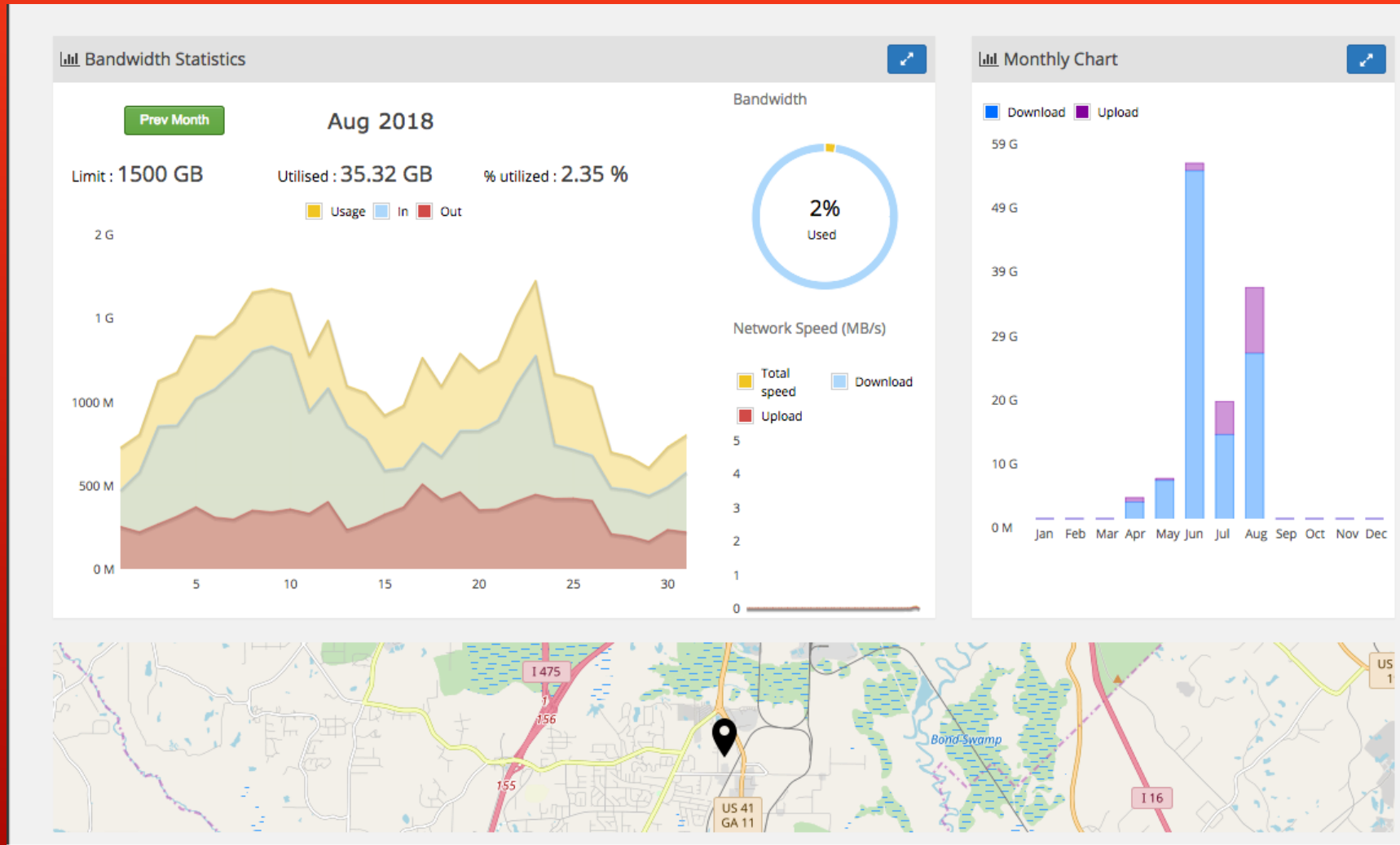


Google Authenticator

Spartan Host Provisioning Example (Control Panel)



Spartan Host Provisioning Example (Report)



