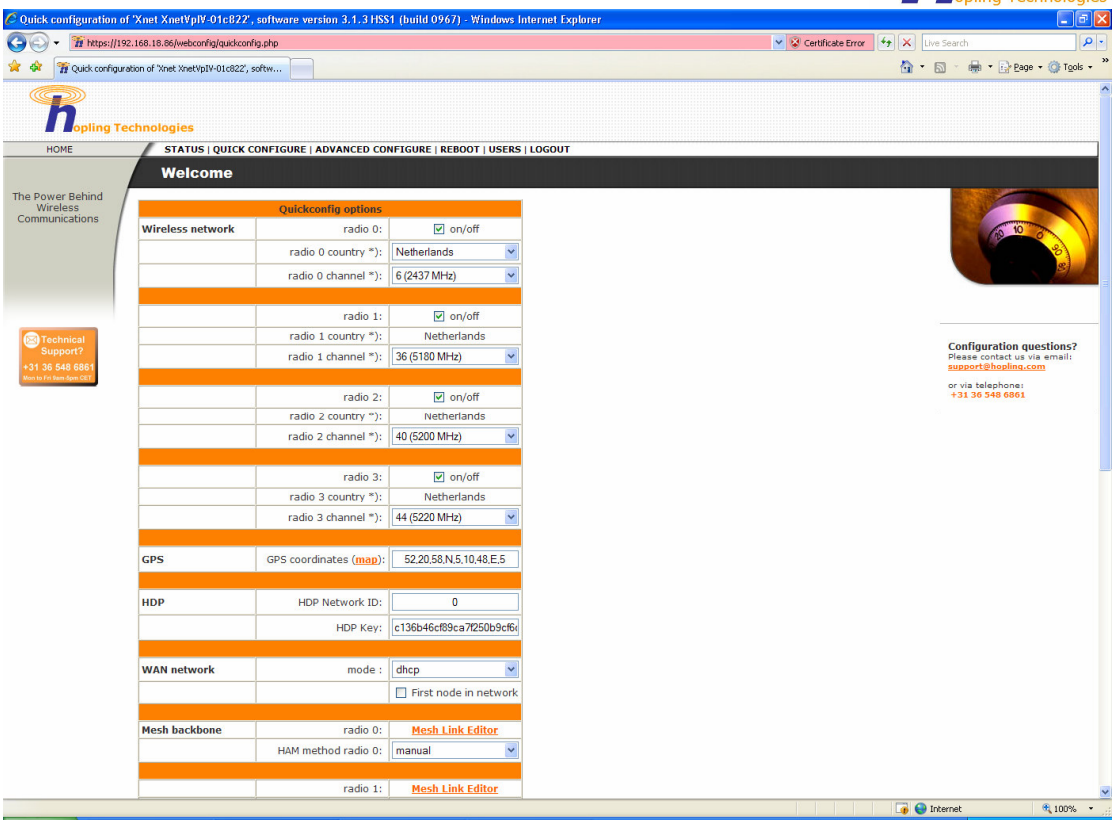


Figure 8, Quick Configuration screen of the Xnet Viper web interface

5.2 Console login via SSH

Connecting via SSH is usually a simple procedure, but requires some knowledge of how to configure the network settings of your desktop or laptop PC. When your Xnet Viper ships from Hopling technologies B.V., the unit has been configured to get an IP address from the local area network using DHCP. In order to log in to the Xnet Viper you can either connect using a wireless connection from a laptop or desktop or across the wired Ethernet network connection.

After configuring your PC to be able to contact the Xnet Viper, you can login using your favorite SSH client. SSH clients can be downloaded from for example http://www.ssh.com (OpenSSH) or http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html (PuTTY). In our examples the OpenSSH client will be used. Consult your SSH client documentation if you use a different SSH client.

SSH is used as the default network shell login protocol because it is a secure protocol, unlike the more commonly used Telnet. All communication between a client and server is encrypted before being sent over the network, thus packet **sniffers** are unable to extract usernames, passwords, and other potentially sensitive data. If you don't have an SSH client, a number of good free or low-cost options are available. For Unix, Linux, and Cygwin Windows environments, check out OpenSSH. For Windows consider PuTTY, an excellent free SSH client for all Win32 platforms.

To connect to your Xnet Viper for the first time using the OpenSSH client, start the client from the Windows START menu. Then press the enter key to open the "Connect to Remote Host" dialogue box. Enter the IP address, User Name (**root**) and port number (**22**) for the Xnet Viper in the dialogue box:

```
Host Name: 192.168.18.86
User Name: root
Port Number: 22
```

Then click the **`Quick Connect`** button

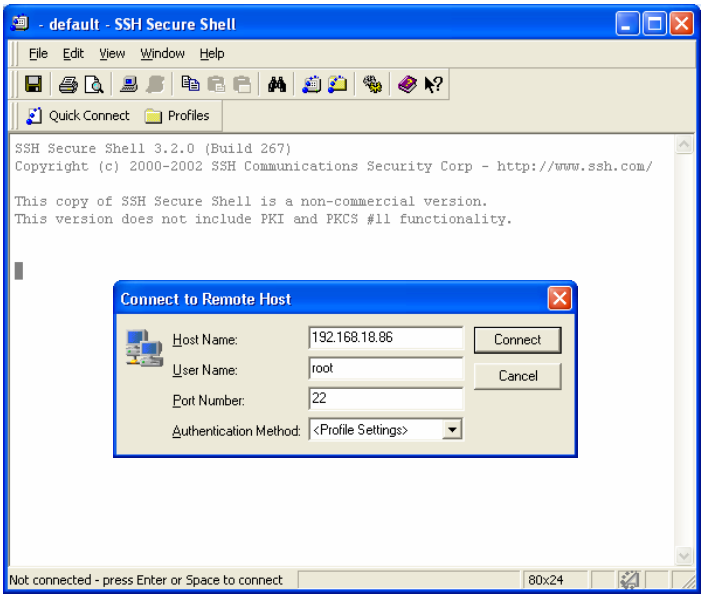


Figure 9, Logging in to the Xnet Viper using SSH Tool

You will be prompted to enter a password, which is provided to you by your reseller[1].

[1] The default password for user 'root' on the Xnet Viper is: **hoplingtech01**. It is strongly advised to change

After logging in, you may proceed to the directions for system configuration. The most relevant configuration files will be shown upon logging in. For example:

```
Welcome to Xnet: XnetVpIV-01c822
release  : 3.1.3-HSS1
released : Fri Apr 13 16:48:12 CEST 2007
buildnr  : 0967
buildtag : release

To make changes in configuration:
 - remount the file system read-write: remount rw
 - edit the Hopling configuration files:
   General file:
       /config/hopling/hopling.conf
   Specific files in directories:
       /config/hopling/virtual_gw/*
       /config/hopling/wifi_backbone/*
 - remount the file system read-only: remount ro
 - reboot: reboot
XnetVpIV-01c822:~$
```

5.3 Logging out

Before going further you should know how to log out of the system. At the shell prompt use the command `exit` to log out.
As an example,

```
XnetVpIV-01c822:~$ exit
```

to logout.

5.4 Changing your password

The Xnet Viper ships with the default password **`hoplingtech01`**. It is advisable to change this password when the system is installed. The command `passwd` will prompt you for your old password, and your new password. It will ask you to reenter the new password for validation. Before the password can be changed the file system needs to be writeable. This is done with the following command:

```
XnetVpIV-01c822:~$ remount rw
```

Then the password can be changed, as an example of a password dialogue:

```
XnetVpIV-01c822:~$ passwd
Changing password for root
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and numbers.
Enter new password:
Re-enter new password:

XnetVpIV-01c822:~$
```

When the password is successfully updated the file system needs to be set read only again. This is done with the following command:

```
XnetVpIV-01c822:~$ remount ro
```

---

this default password after installation of the system

6 Xnet Viper modes of operation

This section explains how to configure the Xnet Viper to fit into different network topologies. The Xnet Viper can be configured to operate the following networks:

- In Point-to-Point (PtP) systems with the Xnet Viper acting as transparent wireless bridge.
- In Point-to-Multi-Point (PtMP) systems with the Xnet Viper acting as WiFi Access Point.
- In Point-to-Multipoint (PtMp) systems as WiFi Access Point with integrated Hotspot Access controller.
- In Network Mesh systems with each Xnet Viper acting as Mesh router and Access Point.
- In Hotspot Mesh systems, with each Xnet Viper acting as Mesh router and Access Point with integrated Hotspot Access Controller.

