To prevent this from happening you should enable the bridging firewall on the Xnet Viper nodes, and tell the Xnet Viper nodes to only allow traffic to the Xfire Hopgate. This way, clients can only access the Xfire Hopgate, and control is regained over the bandwidth and the network usage.

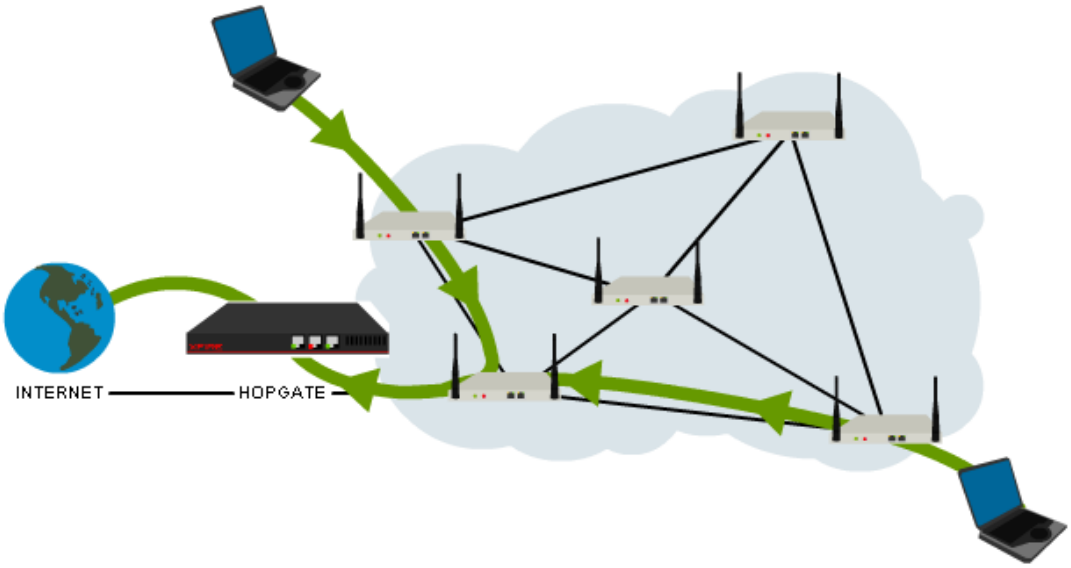



**Figure 20: Forcing user traffic only to go to the gateway**

### 8.4.3 Setup Bridging Firewall

The default settings for the bridging firewall are shown in Figure 21: Configure the Bridging Firewall. To enable the bridging firewall for the CLIENT and the LAN interface select "yes" for the ENABLE_BRIDGE_FIREWALL parameter.

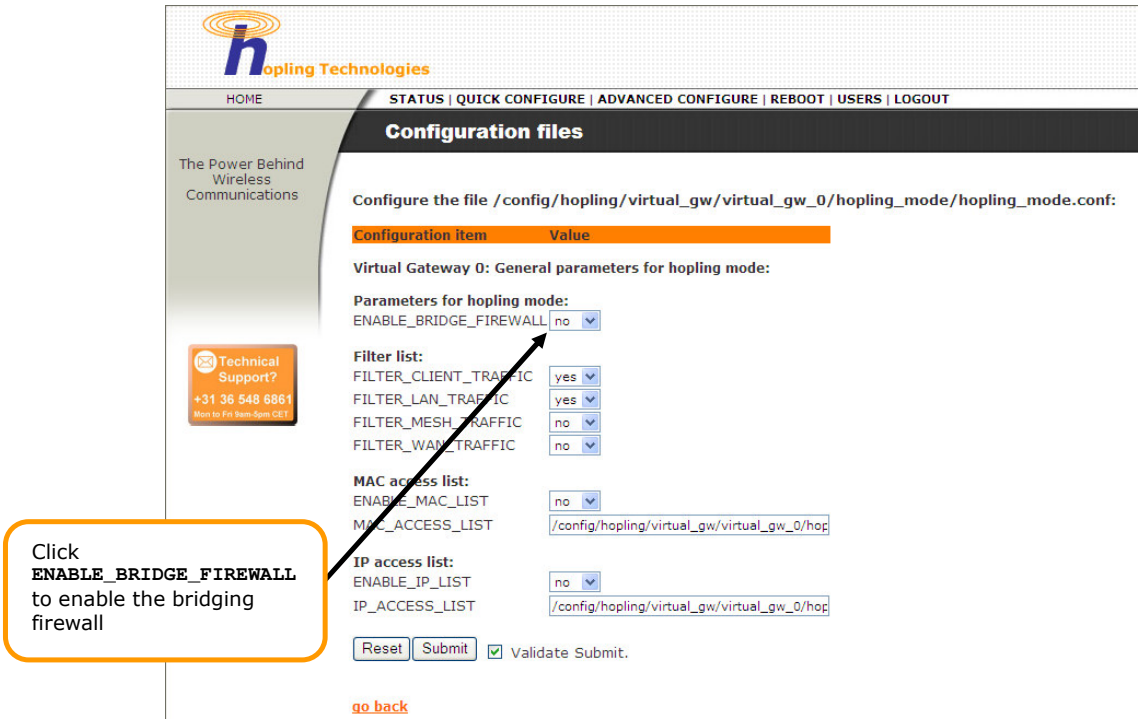



**Figure 21: Configure the Bridging Firewall**

Since this prevents all traffic across the Xnet node one should enable access to the device that give access to the Internet, for example the gateway device such as Xfire Hopgate.

On Ethernet-level it means we need to give access to the MAC address of the Xfire Hopgate. So set the ENABLE_MAC_LIST to "yes" and after clicking "Submit" go to the MAC access list configuration as shown in Figure 22: Configure the Bri.

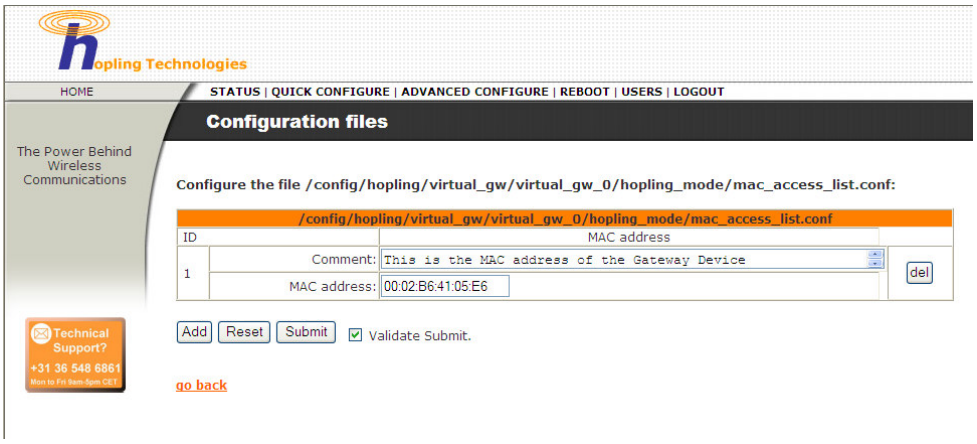



**Figure 22: Configure the Bridging Firewall MAC access list**

Fill in the MAC address of the Xfire Hopgate and after you have saved the data and rebooted the Xnet node, only data passing back and forth to your Xfire Hopgate will pass the Xnet node, everything else is blocked, which is exactly what we wanted.