Spartan Host Provisioning Example

ssh or **vnc** into your host

A screenshot of a macOS terminal window. The title bar shows the window name as 'john.h' and the current session as 'root@test: ~ — ssh root@test.k7ve.net — 100x25'. The terminal content shows a user at 'Johns-MacBook-Pro:~ john.h' running the command 'ssh root@test.k7ve.net'. The prompt then changes to 'root@test.k7ve.net's password:' followed by a password input icon (a circle with a question mark).

```
john.h — root@test: ~ — ssh root@test.k7ve.net — 100x25
[Johns-MacBook-Pro:~ john.h$ ssh root@test.k7ve.net
root@test.k7ve.net's password: ?
```

Update the VPS Server

See <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:

```
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**

Set Tunnel Value and Start OpenVPN

Define the Tunnel

Edit the file **/etc/openvpn/variables** it will contain two lines

```
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 it's status, and if OK, then enable it.

```
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.openvpn.tpl.new` which should be copied to `config.openvpn.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.openvpn.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 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.

```
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
```

Running OpenVPN on Clients

Startup Your Client

```
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



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 44.1.0.20 255.255.255.0
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::
```

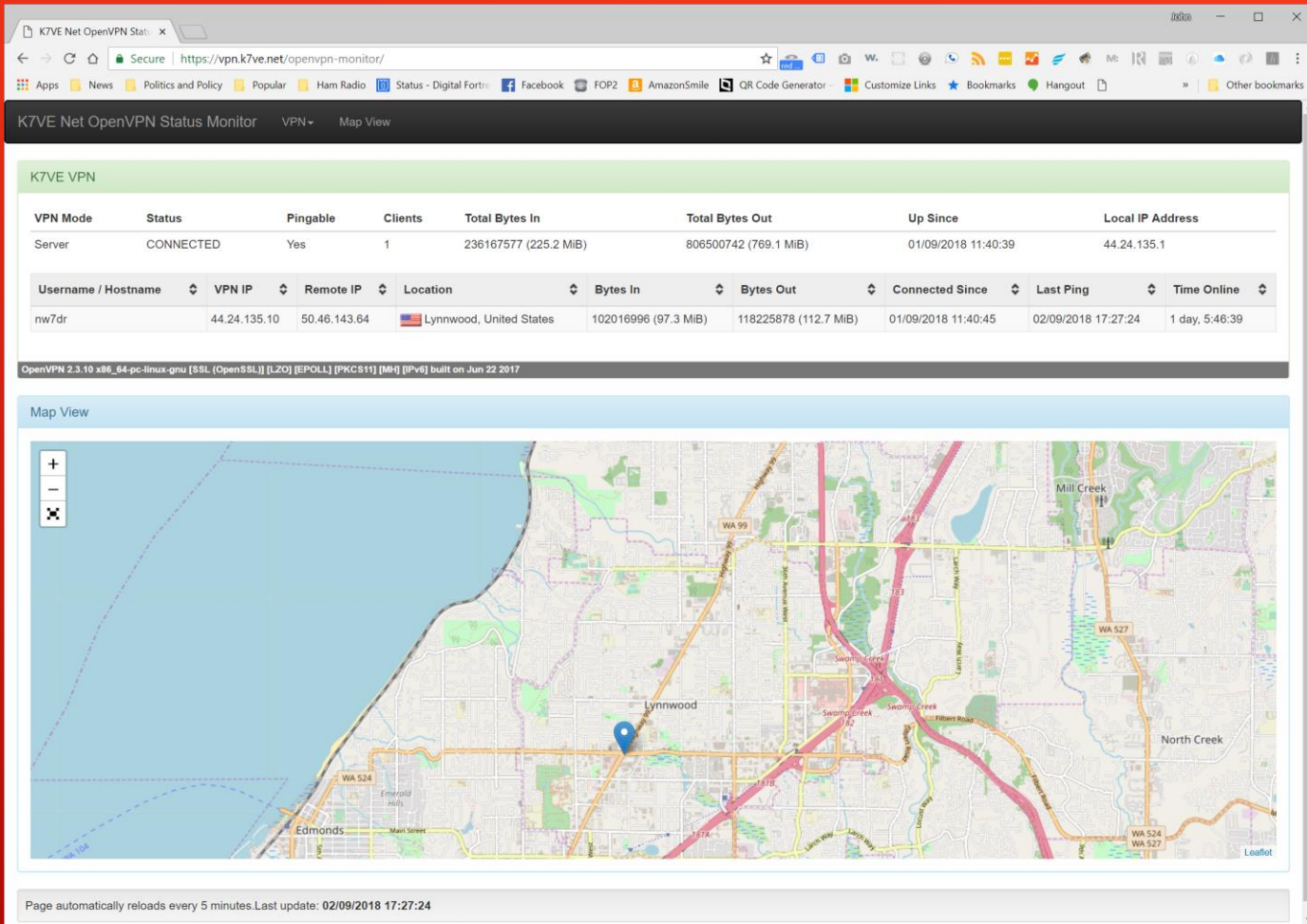
If your client doesn't pick up these values, restart the OpenVPN server, as root on your VPS:

systemctl restart openvpn@server

You can see the clients that logged in with:

cat /etc/openvpn/openvpn-status.log

Monitoring Connected Clients



K7VE Net OpenVPN Status Monitor

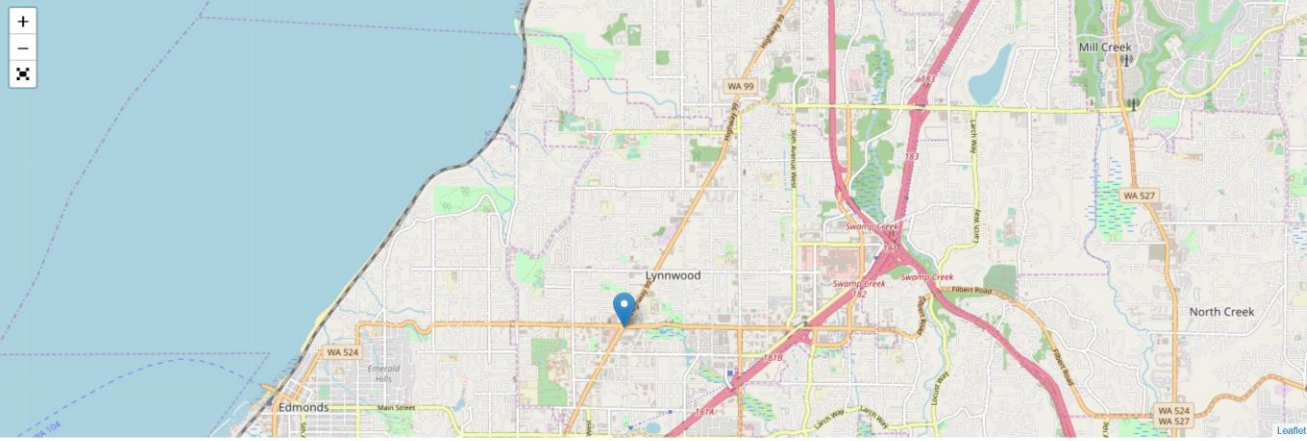
K7VE VPN

VPN Mode	Status	Pingable	Clients	Total Bytes In	Total Bytes Out	Up Since	Local IP Address
Server	CONNECTED	Yes	1	236167577 (225.2 MiB)	806500742 (769.1 MiB)	01/09/2018 11:40:39	44.24.135.1

Username / Hostname	VPN IP	Remote IP	Location	Bytes In	Bytes Out	Connected Since	Last Ping	Time Online
nw7dr	44.24.135.10	50.46.143.64	Lynnwood, United States	102016996 (97.3 MiB)	118225878 (112.7 MiB)	01/09/2018 11:40:45	02/09/2018 17:27:24	1 day, 5:46:39

OpenVPN 2.3.10 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH] [IPv6] built on Jun 22 2017

Map View



Page automatically reloads every 5 minutes. Last update: 02/09/2018 17:27:24

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>

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 useage 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>