7 Radio Configuration Parameters

This chapter describes the radio configuration parameters for the Xnet Viper. A number of configuration parameters are set system wide. Examples of system wide configuration parameters are WiFi channel(s), SSIDs, Encryption types and Regulatory Domain.

7.1 2.4GHz and 5GHz Channel planning

Both the 2.4GHz and the 5GHz frequency bands are unlicensed bands and are subject to local rules and regulations. Below are some considerations that need to be taken into account when planning 2.4GHz and 5GHz outdoor networks using Xnet Viper routers.

7.1.1 2.4GHz channel overlap considerations

The 802.11b standard defines 14 frequency channels in the 2.4GHz range, but only eleven are allowed for unlicensed use by the FCC in the US, thirteen in Canada and thirteen in Europe. Each channel uses "Direct Sequence Spread Spectrum" (DSSS) to spread the data over the channel that extends 11MHz on each side of the center frequency, and the channels overlap. The figure below depicts the center frequency of each channel and the overlap each channel has with its neighbors.

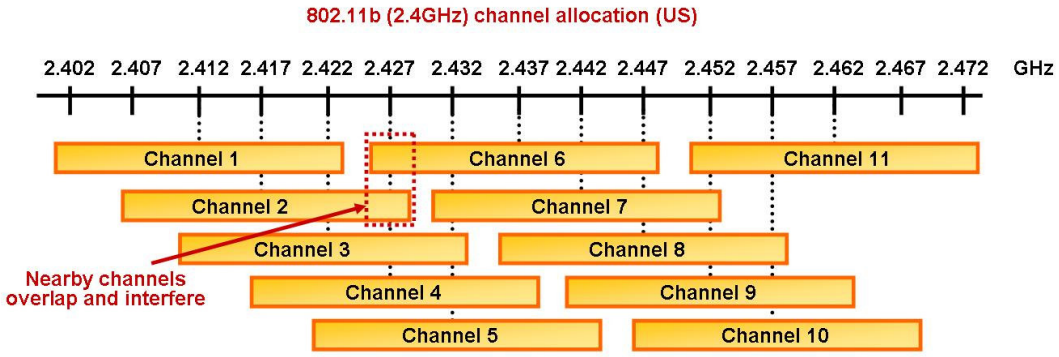


Figure 10: 2.4GHz channel allocation

To the extent that channels overlap, they interfere with each other and reduce available bandwidth for the access points. For Hopling Xnet Viper multi radio systems that are forming a mesh network using the 5GHz band as back bone the 2.4GHz access points need to be tuned to non-overlapping frequencies. A typical channel plan is shown below.

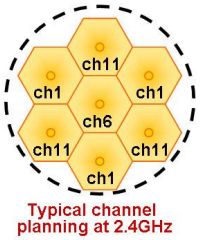


Figure 11: Typical channel planning at 2.4GHz

7.1.2 5GHz radar, satellite interference considerations

The 802.11a standard defines 12 non-overlapping channels (5.15 - 5.35GHz, 5.725 - 5.825GHz) in the 5GHz band. Recently the FCC added additional channels in the middle band (5.470-5.725 GHz). Some of the channels in the 5GHz band are in use by radar, satellite and other sensitive broadcasts. This requires the use of Dynamic Frequency Selection (DFS) on these frequencies. DFS checks for the presence of protected communications equipment and prevents interference.

7.1.3 Configuration of WiFi Channel on Xnet Viper-I

The channel settings for the Xnet Viper-I are held in the file:
`/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0.general.conf`

To change the channel of the Xnet Viper-I network edit the **`WIFI_0_CHANNEL`** parameter in the file. The parameter can be the frequency in MHz or the channel number.

As an example,

```
#@! <upload> <config> <reserved2> <reserved3> <reserved4>
#@$ <"Virtual Gateway 0: General Wifi parameters for radio 0">
#
# file: /config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0.general.conf
#
# Author: Bas Muns
# (c) Hopling Technologies 2005, 2006
#
# General configuration file for wireless WiFi interface.
#
# This file is specific for the Atheros hardware.

#@$ <"Wifi internal info">
#@@ <WIFI_0_HW>            <STRING>    <0,128>  <READ_ONLY>   <RESERVED>   <"Wifi
HW type. Please do not change this yourself">
#@@ <WIFI_0_PHYS>          <STRING>    <0,128>  <READ_ONLY>   <RESERVED>   <"Wifi
HW physical iface name. Please do not change this yourself">

WIFI_0_HW="ath"
WIFI_0_PHYS="wifi0"

#@$ <"General wifi parameters">
#@@ <WIFI_0_CHANNEL>         <INT>       <0,10000>         <NONE>   <RESERVED>
<"Frequency (in MHz) or Channel. Please use quick configuration webinterface when
you don't know what to fill in here">
#@@ <WIFI_0_MODE>            <DROPDOWN>  <master,ad-hoc>   <NONE>   <RESERVED>
<"Expert setting. Leave this set to master! Should only be changed when asked so by
Hopling">
#@@ <WIFI_0_COUNTRY>         <STRING>    <0,10>            <NONE>   <RESERVED>
<"Country where this device is installed. Please use quick config on the web
interface to change this value. See wifi0.countrylist.conf for a list of available
countries for this device">
#@@ <WIFI_0_LOCATION>        <DROPDOWN>  <indoor,outdoor>  <NONE>   <RESERVED>
<"Specify if the unit is used indoor or outdoor">
#@@ <WIFI_0_DISTANCE>        <INT>       <300,20000>       <NONE>   <RESERVED>
<"Specify the distance in meters of the longest link. Distance shorter that 300
meters should not be specified.">
#@@ <WIFI_0_RATECTRL>        <STRING>    <0,30>    <READ_ONLY>   <RESERVED>  <"Rate
control algorithm to use currently sample, amrr">

WIFI_0_CHANNEL="6"
WIFI_0_MODE="master"
WIFI_0_COUNTRY="NL"
WIFI_0_LOCATION="indoor"
WIFI_0_DISTANCE="300"
WIFI_0_RATECTRL="sample"
# End
```

7.1.4 Configuration of WiFi Channels on Xnet Viper-II

The channel settings for the Xnet Viper-II are held in two files, one for each radio.

Radio 0:
`/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0.general.conf`

To change the channel of the first radio in the Xnet Viper-II network edit the **`WIFI_0_CHANNEL`** parameter in the file. The parameter can be the frequency in MHz or the channel number.