**Note:** If you run your own DNS servers or have a DHCP server within the wireless network, you should also add the MAC addresses for those machines.

### 8.4.4 Bridging firewall on the WAN and MESH interface

The bridging firewall can also be enabled for the WAN and MESH interfaces. If you are not careful, though, you might prevent access to your Xnet node for configuration purposes, or you might disconnect links from your mesh network, or even prevent the entire mesh network from working. If you have locked yourself out from the Xnet node, there is only one way to restore the settings and that is by returning the unit to Hopling Technologies. **So be careful!**

Enabling the bridging firewall on the WAN interface blocks all traffic on the interface. This means that it also blocks requests to the SSH or HTTP configuration interfaces. Make sure that you first add the machines that are used for configuration to the allowed MAC list, before you enable this setting. Think of all management machines that should have access. Make sure that you put at least two management nodes in the list (if one network card dies, you can use the other one to change the MAC access list).

Enabling the bridging firewall on the mesh interface should only be done when you have first added all MAC addresses with which the Xnet node (mesh) communicates to the allowed MAC address list otherwise you will break your mesh. And you should never enable this feature when you use Hopling Auto Mesh. Note also that as soon as you replace one or more Xnet nodes, that you should update the allowed MAC access list as soon as possible.

### 8.4.5 Allowed IP address list

Although the Xnet node in hopling mode is a bridge, it can filter on IP level. **This is not recommended: IP filtering should be done on the Hopgate.**

To filter on a specific IP address set the ENABLE_IP_LIST setting to "yes". This will block all IP traffic. You should add the allowed IP addresses to the ip_access_list.conf, as shown in **Figure 23: Configure the Bridging Firewall IP Address Lis**t.

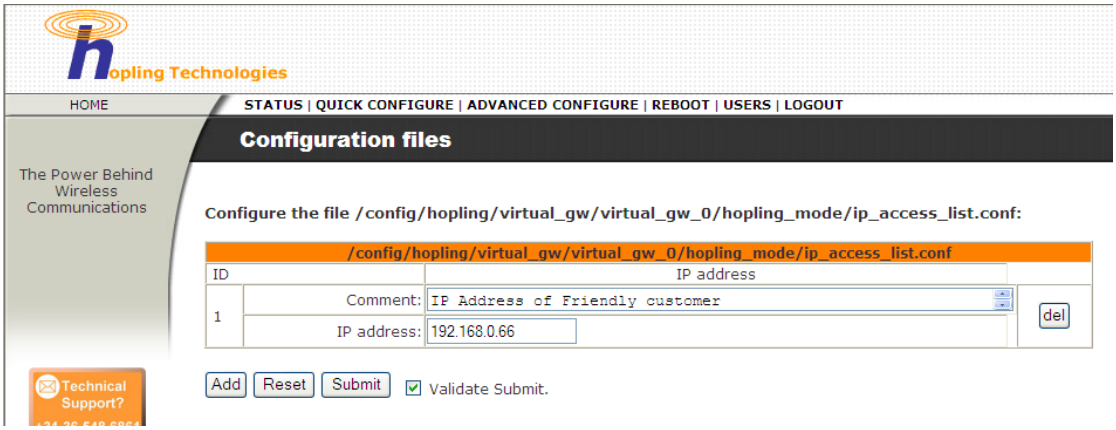



**Figure 23: Configure the Bridging Firewall IP Address Lis**t

# 9 Virtual Gateway Configuration Parameters

The Xnet Viper node can be split into one or more (maximum 4) Virtual systems called **Virtual Gateways**. Each Virtual Gateway can be configured with its own set of parameters such as SSID (WiFi network name) IP addresses, Virtual LAN and operational mode (hopling or hotspot). By default the first Virtual Gateway (VGW0) is always enabled. The other three Virtual gateways (VGW1, VGW2 and VGW3) are disabled when the Xnet Viper is set to factory defaults.

## *9.1 Setting SSID or network name for Virtual Gateway 0.*

When creating a wireless network using the Xnet Viper, you must give the network a name. In order for a client to connect to your network they must know the name of the network. The SSID is the identifying name of an 802.11a/b/g (WiFi) wireless network. By specifying the SSID in your setup is how you make sure that they connect to your wireless network instead of another operators' network by mistake. The SSID or network name for the Xnet Viper is tied to a specific Virtual Gateway. Each Virtual Gateway holds its own SSID parameter.

### 9.1.1 Setting SSID through Command Line Interface

For Virtual Gateway 0 the SSID is held in the parameter **`WIFI_0_0_SSID`** in the file:

```
/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0_0.conf.
```

As an example,

```
#@! <upload> <config> <reserved2> <reserved3> <reserved4>
#@$ <"Virtual Gateway 0: Specific Wifi parameters for radio 0">
#
# file: /config/hopling/virtual_gw/virtual_gw_0/wifi/WIFI_0_0.conf
#
# Author: Rudger van Brenk
# (c) Hopling Technologies 2005, 2006
#
# Configuration file for wireless VAP interface 0.
#
# This file is specific for the Atheros hardware.

#@$ <"Wifi internal info">
#@@ <WIFI_0_0_HW>             <STRING>    <0,128>  <READ_ONLY>   <RESERVED>   <"Wifi
HW type. Please do not change this yourself">
#@@ <WIFI_0_0_IFACE_NAME>     <STRING>    <0,128>  <READ_ONLY>   <RESERVED>   <"Wifi
HW interface name. Please do not change this yourself">

WIFI_0_0_HW="ath"
WIFI_0_0_IFACE_NAME="ath00"

#@$ <"General wifi parameters">
#@@ <WIFI_0_0_ENABLE>         <DROPDOWN>  <yes,no>  <NONE>   <RESERVED>  <"Enable
this interface. If disabled, all other settings are ignored">
#@@ <WIFI_0_0_SSID>           <STRING>    <0,32>    <NONE>   <RESERVED>  <"SSID
(network name)">
#@@ <WIFI_0_0_HIDDEN_SSID>    <DROPDOWN>  <yes,no>  <NONE>   <RESERVED>  <"Disable
SSID beacon broadcasting for this device">
#@@ <WIFI_0_0_ALLOW_ACCESS>   <DROPDOWN>  <yes,no>  <NONE>   <RESERVED>  <"Allow
client access to this VGW SSID">

WIFI_0_0_ENABLE="yes"
WIFI_0_0_SSID="Hopling Services Bas"
WIFI_0_0_HIDDEN_SSID="no"
WIFI_0_0_ALLOW_ACCESS="yes"

#@$ <"Wifi security parameters">
#@@ <WIFI_0_0_ENABLE_SECURITY>         <DROPDOWN>  <yes,no>  <NONE>   <RESERVED>
<"Enable Security for this Service Set. If disabled, all other security settings are
ignored">

WIFI_0_0_ENABLE_SECURITY="no"

#@$ <"WEP Configuration">
```

```
#@@ <WIFI_0_0_ENABLE_WEP>         <DROPDOWN>  <yes,no> <NONE>   <RESERVED>  <"Enable
WEP encryption. Note: only ONE VGW can use WEP at the same time!">
#@@ <WIFI_0_0_WEP_KEY_1>          <STRING>    <10,26>  <NONE>   <RESERVED>  <"The
default WEP key for keyid 1. Enter  the  key  in  hex digits  as  XXXXXXXXXX. 10
digits for WEP 64 bits, 26 digits for WEP 128 bits.">
#@@ <WIFI_0_0_WEP_KEY_2>          <STRING>    <10,26>  <NONE>   <RESERVED>  <"The
default WEP key for keyid 2. Enter  the  key  in  hex digits  as  XXXXXXXXXX. 10
digits for WEP 64 bits, 26 digits for WEP 128 bits.">
#@@ <WIFI_0_0_WEP_KEY_3>          <STRING>    <10,26>  <NONE>   <RESERVED>  <"The
default WEP key for keyid 3. Enter  the  key  in  hex digits  as  XXXXXXXXXX. 10
digits for WEP 64 bits, 26 digits for WEP 128 bits.">
#@@ <WIFI_0_0_WEP_KEY_4>          <STRING>    <10,26>  <NONE>   <RESERVED>  <"The
default WEP key for keyid 4. Enter  the  key  in  hex digits  as  XXXXXXXXXX. 10
digits for WEP 64 bits, 26 digits for WEP 128 bits.">
#@@ <WIFI_0_0_WEP_KEY_ID>         <DROPDOWN>  <1,2,3,4> <NONE>   <RESERVED>
<"Default WEP key id to use, 1 for KEY1, 2 for KEY2, etc.">

WIFI_0_0_ENABLE_WEP="no"
WIFI_0_0_WEP_KEY_1="1122334455"
WIFI_0_0_WEP_KEY_2="1122334455"
WIFI_0_0_WEP_KEY_3="1122334455"
WIFI_0_0_WEP_KEY_4="1122334455"
WIFI_0_0_WEP_KEY_ID="1"

#@$ <"WPA/RSN Configuration">
#@@ <WIFI_0_0_ENABLE_WPA>         <DROPDOWN>  <yes,no>          <NONE>   <RESERVED>
<"Enable WPA encryption.">
#@@ <WIFI_0_0_WPA_PROTO>          <DROPDOWN>  <wpa,rsn,both>    <NONE>   <RESERVED>
<"Use WPA, use RSN (WPA2) or use both">
#@@ <WIFI_0_0_WPA_METHOD>         <DROPDOWN>  <wpa_psk,wpa_eap> <NONE>   <RESERVED>
<"WPA method, either WPA-PSK or WPA-EAP (WPA-RADIUS)">
#@@ <WIFI_0_0_WPA_CIPHER_SUITE>   <DROPDOWN>  <tkip,aes,both>   <NONE>   <RESERVED>
<"WPA cipher suite(s) for pairwise keys.">
#@@ <WIFI_0_0_WPA_PSK_KEY_METHOD> <DROPDOWN>  <passphrase,psk>  <NONE>   <RESERVED>
<"Which method to use for setting the WPA-PSK key.">
#@@ <WIFI_0_0_WPA_PSK_PASSPHRASE> <STRING>    <8-63>           <NONE>   <RESERVED>
<"ASCII passphrase (8..63 characters) that will be converted to PSK.">
#@@ <WIFI_0_0_WPA_PSK_PSK>        <HEX>       <64>             <NONE>   <RESERVED>
<"WPA pre-shared key for WPA-PSK. A 256-bit secret in hex format (64 hex digits)">
#@@ <WIFI_0_0_WPA_GROUP_REKEY>    <INT>       <0,1000000>      <NONE>   <RESERVED>
<"Time interval for rekeying GTK (broadcast/multicast encryption keys) in seconds.">
#@@ <WIFI_0_0_WPA_STRICT_REKEY>   <DROPDOWN>  <yes,no>          <NONE>   <RESERVED>
<"Rekey GTK when any STA that possesses the current GTK is leaving the BSS.">
#@@ <WIFI_0_0_WPA_GMK_REKEY>      <INT>       <0,1000000>      <NONE>   <RESERVED>
<"Time interval for rekeying GMK (master key used internally to generate GTKs (in
seconds).">
#@@ <WIFI_0_0_EAP_REAUTH_PERIOD>  <INT>       <0,1000000>      <NONE>   <RESERVED>
<"EAP reauthentication period in seconds (default: 3600 seconds; 0 = disable
reauthentication).">

WIFI_0_0_ENABLE_WPA="no"
WIFI_0_0_WPA_PROTO="wpa"
WIFI_0_0_WPA_METHOD="wpa_psk"
WIFI_0_0_WPA_CIPHER_SUITE="tkip"
WIFI_0_0_WPA_PSK_KEY_METHOD="passphrase"
WIFI_0_0_WPA_PSK_PASSPHRASE="passwordwpa"
WIFI_0_0_WPA_PSK_PSK="0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcd
ef"
WIFI_0_0_WPA_GROUP_REKEY="600"
WIFI_0_0_WPA_STRICT_REKEY="no"
WIFI_0_0_WPA_GMK_REKEY="86400"
WIFI_0_0_EAP_REAUTH_PERIOD="3600"

#@$ <"Parameters for RADIUS authentication server">
#@@ <WIFI_0_0_RADIUS_NASID>              <STRING>    <0,253>              <NONE>
<RESERVED>   <"Optional NAS-identifier for RADIUS messages. Leave empty when not
used">
#@@ <WIFI_0_0_RADIUS_AUTH_SERVER>       <HOST_IP>   <1>                  <NONE>
<RESERVED>   <"RADIUS authentication server">
#@@ <WIFI_0_0_RADIUS_AUTH_PORT>         <PORT>      <1>                  <NONE>
<RESERVED>   <"Port number of RADIUS authentication server">
#@@ <WIFI_0_0_RADIUS_AUTH_SECRET>       <STRING>    <0,128>              <NONE>
<RESERVED>   <"Shared secret for RADIUS authentication server">
#@@ <WIFI_0_0_RADIUS_SEC_AUTH_SERVER>   <HOST_IP>   <1>                  <NONE>
<RESERVED>   <"Secondary RADIUS authentication server, to be used if primary one
does not reply to RADIUS packets. Leave empty when not used.">
#@@ <WIFI_0_0_RADIUS_SEC_AUTH_PORT>     <PORT>      <1>                  <NONE>
<RESERVED>   <"Port number of secondary RADIUS authentication server">
#@@ <WIFI_0_0_RADIUS_SEC_AUTH_SECRET>   <STRING>    <0,128>              <NONE>
<RESERVED>   <"Shared secret for secondary RADIUS authentication server">
#@@ <WIFI_0_0_RADIUS_RETRY_PRIMARY_INTERVAL> <INT>  <0,1000000>          <NONE>
<RESERVED>    <"Retry interval for trying to return to the primary RADIUS server (in
seconds). Primary server will be retried after configured amount of time even if the
currently used secondary server is still working. Set to 0 to disable.">
```

```
WIFI_0_0_RADIUS_NASID=""
WIFI_0_0_RADIUS_AUTH_SERVER="127.0.0.1"
WIFI_0_0_RADIUS_AUTH_PORT="1812"
WIFI_0_0_RADIUS_AUTH_SECRET="secret"
WIFI_0_0_RADIUS_SEC_AUTH_SERVER=""
WIFI_0_0_RADIUS_SEC_AUTH_PORT="1812"
WIFI_0_0_RADIUS_SEC_AUTH_SECRET="secret2"
WIFI_0_0_RADIUS_RETRY_PRIMARY_INTERVAL="600"

#@$ <"Parameters for RADIUS accounting server">
#@@ <WIFI_0_0_RADIUS_ACCT_ENABLE>       <DROPDOWN>  <no,yes>            <NONE>
<RESERVED>   <"Enable RADIUS accounting.">
#@@ <WIFI_0_0_RADIUS_ACCT_SERVER>       <HOST_IP>   <1>                 <NONE>
<RESERVED>   <"RADIUS accounting server">
#@@ <WIFI_0_0_RADIUS_ACCT_PORT>         <PORT>      <1>                 <NONE>
<RESERVED>   <"Port number of RADIUS accounting server">
#@@ <WIFI_0_0_RADIUS_ACCT_SECRET>       <STRING>    <0,128>             <NONE>
<RESERVED>   <"Shared secret for RADIUS accounting server">
#@@ <WIFI_0_0_RADIUS_SEC_ACCT_SERVER>   <HOST_IP>   <1>                 <NONE>
<RESERVED>   <"Secondary RADIUS accounting server.  Leave empty when not used.">
#@@ <WIFI_0_0_RADIUS_SEC_ACCT_PORT>     <PORT>      <1>                 <NONE>
<RESERVED>   <"Port number of secondary RADIUS accounting server">
#@@ <WIFI_0_0_RADIUS_SEC_ACCT_SECRET>   <STRING>    <0,128>             <NONE>
<RESERVED>   <"Shared secret for secondary RADIUS accounting server">
#@@ <WIFI_0_0_RADIUS_ACCT_INT_VAL>      <INT>       <0,10000>           <NONE>
<RESERVED>   <"Default Accounting Interim interval in seconds. Note: if set ( larger
than 0), this overrides possible Acct-Interim-Interval attribute in Access-Accept
message. Thus, this value should not be set, if RADIUS server is used to control the
interim interval.">

WIFI_0_0_RADIUS_ACCT_ENABLE="no"
WIFI_0_0_RADIUS_ACCT_SERVER="127.0.0.1"
WIFI_0_0_RADIUS_ACCT_PORT="1813"
WIFI_0_0_RADIUS_ACCT_SECRET="secret"
WIFI_0_0_RADIUS_SEC_ACCT_SERVER=""
WIFI_0_0_RADIUS_SEC_ACCT_PORT="1813"
WIFI_0_0_RADIUS_SEC_ACCT_SECRET="secret2"
WIFI_0_0_RADIUS_ACCT_INT_VAL="600"

# End
```