As an example,

```
#@! <upload> <config> <reserved2> <reserved3> <reserved4>
#@$ <"Virtual Gateway 0: General Wifi parameters for radio 0">
#
# file: /config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0.general.conf
#
# Author: Bas Muns
# (c) Hopling Technologies 2005, 2006
#
# General configuration file for wireless WiFi interface.
#
# This file is specific for the Atheros hardware.

#@$ <"Wifi internal info">
#@@ <WIFI_0_HW>             <STRING>    <0,128>  <READ_ONLY>   <RESERVED>   <"Wifi
HW type. Please do not change this yourself">
#@@ <WIFI_0_PHYS>           <STRING>    <0,128>  <READ_ONLY>   <RESERVED>   <"Wifi
HW physical iface name. Please do not change this yourself">

WIFI_0_HW="ath"
WIFI_0_PHYS="wifi0"

#@$ <"General wifi parameters">
#@@ <WIFI_0_CHANNEL>          <INT>       <0,10000>         <NONE>   <RESERVED>
<"Frequency (in MHz) or Channel. Please use quick configuration webinterface when
you don't know what to fill in here">
#@@ <WIFI_0_MODE>             <DROPDOWN>  <master,ad-hoc>   <NONE>   <RESERVED>
<"Expert setting. Leave this set to master! Should only be changed when asked so by
Hopling">
#@@ <WIFI_0_COUNTRY>          <STRING>    <0,10>            <NONE>   <RESERVED>
<"Country where this device is installed. Please use quick config on the web
interface to change this value. See wifi0.countrylist.conf for a list of available
countries for this device">
#@@ <WIFI_0_LOCATION>         <DROPDOWN>  <indoor,outdoor>  <NONE>   <RESERVED>
<"Specify if the unit is used indoor or outdoor">
#@@ <WIFI_0_DISTANCE>         <INT>       <300,20000>       <NONE>   <RESERVED>
<"Specify the distance in meters of the longest link. Distance shorter that 300
meters should not be specified.">
#@@ <WIFI_0_RATECTRL>         <STRING>    <0,30>    <READ_ONLY>   <RESERVED>  <"Rate
control algorithm to use currently sample, amrr">

WIFI_0_CHANNEL="6"
WIFI_0_MODE="master"
WIFI_0_COUNTRY="NL"
WIFI_0_LOCATION="indoor"
WIFI_0_DISTANCE="300"
WIFI_0_RATECTRL="sample"
# End
```

Radio 1:
/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_1.general.conf

To change the channel of the second radio in the Xnet Viper-II edit the **WIFI_1_CHANNEL** parameter in the file. The parameter can be the frequency in MHz or the channel number.

As an example,

```
#@! <upload> <config> <reserved2> <reserved3> <reserved4>
#@$ <"Virtual Gateway 0: General Wifi parameters for radio 1">
#
# file: /config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_1.general.conf
#
# Author: Bas Muns
# (c) Hopling Technologies 2005, 2006
#
# General configuration file for wireless WiFi interface.
#
# This file is specific for the Atheros hardware.

#@$ <"Wifi internal info">
#@@ <WIFI_1_HW>            <STRING>    <0,128>  <READ_ONLY>   <RESERVED>   <"Wifi
HW type. Please do not change this yourself">
#@@ <WIFI_1_PHYS>          <STRING>    <0,128>  <READ_ONLY>   <RESERVED>   <"Wifi
HW physical iface name. Please do not change this yourself">

WIFI_1_HW="ath"
WIFI_1_PHYS="wifi1"

#@$ <"General wifi parameters">
#@@ <WIFI_1_CHANNEL>          <INT>       <0,10000>         <NONE>   <RESERVED>
<"Frequency (in MHz) or Channel. Please use quick configuration webinterface when
you don't know what to fill in here">
#@@ <WIFI_1_MODE>             <DROPDOWN>  <master,ad-hoc>   <NONE>   <RESERVED>
<"Expert setting. Leave this set to master! Should only be changed when asked so by
Hopling">
#@@ <WIFI_1_COUNTRY>          <STRING>    <0,10>            <NONE>   <RESERVED>
<"Country where this device is installed. Please use quick config on the web
interface to change this value. See wifi0.countrylist.conf for a list of available
countries for this device">
#@@ <WIFI_1_LOCATION>         <DROPDOWN>  <indoor,outdoor>  <NONE>   <RESERVED>
<"Specify if the unit is used indoor or outdoor">
#@@ <WIFI_1_DISTANCE>         <INT>       <300,20000>       <NONE>   <RESERVED>
<"Specify the distance in meters of the longest link. Distance shorter that 300
meters should not be specified.">
#@@ <WIFI_1_RATECTRL>         <STRING>    <0,30>    <READ_ONLY>   <RESERVED>  <"Rate
control algorithm to use currently sample, amrr">

WIFI_1_CHANNEL="36"
WIFI_1_MODE="master"
WIFI_1_COUNTRY="NL"
WIFI_1_LOCATION="indoor"
WIFI_1_DISTANCE="300"
WIFI_1_RATECTRL="sample"
# End

#
# file: /config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_1.general.conf
#
# Author: Bas Muns
# (c) 2005 Hopling Technologies
#
# General configuration file for wireless WiFi interface.
#
# This file is specific for the Atheros hardware.
# Do not change this!
WIFI_1_HW="ath"
```

7.1.5 Canada: outdoor 2.4GHz

Country	Frequencies	EIRP (mW)	EIRP (dBm)	DFS	Channels
Canada	2412-2472	100	20	No	1 2 3 4 5 6 7 8 9 10 11 12 13

7.1.6 Canada: indoor 5GHz

Country	Frequencies	EIRP (mW)	EIRP (dBm)	DFS	Channels
Canada	5150-5250	200	23	No	36 40 44 48

7.1.7 Canada: outdoor 5GHz

Country	Frequencies	EIRP (mW)	EIRP (dBm)	DFS	Channels
Canada	5150-5250	200	23	No	36 40 44 48
Canada	5250-5350	250	24	No	52 56 60 64
Canada	5725-5850	1000	30	No	149 153 157 161 165
Canada	5725-5825	1000	30	No	149 153 157 161 165
Canada	5725-5825	4000	36	No	149 153 157 161 165
Canada	5250-5350	1000	30	Yes	52 56 60 64
Canada	5470-5725	1000	30	Yes	100 104 108 112 116 120 124 128 132 136 140
Canada	5725-5850	4000	36	No	149 153 157 161 165

7.1.8 United States: outdoor 2.4GHz

Country	Frequencies	EIRP (mW)	EIRP (dBm)	DFS	Channels
United States	2412-2462	1000	30	No	1 2 3 4 5 6 7 8 9 10 11

For 2.4GHz outdoor operation in the United States it is advised to use channel 1, 6 and 11 to minimize co-channel interference.

7.1.9 United States: indoor 5GHz

Country	Frequencies	EIRP (mW)	EIRP (dBm)	DFS	Channels
United States	5180-5240	40	16	No	36 40 44 48

7.1.10 United States: outdoor 5GHz

Country	Frequencies	EIRP (mW)	EIRP (dBm)	DFS	Channels
US	5250-5350	250	24	Yes	52 56 60 64
US	5725-5850	1000	30	No	149 153 157 161 165
US	5470-5725	1000	30	Yes	100 104 108 112 116 120 124 128 132 136 140
US	5250-5350	1000	30	Yes	52 56 60 64
US	5725-5850	4000	36	No	149 153 157 161 165
US DSRC/WAVE	5850-5925	2000	33	No	172 174 176 178 180 182 184
US DSRC/WAVE		200	23	No	181

For 5GHz outdoor operation in the United States channels 149 to 165 will predominantly be used due to the largest output power regime and no use of DFS required. However, in case more channels are required, or in case the channels are already in use by another operator, then the additional channels can be used albeit using slightly lower output power and the requirement for DFS.

7.2 Setting Regulatory Domain or Country Code

When 802.11 first became available, only a handful of regulatory domains (e.g., U.S., Europe, and Japan) had rules in place for the operation of 802.11 wireless LANs. In order to support a widespread adoption of 802.11, the 802.11d task group has an ongoing charter to define PHY requirements that satisfy regulatory within additional countries. This is especially important for operation in the 5GHz bands because the use of these frequencies differ widely from one country to another. It is therefore important to set the correct regulatory domain or country code prior to using the Xnet Viper system.

7.2.1 Setting Regulatory Domain through Command Line Interface

Viper-I, one radio system
The regulatory domain (country) settings for the Xnet Viper-I are held in the file:
`/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0.general.conf`

And the parameter: **`WIFI_0_COUNTRY="NL"`** defines what country is being used. In this example the county is set to the Netherlands.

A list of valid country codes can be obtained from the file:
`/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0.countrylist.conf`

Viper-II, two radio system
The regulatory domain (country) settings for the Xnet Viper-II are held two files:
`/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0.general.conf`
`/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_1.general.conf`

The parameter: **`WIFI_0_COUNTRY="NL"`** defines what country is being used for the first radio.
The parameter: **`WIFI_1_COUNTRY="NL"`** defines what country is being used for the second radio.

A list of valid country codes for the first radio can be obtained from the file:
`/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0.countrylist.conf`

A list of valid country codes for the second radio can be obtained from the file:
`/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_1.countrylist.conf`

! NOTE ! Please select country and channels which are allowed by your local regulatory authority. Hopling Technologies B.V. can not be held responsible for illegal configurations. In case of questions please contact your local regulatory authority.

7.2.2 Setting Regulatory Domain through Web Interface

If you are unsure how to set the WiFi channel in accordance to your regulatory domain please use the web interface of the Xnet Viper router instead of the command line interface. The web interface will correctly show a list of available channels according to the selected regulatory domain (country code).

The country code can be selected by clicking on the **`radio country`** list box. When another country is selected the quick configuration screen will refresh to load the new channels that are available for that country. The page will take a few seconds to reload because the system is retrieving the available frequencies from the radio hardware.

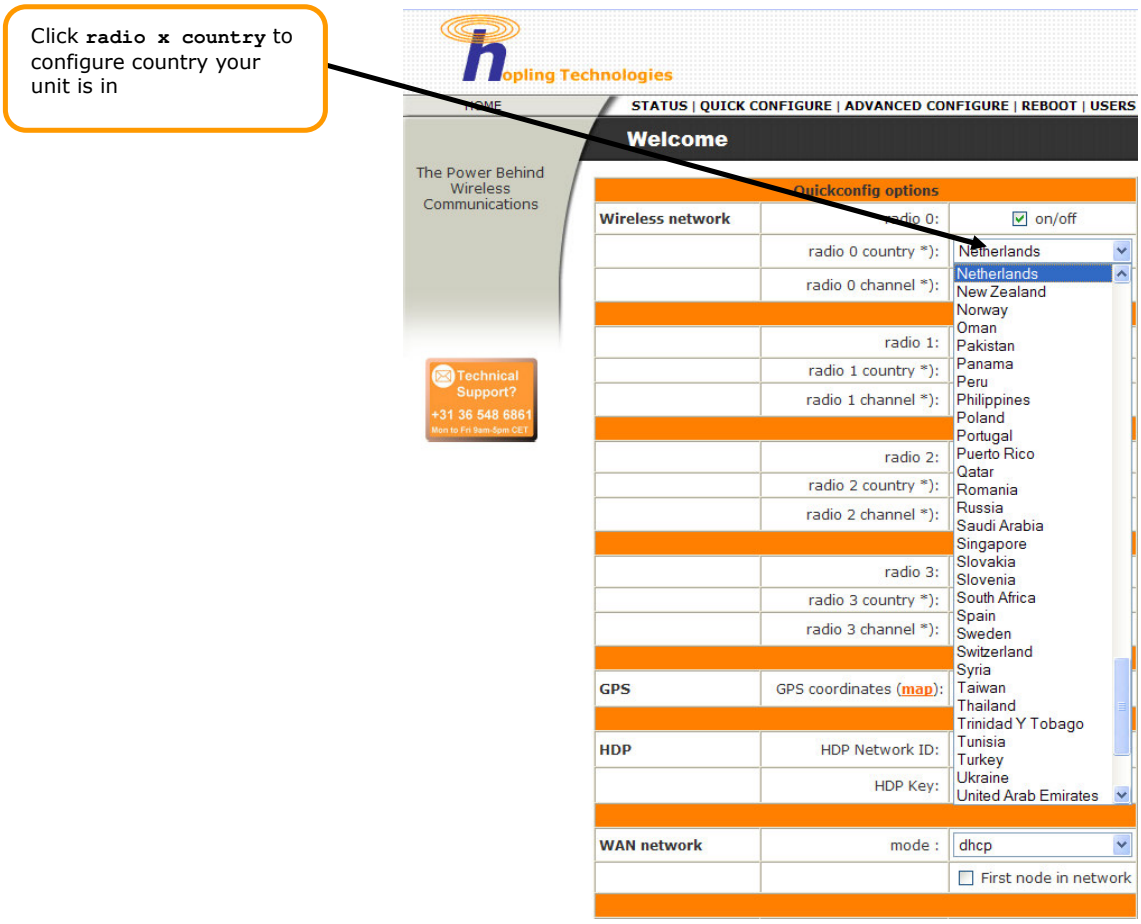


Figure 12: Select country to configure the Xnet Viper.

Please select country and channels which are allowed by your local regulatory authority. Hopling Technologies B.V. can not be held responsible for illegal configurations. In case of questions please contact your local regulatory authority.

8 Mesh Networking Configuration Parameters

In order for the Xnet Viper nodes to communicate to neighboring nodes the mesh links to each neighbor need to be configured. In Xnet systems running Hopware version 3.0.x or earlier this configuration can only be done manually. This is achieved by entering the MAC address of the wireless neighboring node into the neighbor MAC address list on the Xnet Viper router.

Fully automatic mesh configuration was introduced in HopWARE version 3.1.1. and higher. Xnet Viper series nodes come installed with HopWARE version 3.1.x or higher and have this feature enabled as default. Xnet Mark-I and Xnet Mark-II units can be upgraded to the same HopWARE version as the Xnet Viper units to give fully automatic mesh configuration across different platforms.

An Xnet Viper supports up to up to 10 mesh links to different neighbors per radio.

8.1.1 Manual Configuring Mesh Links through Command Line Interface

The default configuration of the Xnet Viper only allows other Xnet Vipers to connect to the network when their MAC addresses are listed in the following files:

For one radio system:

```
/config/hopling/wifi_backbone/wifi_backbone_0/neighbors_0.conf
```

For a multiple radio system:

```
/config/hopling/wifi_backbone/wifi_backbone_0/neighbors_0.conf
/config/hopling/wifi_backbone/wifi_backbone_1/neighbors_1.conf
```

To add a Mesh Link the neighbors file needs to be edited to include the neighboring nodes. Every node you wish to add must have an entry in the file.