After making changes to the `/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0_0.conf` 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.

The other Virtual Gateways also have the SSID parameter, but this parameter is stored in the files corresponding to each Virtual Gateway.

**Virtual Gateway 1**

`/config/hopling/virtual_gw/virtual_gw_1/wifi/ wifi_0_1.conf.`

**Virtual Gateway 2**

`/config/hopling/virtual_gw/virtual_gw_2/wifi/ wifi_0_2.conf.`

**Virtual Gateway 3**

`/config/hopling/virtual_gw/virtual_gw_3/wifi/ wifi_0_3.conf.`

### 9.1.2 Setting SSID through Web Interface

When you create a network using the Xnet Viper, you must give the wireless network a name. In order for wireless clients to connect to your network they must know the name of the network. The SSID is the identifying name of an 802.11a/b/g (WiFi) wireless network. By specifying the SSID in your setup is how you make sure that wireless clients connect to your wireless network instead of your competitor's network by mistake.

The Xnet Viper can contain four independent SSIDs per radio. Each SSID is tied to a Virtual Gateway numbered 0 to 3. You can set the first SSID using the **QUICK CONFIGURE** page of the web interface. Additional SSIDs must be set through the **ADVANCED CONFIGURE** pages.

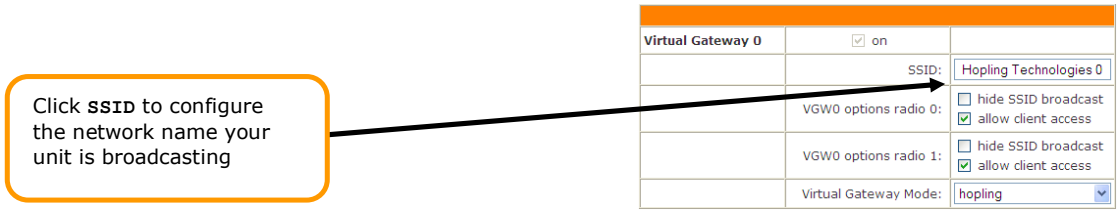



**Figure 24: Setting the SSID on the Xnet Viper**

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

## 9.2 System configuration files for hopling mode

When the Xnet Viper boots, a number of scripts are executed automatically by the system before any user can log in. The main user editable configuration files for the Xnet Viper in hopling mode are:

```
/config/hopling/hopling.conf
/config/hopling/virtual_gw/virtual_gw_0/virtual_gw.0.conf
/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0_0.conf
/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0_general.conf
/config/hopling/virtual_gw/virtual_gw_0/wan/wan_0.conf
/config/hopling/wifi_backbone/wifi_backbone_0/neighbors_0.conf
```

On an Xnet Viper-II there are additional files for the second radio:

```
/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_1_0.conf
/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_1_general.conf
/config/hopling/wifi_backbone/wifi_backbone_1/neighbors_1.conf
```

These files contain the initialization settings specific to your own system, such as setting the wireless network name (SSID), wireless channel and other parameters needed for the wireless network. Before changes can be made to the file system it needs to be set to a writeable state. This is done with the following command:

```
XnetMkII-c3a124:~$ remount rw
```

After this any changes can be made to the configuration files. To make the file system read-only again type the following command:

```
XnetMkII-c3a124:~$ remount ro
```

## 9.3 Changing WAN IP address and DHCP/STATIC settings

Initially, all Xnet Viper's that are shipped by Hopling Technologies will have default settings for the IP addresses. The factory default settings are for the WAN interface of the Xnet to receive an IP from an external DHCP server. This can be changed so that the WAN interface has a static IP address.

### 9.3.1 Setting WAN IP address through Command Line Interface

These default IP addresses and whether or not the interface is configured in STATIC or DHCP mode can be changed by editing the file parameters in the file:

```
/config/hopling/virtual_gw/virtual_gw_0/wan/wan_0.conf.
```

In this file you can find the variables to change the IP address: **`WAN_0_IP`**, the method to use to set the IP address (DHCP or STATIC): **`WAN_0_METHOD`**. The WAN interface is called `br_wan0`.

As an example to change the IP address on the WAN interface edit the `WAN_0_IP` entry in the `wan_0.conf` file;

```
#@! <upload> <config> <reserved2> <reserved3> <reserved4>
#@$ <"Virtual Gateway 0: WAN parameters">
#
# File:/config/hopling/virtual_gw/virtual_gw_0/wan/wan_0.conf
#
# Configuration file for the WAN interfaces
# (c) Hopling Technologies 2004, 2005, 2006
# Bas Muns
#
# This file is used to configure the WAN interfaces.
# When VLAN is enabled, several WAN interfaces can be configured.
# Note that the IP address range for all VLAN enabled WAN interfaces
# should be different!
#

#@$ <"Internal parameters">
#@@ <WAN_0_IFACE_NAME>      <STRING>    <0,128>  <READ_ONLY>   <RESERVED>
<"Interface name. Please do not change this yourself">

WAN_0_IFACE_NAME="eth0"

#@$ <"Parameters for the ethernet WAN interface">
#@@ <WAN_0_ENABLE>           <DROPDOWN>  <yes,no>       <READ_ONLY> <RESERVED>
<"Configure this interface. Never disable it!!! If disabled, the rest of the
settings will be ignored.">
#@@ <WAN_0_METHOD>           <DROPDOWN>  <static,dhcp>  <NONE>      <RESERVED>
<"If set to dhcp the IP address is configured through DHCP">
#@@ <WAN_0_IP>               <IP>        <1>            <NONE>      <RESERVED>
<"IP address for the wan interface if WAN_0_METHOD is set to static. NOTE: The IP
address should be unique for every WAN.x interface">
#@@ <WAN_0_MASK>             <NETMASK>   <1>            <NONE>      <RESERVED>
<"Netmask for wired interface">
#@@ <WAN_0_GW>               <IP>        <1>            <NONE>      <RESERVED>
<"Default gateway">
#@@ <WAN_0_NETADDR>          <IP>        <1>            <NONE>      <RESERVED>
<"Subnet address">
#@@ <WAN_0_DHCP_START>       <IP>        <1>            <NONE>      <RESERVED>
<"Starting range for giving out IP addresses">
#@@ <WAN_0_DHCP_END>         <IP>        <1>            <NONE>      <RESERVED>
<"End of range for giving out IP addresses">
#@@ <WAN_0_BCAST>            <IP>        <1>            <NONE>      <RESERVED>
<"Broadcast address used in DHCP lease">
#@@ <WAN_0_DNS>              <IP>        <3>            <SPACESEP>  <RESERVED>
<"IP address of the DNS server to give in the DHCP lease">
#@@ <WAN_0_DNS_METHOD>       <DROPDOWN>  <static,dhcp>  <NONE>      <RESERVED>
<"If set to dhcp the IP address(es) supplied via dhcp are used. When set to static,
the IP address(es) set in WAN_0_DNS are used">
#@@ <WAN_0_SUPPLY_DHCP>      <DROPDOWN>  <yes,no>       <NONE>      <RESERVED>
<"If enabled, the DHCP server will give out leases for this interface. NOTE: Only
possible if WAN_0_METHOD is set to static">

WAN_0_ENABLE="yes"
WAN_0_METHOD="dhcp"
```

```
WAN_0_IP="10.0.0.1"
WAN_0_MASK="255.255.255.0"
WAN_0_GW="10.0.0.1"
WAN_0_NETADDR="10.0.0.0"
WAN_0_DHCP_START="10.0.0.10"
WAN_0_DHCP_END="10.0.0.250"
WAN_0_BCAST="10.0.0.255"
WAN_0_DNS="10.0.0.1"
WAN_0_DNS_METHOD="dhcp"
WAN_0_SUPPLY_DHCP="no"

#@$ <"VLAN parameters">
#@@ <WAN_0_ENABLE_VLAN>    <DROPDOWN>  <yes,no>       <NONE>      <RESERVED>
<"Enable VLAN">
#@@ <WAN_0_VLAN_TAG>       <INT>       <1,4069>       <NONE>      <RESERVED>
<"Specifies the VLAN tag number used for this interface. NOTE: The VLAN_TAG should
be unique for every WAN.x interface">

WAN_0_ENABLE_VLAN="no"
WAN_0_VLAN_TAG="0"

#@$ <"Extra IP address(es)">
#@@ <WAN_0_EXTRA_IP_ENABLE>   <DROPDOWN>  <yes,no>       <NONE>      <RESERVED>
<"Enable adding of extra IP aliases">
#@@ <WAN_0_EXTRA_IP_ADDR>     <IP_MASK>   <5>            <SPACESEP>  <RESERVED>
<"List of IP alias(es) to create. It needs to be in the format IP-address/Netmask.
When multiple entries are added, separate them with a space">

WAN_0_EXTRA_IP_ENABLE="no"
WAN_0_EXTRA_IP_ADDR="172.16.16.2/255.255.0.0"

#@$ <"Extra parameters">
#@@ <WAN_0_FIRST_HOP>          <DROPDOWN>  <yes,no>       <NONE>      <RESERVED>
<"Set to yes if this is the fist hop in a hopling mode network">

WAN_0_FIRST_HOP="no"

# End
```

After making changes to the `/config/hopling/virtual_gw/virtual_gw_0/wan/wan_0.conf` 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.

### 9.3.2 Setting WAN IP address through Web Interface

You can set the WAN network interface on the Xnet Viper to use DHCP (default setting) or to use a static IP address. Select the list box **mode** to switch the mode from DHCP to static.