As an example,

```
#@! <upload> <config> <reserved2> <reserved3> <reserved4>
#@$ <"Neighboring nodes for radio 0">
#
# file: /config/hopling/wifi_backbone/wifi_backbone_0/neighbors_0.conf
#
# (c) Hopling Technologies 2005, 2006
# Ivo van Ling (support@hopling.com)
#
# MAC address control list for neigboring nodes
# with a maximum of 10 connections to other Hopling nodes
#

#@$ <"Parameters for Hopling Auto Mesh for radio 0">
#@@ <NEIGHBOR_0_HAM_METHOD>        <DROPDOWN>  <manual,auto>   <NONE>   <RESERVED>
<"Hopling Auto Meshing method for radio 0">

NEIGHBOR_0_HAM_METHOD="manual"

#@$ <"List of neighboring nodes for radio 0">
#@@ <NEIGHBOR_0_0>        <MAC>    <1>      <NONE>   <RESERVED>  <"MAC address of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_0_LOC>    <STRING> <0,128>  <NONE>   <RESERVED>  <"Location of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_1>        <MAC>    <1>      <NONE>   <RESERVED>  <"MAC address of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_1_LOC>    <STRING> <0,128>  <NONE>   <RESERVED>  <"Location of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_2>        <MAC>    <1>      <NONE>   <RESERVED>  <"MAC address of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_2_LOC>    <STRING> <0,128>  <NONE>   <RESERVED>  <"Location of
neighboring node to mesh with">
```

```
#@@ <NEIGHBOR_0_3>        <MAC>    <1>      <NONE>   <RESERVED>  <"MAC address of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_3_LOC>    <STRING> <0,128>  <NONE>   <RESERVED>  <"Location of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_4>        <MAC>    <1>      <NONE>   <RESERVED>  <"MAC address of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_4_LOC>    <STRING> <0,128>  <NONE>   <RESERVED>  <"Location of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_5>        <MAC>    <1>      <NONE>   <RESERVED>  <"MAC address of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_5_LOC>    <STRING> <0,128>  <NONE>   <RESERVED>  <"Location of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_6>        <MAC>    <1>      <NONE>   <RESERVED>  <"MAC address of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_6_LOC>    <STRING> <0,128>  <NONE>   <RESERVED>  <"Location of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_7>        <MAC>    <1>      <NONE>   <RESERVED>  <"MAC address of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_7_LOC>    <STRING> <0,128>  <NONE>   <RESERVED>  <"Location of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_8>        <MAC>    <1>      <NONE>   <RESERVED>  <"MAC address of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_8_LOC>    <STRING> <0,128>  <NONE>   <RESERVED>  <"Location of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_9>        <MAC>    <1>      <NONE>   <RESERVED>  <"MAC address of
neighboring node to mesh with">
#@@ <NEIGHBOR_0_9_LOC>    <STRING> <0,128>  <NONE>   <RESERVED>  <"Location of
neighboring node to mesh with">

NEIGHBOR_0_0="00:11:22:33:44:55"
NEIGHBOR_0_0_LOC="Tower_1_rooftop"
NEIGHBOR_0_1="00:22:33:44:55:66"
NEIGHBOR_0_1_LOC="Tower_2_rooftop"
NEIGHBOR_0_2="00:00:00:00:00:00"
NEIGHBOR_0_2_LOC=""
NEIGHBOR_0_3="00:00:00:00:00:00"
NEIGHBOR_0_3_LOC=""
NEIGHBOR_0_4="00:00:00:00:00:00"
NEIGHBOR_0_4_LOC=""
NEIGHBOR_0_5="00:00:00:00:00:00"
NEIGHBOR_0_5_LOC=""
NEIGHBOR_0_6="00:00:00:00:00:00"
NEIGHBOR_0_6_LOC=""
NEIGHBOR_0_7="00:00:00:00:00:00"
NEIGHBOR_0_7_LOC=""
NEIGHBOR_0_8="00:00:00:00:00:00"
NEIGHBOR_0_8_LOC=""
NEIGHBOR_0_9="00:00:00:00:00:00"
NEIGHBOR_0_9_LOC=""

# End
```

After making changes to the file you can make the changes take effect by typing `reboot` at the command prompt. This will reboot the system upon which the new configuration files will be read and executed.

8.1.2 Manually Configuring Mesh Links through Web Interface

The MAC addresses of the radio units in the Xnet Viper can be found on the **`status`** page. Generally the first radio interface (WLAN Interface 0) will be the 2.4GHz radio and the second radio interface (WLAN Interface 1) will be the 5GHz radio.

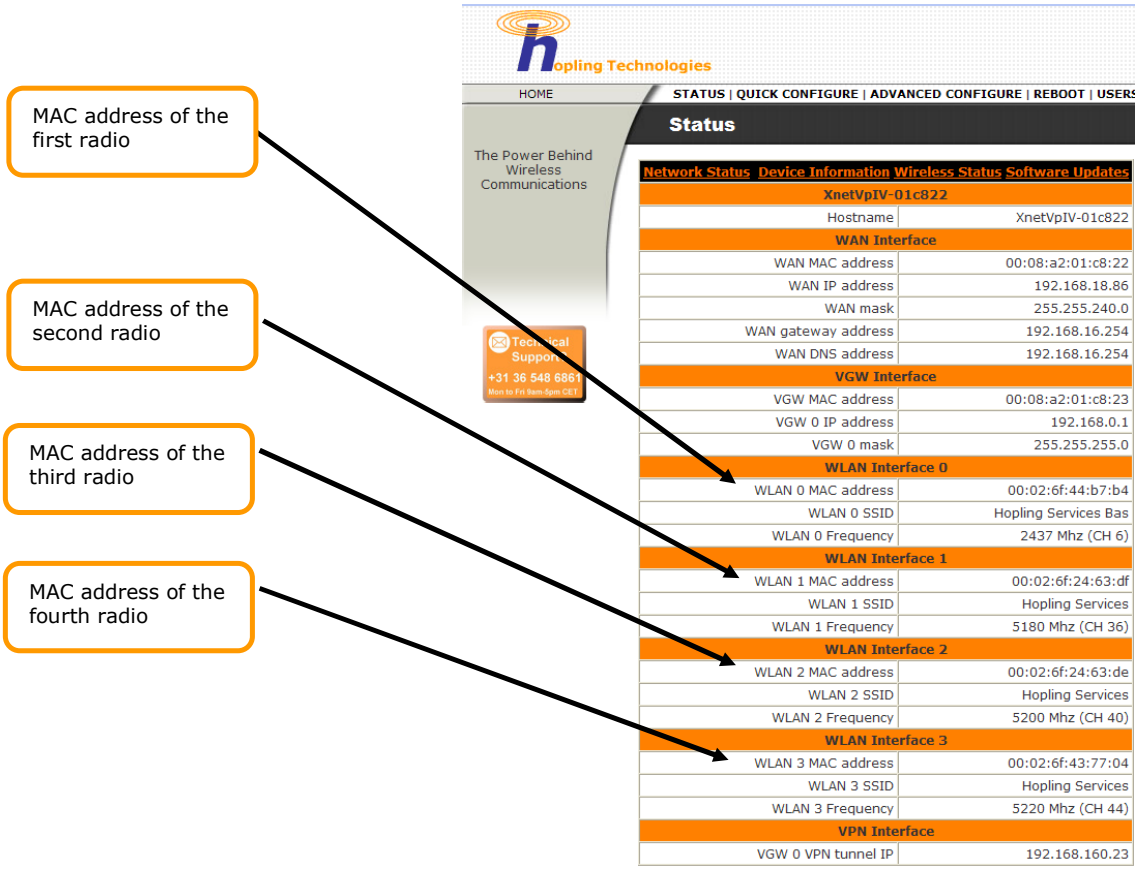


Figure 13: Finding the MAC addresses of the installed WiFi interfaces

Neighboring mesh nodes can be added by clicking on the Mesh Link Editor for the corresponding radio in the **QUICK CONFIGURATION** page.

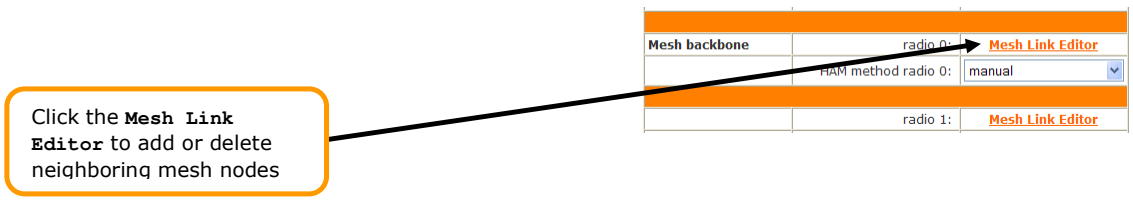


Figure 14: Click the Mesh Link Editor to add or delete mesh nodes

When the **`Mesh Link Editor`** for a radio is clicked the mesh link editor is shown. You can add a maximum of 10 MAC addresses of neighboring devices in the configuration page. Together with the MAC address of it is possible to enter the location of the neighboring device. This can be a description of the location or the GPS coordinates of the location.

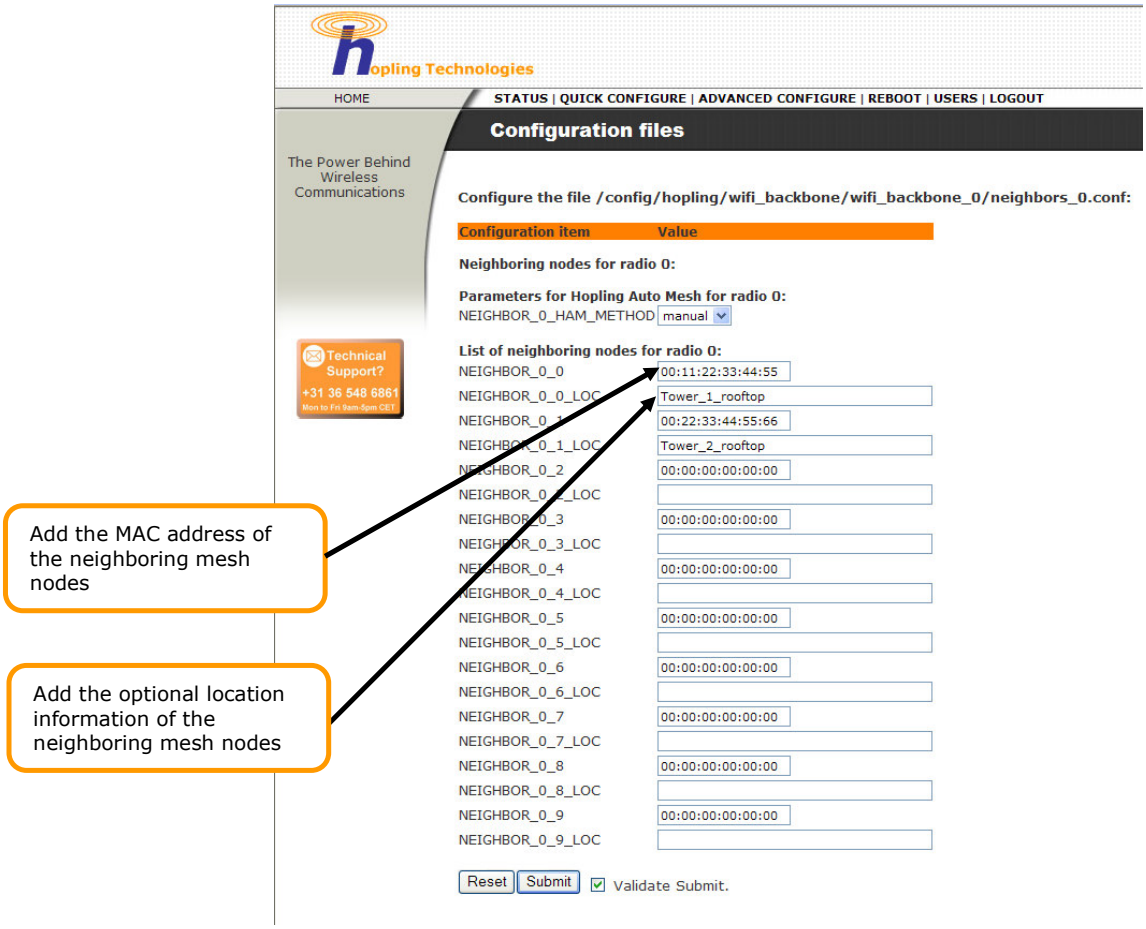
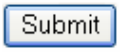


Figure 15: Mesh Link Editor

Click the  button to write out the settings to disk. In order to make the changes active you will have to reboot the Xnet Viper.

8.2 Automatically Configuring Mesh Links with HDP

There are two ways to setup a mesh network, manually and automatic. The automatic mesh configuration was introduced in HopWARE version 3.1.1 and is standard available on all Viper nodes.

The Hopling Mesh Architecture (HMA) is the complete suite of Hopling Protocols used to setup, maintain and teardown a mesh network. HMA ensures mesh integrity and prevents broadcast storms. The architecture consists of two protocols: Hopling Discovery Protocol (HDP) and Hopling Mesh Protocol (HMP) which together form the Hopling Auto Mesh (HAM) feature. HAM uses HDP for the automatic mesh configuration with which it maintains the HMP links.

OSI	Hopling Protocol
7	
6	
5	
4	
3	
2	HDP HMP
1	Wireless link

Hopling Discovery Protocol (HDP) is the protocol responsible for the collection of information needed to auto create mesh links. HDP packets are sent periodically across the network to advertise the wireless capabilities of the Xnet nodes. The Xnet nodes also receive the messages sent by their neighboring nodes. It is an OSI layer 2 protocol and thus non-routable.

The Hopling Mesh Protocol (HMP) delivers a connection between two neighboring nodes. It is a peer-to-peer OSI layer 2 protocol that enables a mesh link between two nodes. And it makes sure that the different mesh links won't interfere with one another. HMP can be configured automatically through the use of HDP, or can be configured manually with the Mesh Editor.

8.2.1 Advanced Hopling Discovery Protocol (HDP) Configuration

More advanced settings can be set through the Advanced Configure section. The default HDP configuration looks like.

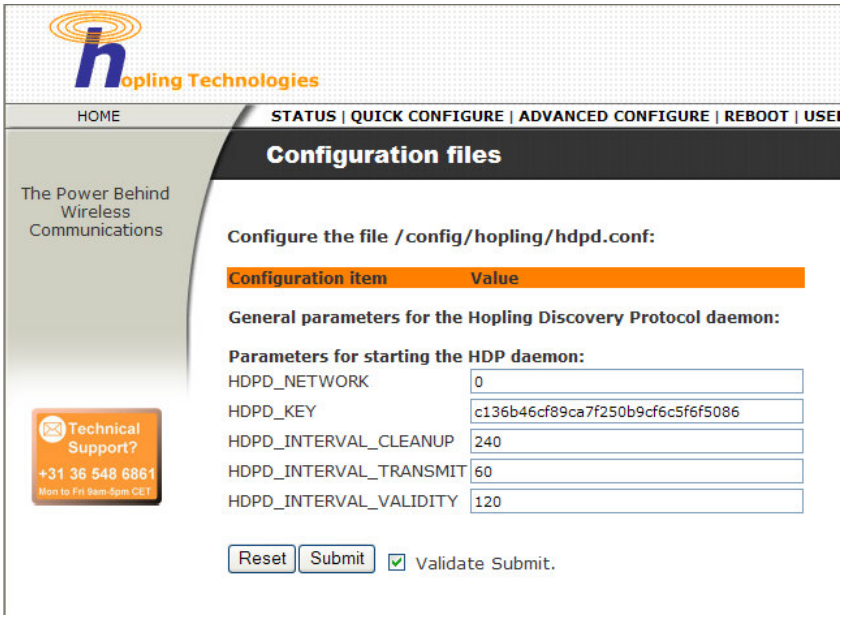


Figure 16 Advance HDP parameters

The HDPD_NETWORK parameter is the HDP Network ID (0-65535) as found in the Quick Configure page and the HDPD_KEY is identical to the HDP Key setting.

By default the HDP process sends its data across the network with 60 second intervals. This parameter can be controlled through the HDPD_INTERVAL_TRANSMIT.

The received data is cached and should thus be refreshed every 60 seconds. If data is not received after HDPD_INTERVAL_VALIDITY the data is considered non-valid, but will remain in the cache.

If after the expiration of HDPD_INTERVAL_CLEANUP seconds the data marked as invalid is still not refreshed the data is removed from the cache.

Note there is always a factor 2 between the different parameters. HDPD_INTERVAL_VALIDITY should be **at least** twice the HDPD_INTERVAL_TRANSMIT and the HDPD_INTERVAL_CLEANUP should be **at least** twice the HDPD_INTERVAL_VALIDITY. When you change the parameters, keep this ratio.

8.3 The HDP cache

As briefly noted before, the HDP information sent over the network is temporarily cached on a system. It is possible to display this information using a utility available through the command line called **hdp**.

When invoking this utility without any parameters, the following output is displayed:

```
XnetVpIV-01c822:~$ hdp
HDP cache browser - Copyright (C) 2007 Hopling Technologies B.V. All Rights Reserved.

        Usage:
        hdp [ANY|Information type][@Peer ID] [interface@MAC address] [timeout in seconds]
        [configuration file]

        Supported values for [Information type] are:
                Address
                Stations
                BuildInformation
                DeviceInformation
                DeviceLocation
                DeviceName
                DeviceType
                InterfaceID
                LastSeen
                HoplingMeshSNR
                SerialNumber
                SoftwareRelease

        XnetVpIV-01c822:~$
```

The last two options, **timeout in seconds** and **configuration file** are used for debugging purposes only. The former defines the time frame in which a response is expected, the latter allows you to specify a configuration file different from the default (**/config/hopling/hdpd.conf**).