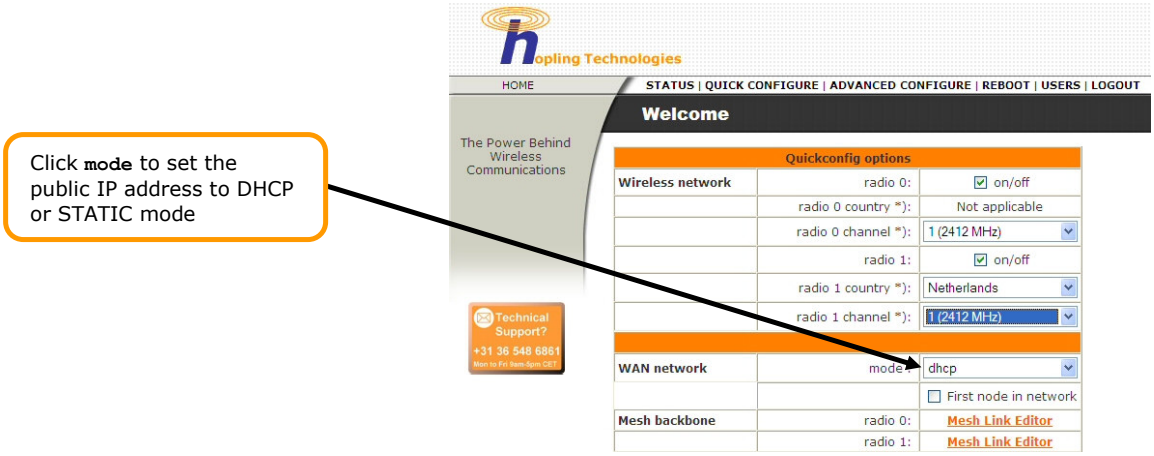



**Figure 25: Select MODE to set the public IP address to DHCP or STATIC**

Configure the public network IP address (WAN) Port

**WAN network mode**: if set to "dhcp" then the Xnet Viper will use DHCP to determine the public network IP address. If the WAN network mode switch is set to static the screen will refresh and you can set the IP address and IP netmask as shown in the fields below.

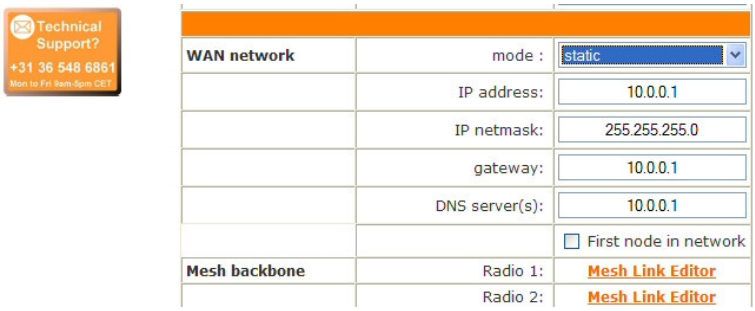



**Figure 26: Static Public IP address configuration menu**

## 9.4 DHCP protocol

DHCP (Dynamic Host Configuration Protocol) is a server service that dynamically assigns, or leases, IP addresses and related IP information to network clients. At first glance, this may not seem like an important task. However, you have to remember that, on a TCP/IP network, each network client must have a unique IP address and an appropriate subnet mask. Without these items, a client cannot communicate on the network. For example, if two clients have the same IP address, neither will be able to communicate on the network. DHCP handles all this work automatically. Each client gets a unique IP address, subnet mask, and other IP information such as default gateways and the IP addresses of WINS (Windows Internet Name Service) and DNS (Domain Name System) servers. DHCP makes certain that no clients have duplicate addresses, and this entire process is invisible to network administrators and network users.

DHCP works by leasing IP addresses and IP information to network clients for a period of time. For the lease to happen, the following negotiation process occurs:

1. During the boot process, a client computer that is configured as a DHCP client sends out a broadcast packet called DHCPDISCOVER. This Discover packet contains the client's computer name and Media Access Control (MAC) address so the DHCP servers can respond to it.

2. DHCP servers on the network respond to the broadcast with a DHCPOFFER. In essence, the DHCPOFFER says, "I am a DHCP server and I have a lease for you." If several DHCP servers respond to the request, the client accepts the first offer that it receives.

3. The client responds via a broadcast message called a DHCPREQUEST. This message basically says, "I accept your lease offer and would like an IP address." If other DHCP servers made offers, they also see their lease offers were not accepted by the broadcast message, so they rescind their offers. (They must not like getting snubbed by a client computer.)

4. The DHCP server whose offer was accepted responds with a DHCPACK message, which acknowledges the lease acceptance and contains the client's IP address lease as well as other IP addressing information that you configure the server to provide. The client is now a TCP/IP client and can participate on the network.

Hopling can both act as DHCP server, giving out IP addresses to end customers, and as DHCP client, receiving its own IP address from a central DHCP server.

### 9.4.1 Configuring VGW0 as DHCP server

Each Virtual Gateway on the Xnet can act as DHCP server for both the wireless network as well as the wired network. For this is has to run a program called the DHCP daemon, or `dhcpd`. If the DHCP daemon is running for this particular Virtual Gateway or not is controlled by the `LAN_0_SUPPLY_DHCP="yes"` parameter in the `/config/hopling/virtual_gw/virtual_gw_0/lan/lan_0.conf` file.

If you want the system to provide IP addresses to wireless or wired clients this parameter must be set to "**yes**". To disable the DHCP server set this parameter to "**no**".