In order to retrieve HDP data from the local system, it is possible to specify the value **ANY** or any combination of the **Information types** as listed for the **Supported values**.

Information displayed is sorted by peer. A peer can be considered a separate device from which HDP information was received. Note that peer 0 is always the local system.

The additional suffix of **@Peer ID** can be appended to an Information type to indicate that the information from a specific peer is desired, where Peer ID is an integer number. If the suffix is omitted, the information type is requested from any peer that the host currently has cached.

Specifying the ANY value will cause hdp to display any and all information available. If one or more of the **Information types** are specified, only these will be displayed.

For example;

```
XnetVpIV-01c822:~$ hdp LastSeen DeviceName ANY@1
HDP cache browser - Copyright (C) 2007 Hopling Technologies B.V. All Rights
Reserved.

Last Seen on peer 0: 4 seconds ago
Device Name on peer 0: XnetVpIV-01c822
Last Seen on peer 1: 24 seconds ago
Last Seen on peer 1: 24 seconds ago
Device Name on peer 1: Hopgate150-4105e5
Device Name on peer 1: Hopgate150-4105e5
Address on peer 1: unknown IP version 4 address 172.16.172.16/16
Address on peer 1: unknown IP version 4 address 192.168.16.127/20
Address on peer 1: wired IEEE 802.3 Ethernet address 00:02:B6:41:05:E6
Address on peer 1: unknown IP version 4 address 192.168.0.1/24
Address on peer 1: identifier IEEE 802.3 Ethernet address 00:02:B6:41:05:E5
Serial Number on peer 1: HG0115000046
Interface ID on peer 1: br_wan0
Device Location on peer 1: 52 20'58" N 5 10'48" E, height 5 meters
Device Type on peer 1: Unknown running on hardware ID 0002.00
15 records received
XnetVpIV-01c822:~$
```

will only display device name and last seen information, as well as any information from peer 1.

A brief description of the possible information types is given in the following paragraphs.

8.3.1 Address

This information type governs addresses available on a system. These addresses include IP version 4, IP version 6 and IEEE 802.3 Ethernet addresses. For every address, its approximate purpose is also displayed, if this is known by the device.

For example:

```
XnetVpIV-01c822:~$ hdp Address
HDP cache browser - Copyright (C) 2007 Hopling Technologies B.V. All Rights
Reserved.

Address on peer 0: wireless IEEE 802.3 Ethernet address 00:02:6F:24:63:DE
Address on peer 0: wireless IEEE 802.3 Ethernet address 00:02:6F:44:B7:B4
Address on peer 0: unknown IP version 4 address 172.16.172.16/16
Address on peer 0: identifier IEEE 802.3 Ethernet address 00:08:A2:01:C8:22
Address on peer 0: wireless IEEE 802.3 Ethernet address 00:02:6F:24:63:DF
Address on peer 0: wireless IEEE 802.3 Ethernet address 00:02:6F:43:77:04
Address on peer 0: wired IEEE 802.3 Ethernet address 00:08:A2:01:C8:23
Address on peer 0: unknown IP version 4 address 192.168.160.23/32
Address on peer 0: unknown IP version 4 address 192.168.18.86/20
Address on peer 0: unknown IP version 4 address 192.168.0.1/24
Address on peer 1: wired IEEE 802.3 Ethernet address 00:02:B6:41:05:E6
Address on peer 1: unknown IP version 4 address 192.168.16.127/20
Address on peer 1: unknown IP version 4 address 192.168.0.1/24
Address on peer 1: identifier IEEE 802.3 Ethernet address 00:02:B6:41:05:E5
Address on peer 1: unknown IP version 4 address 172.16.172.16/16
15 records received
```

8.3.2 BuildInformation

This information type shows information about the currently running software. This information is useful only for support purposes.

For example:

```
XnetVpIV-01c822:~$ hdp BuildInformation
HDP cache browser - Copyright (C) 2007 Hopling Technologies B.V. All Rights
Reserved.

Build Information on peer 0: 967 (development), Fri Apr 13 17:48:12 CET 2007
1 records received
```

8.3.3 DeviceName

This information type shows the hostname of the device.

For example:

```
XnetVpIV-01c822:~$ hdp DeviceName

HDP cache browser - Copyright (C) 2007 Hopling Technologies B.V. All Rights
Reserved.

Device Name on peer 0: XnetVpIV-01c822
Device Name on peer 1: Hopgate150-4105e5
2 records received
```

8.3.4 DeviceType

This information type shows the type of device. The hardware ID is a number specific to the type of hardware and can vary between two units. It is used for support purposes only.

For example:

```
XnetVpIV-01c822:~$ hdp DeviceType
HDP cache browser - Copyright (C) 2007 Hopling Technologies B.V. All Rights
Reserved.

Device Type on peer 0: Xnet Viper running on hardware ID 000C.00
Device Type on peer 1: Unknown running on hardware ID 0002.00
2 records received
```

8.3.5 Device Information

This information type shows the current system load, as well as the memory usage and the amount of time the device has been running.

For example:

```
XnetVpIV-01c822:~$ hdp DeviceInformation
HDP cache browser - Copyright (C) 2007 Hopling Technologies B.V. All Rights
Reserved.

Device Information on peer 0: Load average 0.14, 37% unused memory. Device up for 0
days, 19 hours, 30 minutes and 6 seconds
1 records received
```

8.3.6 Device Location

This information type shows the geographic location of a device, in the Longitude/Latitude Degrees Minutes'Seconds" notation.

For example:

```
XnetVpIV-01c822:~$ hdp DeviceLocation
HDP cache browser - Copyright (C) 2007 Hopling Technologies B.V. All Rights
Reserved.

Device Location on peer 0: 52 20'58" N 5 10'48" E, height 5 meters
Device Location on peer 1: 52 20'58" N 5 10'48" E, height 5 meters
2 records received
```

8.3.7 Interface ID

This information type shows the interface through which the HDP information was originally sent by the peer device.

For example:

```
XnetVpIV-01c822:~$ hdp InterfaceID
HDP cache browser - Copyright (C) 2007 Hopling Technologies B.V. All Rights
Reserved.

Interface ID on peer 0: lo
Interface ID on peer 1: br_wan0
2 records received
```

In most cases, the interface ID for peer 0 will be 'lo' (local) as the data is sent via the lo network device.

8.3.8 Last Seen

This information type shows the amount of seconds that have passed since the last time HDP information was received from this peer.

For example:

```
XnetVpIV-01c822:~$ hdp lastSeen
HDP cache browser - Copyright (C) 2007 Hopling Technologies B.V. All Rights
Reserved.

Last Seen on peer 0: 39 seconds ago
Last Seen on peer 1: 59 seconds ago
2 records received
```

8.3.9 HoplingMeshSNR

This information type shows the signal strength from any neighboring IEEE 802.11 networks in the mesh. It also shows which devices have connections established via mesh links.

For example:

```
XnetVpIV-01c822:~$ hdp HoplingMeshSNR
Hopling Mesh SNR on peer 6: 00:0C:84:01:9E:6C on radio 0 at 2437 GHz with 39 dB SNR,
SSID 'Hopling Technologies 0', capabilities unknown (unrelated)
Hopling Mesh SNR on peer 6: 00:02:6F:44:B7:B6 on radio 0 at 2437 GHz with 44 dB SNR,
SSID 'Hopling Technologies 0', capabilities HDP (unrelated)
```

8.3.10 Stations

This information type shows any currently associated IEEE 802.11 stations (also known as clients). It also shows the authentication type and the signal strength with which they are connected.

For example:

```
XnetVpIV-01c822:~$ hdp Stations
Association on peer 4: 00:18:DE:54:1C:2E at 42 dB SNR on radio 0 via virtual gateway
0 using no encryption
```

8.3.11 SerialNumber

This information type shows the serial number of any neighboring nodes:

For example:

```
XnetVpIV-01c822:~$ hdp SerialNumber
HDP cache browser - Copyright (C) 2007 Hopling Technologies B.V. All Rights
Reserved.

Serial Number on peer 1: HG0115000046
1 records received
```

8.3.12 SoftwareRelease

This information type shows the software release running on the local node.

For example:

```
XnetVpIV-01c822:~$ hdp SoftwareRelease
HDP cache browser - Copyright (C) 2007 Hopling Technologies B.V. All Rights
Reserved.

Software Release on peer 0: Xnet 3.1.3-HSS1
1 records received
```

8.4 Mesh Networking Security Considerations

This paragraph describes a number of security measures to enhance the overall security of the mesh infrastructure.

8.4.1 Blocking Unauthorized User Access to the Mesh Backbone

In a multiple radio Xnet Viper system one or more radios can be used to establish a mesh networking backbone whereas one or more radios are meant to be used for customer access. In order to prevent users from associating with a radio interface that is only meant as mesh interface client access needs to be switched off for that radio. You can further enhance security of the mesh backbone by hiding the SSID broadcast for those particular radios.

Both settings can be found in the **Quick Configuration** menu.

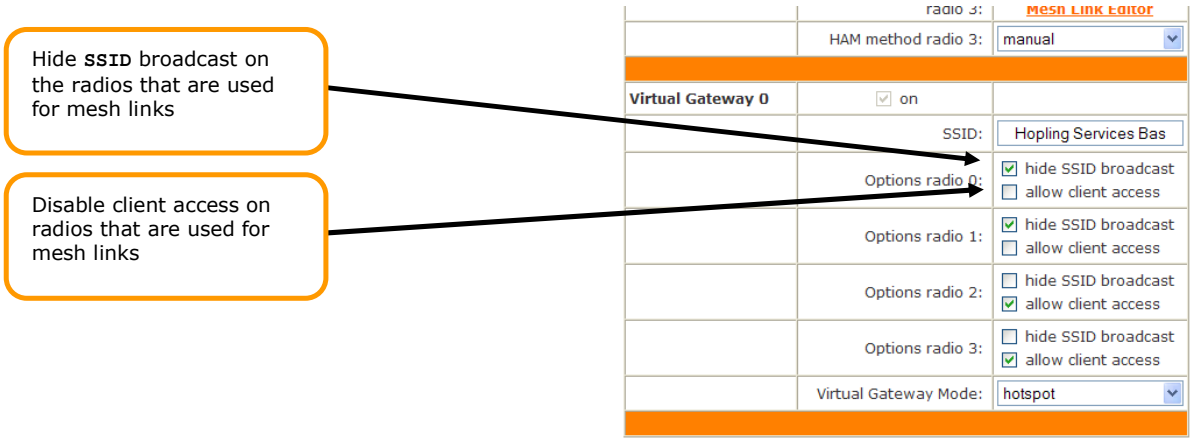


Figure 17: Enhancing Security on the Xnet Viper backbone mesh links

8.4.2 Blocking Unauthorized User Peer-to-Peer traffic

The Xnet Viper nodes incorporate a layer 2 firewall in order to prevent peer-to-peer user traffic from traveling over the mesh network. The Xnet nodes in **Hopling** mode basically act as Ethernet bridges between the wired and wireless networks. The simplest Xnet Viper node has a single wireless network interface and two wired network interfaces (Ethernet), while the most sophisticated version has two Ethernet interfaces and four wireless interfaces. Within this document the version with 2 wireless interfaces is taken as an example, because it most clearly illustrates the function of a bridging firewall.

All the interfaces of an Xnet Viper node are part of the Ethernet bridge that the Xnet Viper node is.

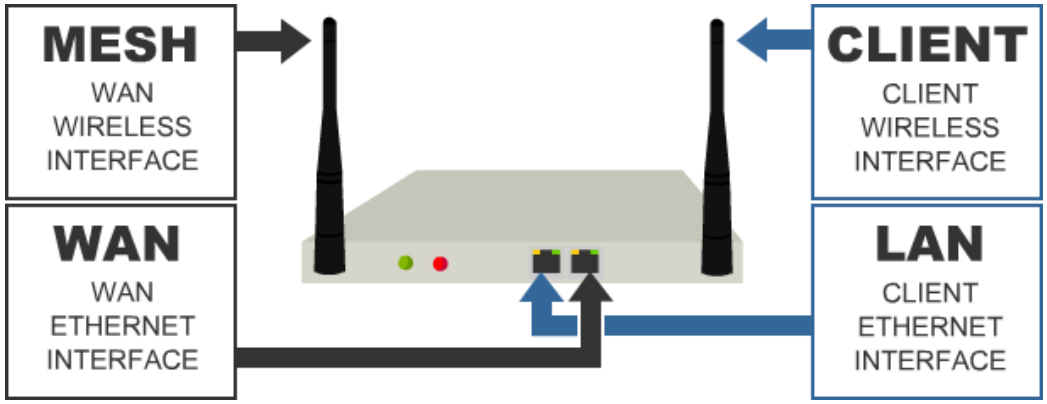


Figure 18: Xnet Viper Ethernet Bridge Explained

The bridging firewall can filter on each of these interfaces, but usually only filters the LAN and the CLIENT interfaces, since those are the ones where the clients are connected.

To illustrate why one might use a bridging firewall in the first place, let us assume a wireless mesh network with a Xfire Hopgate that connects the network to the Internet (see Figure 19: Unwanted peer-to-peer traffic over the mesh network). The Xfire Hopgate is the Access Controller that maintains the up and down speed of each user.

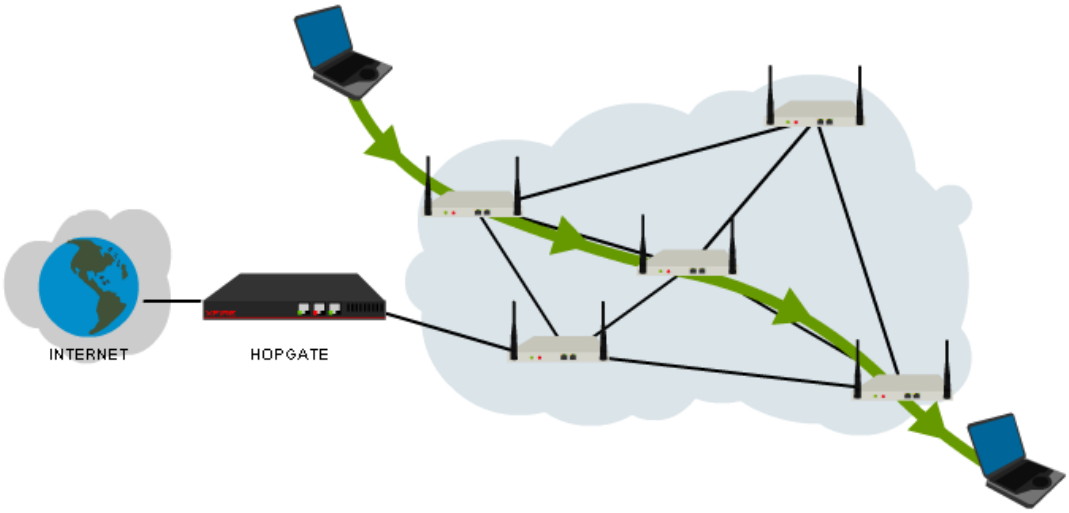


Figure 19: Unwanted peer-to-peer traffic over the mesh network

A direct connection between two wireless clients, with e.g. Peer-to-Peer software, bypasses the Xfire Hopgate. There is no control on access, no bandwidth shaping is done, and they can occupy the total amount of your wireless bandwidth, leaving no room for other users.