As an example for this system to supply IP addresses through DHCP on the wireless interface set the LAN_0_SUPPLY_DHCP parameter to "yes";

```
#@! <upload> <config> <reserved2> <reserved3> <reserved4>
#@$ <"Virtual Gateway 0: LAN parameters">
#
# File:/config/hopling/virtual_gw/virtual_gw_0/lan/lan_0.conf
#
# Configuration file for the LAN interfaces
# (c) Hopling Technologies 2004, 2005, 2006
# Bas Muns
#
# This file is used to configure the LAN interfaces.
```

```
# When VLAN is enabled, several LAN interfaces can be configured.
# Note that the IP address range for all VLAN enabled LAN interfaces
# should be different!
#

#@$ <"Internal parameters">
#@@ <LAN_0_IFACE_NAME>      <STRING>    <0,128>  <READ_ONLY>   <RESERVED>
<"Interface name. Please do not change this yourself">

LAN_0_IFACE_NAME="eth1"

#@$ <"Parameters for the ethernet LAN interface">
#@@ <LAN_0_ENABLE>            <DROPDOWN>  <yes,no>       <NONE>      <RESERVED>
<"Configure this interface. If disabled, the rest of the settings will be ignored">
#@@ <LAN_0_METHOD>            <DROPDOWN>  <static,dhcp>  <NONE>      <RESERVED>
<"If set to dhcp the IP address is configured through DHCP">
#@@ <LAN_0_IP>                <IP>        <1>            <NONE>      <RESERVED>
<"IP address for the wan interface if LAN_0_METHOD is set to static. NOTE: The IP
address should be unique for every LAN.x interface">
#@@ <LAN_0_MASK>              <NETMASK>   <1>            <NONE>      <RESERVED>
<"Netmask for wired interface">
#@@ <LAN_0_GW>                <IP>        <1>            <NONE>      <RESERVED>
<"Default gateway">
#@@ <LAN_0_NETADDR>           <IP>        <1>            <NONE>      <RESERVED>
<"Subnet address">
#@@ <LAN_0_DHCP_START>        <IP>        <1>            <NONE>      <RESERVED>
<"Starting range for giving out IP addresses">
#@@ <LAN_0_DHCP_END>          <IP>        <1>            <NONE>      <RESERVED>
<"End of range for giving out IP addresses">
#@@ <LAN_0_BCAST>             <IP>        <1>            <NONE>      <RESERVED>
<"Broadcast address used in DHCP lease">
#@@ <LAN_0_DNS>               <IP>        <3>            <SPACESEP>  <RESERVED>
<"IP address of the DNS server to give in the DHCP lease">
#@@ <LAN_0_SUPPLY_DHCP>       <DROPDOWN>  <yes,no>       <NONE>      <RESERVED>
<"If enabled, the DHCP server will give out leases for this interface. NOTE: Only
possible if LAN_0_METHOD is set to static">
#@@ <LAN_0_DHCP_LOG_EVENTS>   <DROPDOWN>  <yes,no>       <NONE>      <RESERVED>
<"Enable this option to send events to the log server on client lease commit,
release and expiry">

LAN_0_ENABLE="yes"
LAN_0_METHOD="static"
LAN_0_IP="192.168.0.1"
LAN_0_MASK="255.255.255.0"
LAN_0_GW="192.168.0.1"
LAN_0_NETADDR="192.168.0.0"
LAN_0_DHCP_START="192.168.0.10"
LAN_0_DHCP_END="192.168.0.250"
LAN_0_BCAST="192.168.0.255"
LAN_0_DNS="192.168.0.1"
LAN_0_SUPPLY_DHCP="yes"
LAN_0_DHCP_LOG_EVENTS="no"

#@$ <"VLAN parameters">
#@@ <LAN_0_ENABLE_VLAN>    <DROPDOWN>  <yes,no>       <NONE>      <RESERVED>
<"Enable VLAN">
#@@ <LAN_0_VLAN_TAG>       <INT>       <1,4069>       <NONE>      <RESERVED>
<"Specifies the VLAN tag number used for this interface. NOTE: The VLAN_TAG should
be unique for every LAN.x interface">

LAN_0_ENABLE_VLAN="no"
LAN_0_VLAN_TAG="0"

#@$ <"Extra IP address(es)">
#@@ <LAN_0_EXTRA_IP_ENABLE>   <DROPDOWN>  <yes,no>       <NONE>      <RESERVED>
<"Enable adding of extra IP aliases">
#@@ <LAN_0_EXTRA_IP_ADDR>     <IP_MASK>   <5>            <SPACESEP>  <RESERVED>
<"List of IP alias(es) to create. It needs to be in the format IP-address/Netmask.
When multiple entries are added, separate them with a space">

LAN_0_EXTRA_IP_ENABLE="no"
LAN_0_EXTRA_IP_ADDR="172.16.16.1/255.255.0.0"

# End
```

If you have changed the LAN IP address range of the Xnet Viper you need to also edit the LAN_0_DHCP_START and LAN_0_DHCP_END parameters in the configuration file to correspond with the IP address of this interface. The DNS address for the wireless clients to use can be specified in LAN_0_DNS.

After making changes to the /`config/hopling/virtual_gw/virtual_gw_0/lan/lan_0.conf` 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.

# 10 Xnet Viper in hotspot mode

The Xnet Viper has also an integrated **Access Controller** for public access networks. It combines the mesh networking from the Xnet Viper with a remotely configurable firewall to form a complete Access Controller for WiFi Hotspots in one box. One Xnet Viper in hotspot mode can serve up to 50 simultaneous users, depending on back bone capacity and user up- and download speeds. It takes control over authentication, accounting and routing users to the Internet. The integrated Access Controller can also serve remote Xnet Viper's or even off-the-shelve access points.

When the access controller is enabled on the Xnet Viper the Gateway is effectively divided into two halves. One halve is connected to the broadband (internet) connection and the other halve is used to connect to (wireless) customers. The two halves are separated by a firewall that can be remotely managed and customized by the network operator. The firewall stops all customer traffic until they are allowed through the firewall by the network operator. Authentication can take place in 3 different ways:

1. Remote authentication on the basis of Radius authentication.
2. Remote authentication using a remote web server that has direct control over the gateways' firewall through a VPN connection.
3. Local authentication through the use of a MAC access control list on the Gateway itself.

Customers that are not authenticated are blocked from accessing the network behind the firewall. The Xnet can be configured to redirect all valid subscribers to a Web portal or home page determined by the network operator.

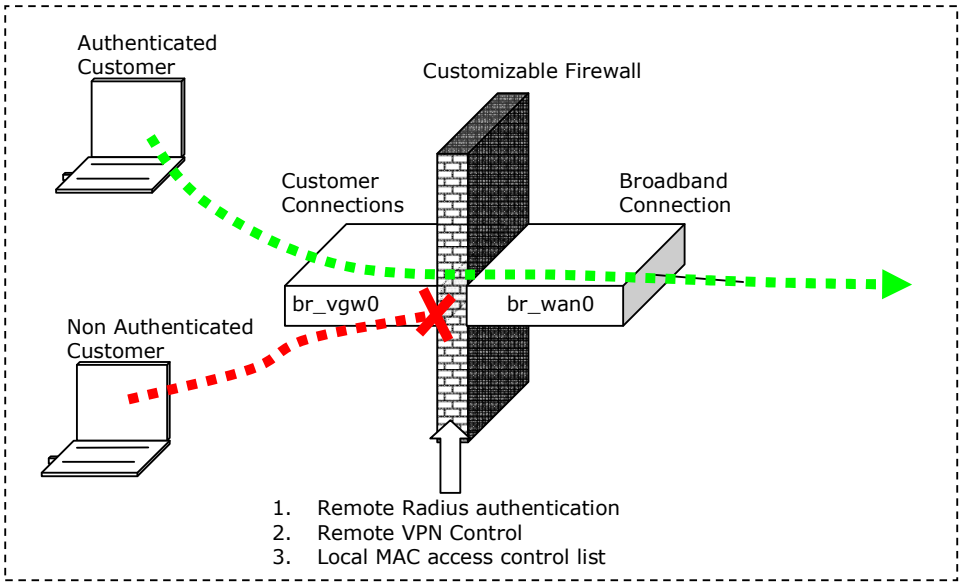



**Figure 27, Access controller functionality with remotely manageable firewall**

## 10.1 Access Control through Radius authentication

Radius (Remote Authentication Dial In User Service), defined in RFC 2865, is a protocol for remote user authentication and accounting. Radius enables centralized management of authentication data, such as usernames and passwords, access privileges, account limits and subscriber attributes.

When a customer attempts to access the internet through the Xnet, the router sends an http(s) request to a remote login page. The remote login page then gives a redirect to back to the Xnet that then generates an authentication request to the Radius server. The communication between the Radius client (the Xnet) and the Radius server are authenticated and encrypted through the use of a shared secret, which is not transmitted over the network. If the subscriber can be authenticated, the Radius server replies to the Xnet with a message instructing it to grant access to the customer.

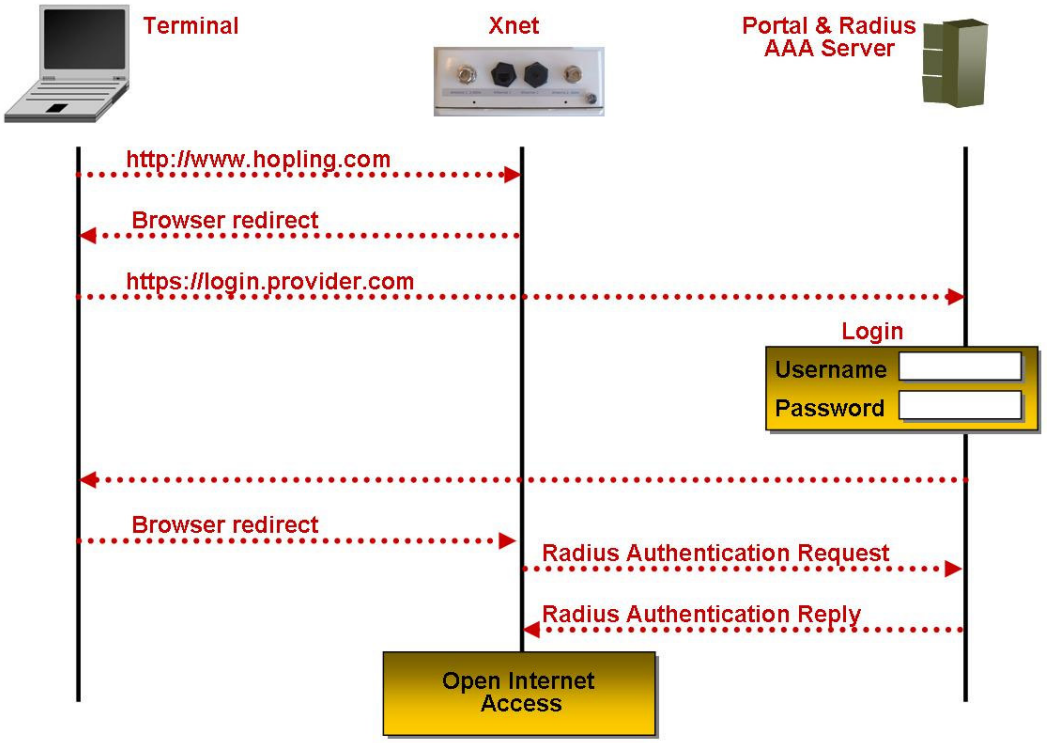
The Radius server may store the authentication data locally, but it can also store authentication data in an external SQL database or an external UNIX /etc/passwd file. The RADIUS server can also plug into a PAM (Pluggable Authentication Service) architecture to retrieve authentication data.

Optionally, the Radius server can instruct the Xspot to perform other functions; for example, the Radius server can tell the Xnet what upstream and downstream bandwidth the subscriber should receive. If RADIUS cannot authenticate the customer, it will instruct the Xnet to deny access to the network.

The Xnet Radius functionality can be broken down into the following three categories:

- Authentication-Request
- Authentication-Reply
- Accounting-Request

### 10.1.1 Radius Authentication Request




### 10.1.2 Setting up Radius Authentication

When Radius Authentication is enabled the Xnet sends the authentication request to the Radius Server. The Xnet Viper is set up to use Radius Authentication mode by modifying the parameters **AUTH_SERVER**, **AUTH_PORT** and **AUTH_SECRET** in the file
`/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/hotspot.conf`

As an example:

```
#@! <upload> <config> <reserved2> <reserved3> <reserved4>
#@$ <"Virtual Gateway 0: General parameters for hotspot mode">
#
# File: /config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/hotspot.conf
#
# Configuration file for the Hopling Xspot
#
# (c) Hopling Technologies 2004, 2005, 2006
# Ivo van Ling (support@hopling.com)
# Bas Muns
#
# Parameters for HOTSPOT mode
#
# In case the HOPLING_MODE is set to hotspot the hopling supports
# the following additional parameters

#@$ <"Parameters for Hotspot mode">
```

```
#@@ <REDIRECT_SERVER>   <HOST_IP>  <1>             <NONE>   <RESERVED>   <"Server to
redirect http and https request to">
#@@ <REDIRECT_URL>      <URL>      <1>             <NONE>   <RESERVED>   <"URL to
redirect to">
#@@ <REDIRECT_METHOD>   <DROPDOWN> <new,old>       <NONE>   <RESERVED>   <"Method
for generating HTTP redirects">

REDIRECT_SERVER="http://hopbase.hopling-services.net"
REDIRECT_URL="index.php"
REDIRECT_METHOD="new"

#@$ <"Parameters for MAC address access">
#@@ <ENABLE_MAC_LIST>   <DROPDOWN> <yes,no>  <NONE>   <RESERVED>   <"Enable MAC
access list">
#@@ <MAC_ACCESS_LIST>   <FILE>     <1>       <NONE>   <RESERVED>   <"List of MAC
addresses that are allowed to go through the firewall Special case is
ff:ff:ff:ff:ff:ff entry in MAC_ACCESS_LIST, which will allow ALL mac addresses to
pass">

ENABLE_MAC_LIST="no"
MAC_ACCESS_LIST="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/mac_access_lis
t.conf"

#@$ <"Allowed hosts">
#@@ <ALLOWED_HOSTS_WEB>    <FILE>     <1>       <NONE>   <RESERVED>   <"Sites that
may be visited for the web user group, without being logged in">
#@@ <ALLOWED_HOSTS_VOIP>   <FILE>     <1>       <NONE>   <RESERVED>   <"Sites that
may be visited for the voip user group, without being logged in">
#@@ <ALLOWED_HOSTS_VIRUS>  <FILE>     <1>       <NONE>   <RESERVED>   <"Sites that
may be visited for the virus user group, without being logged in">
#@@ <ALLOWED_HOSTS_OTHER>  <FILE>     <1>       <NONE>   <RESERVED>   <"Sites that
may be visited for the other user group, without being logged in">

ALLOWED_HOSTS_WEB="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/allowed_host
s.web.conf"
ALLOWED_HOSTS_VOIP="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/allowed_hos
ts.voip.conf"
ALLOWED_HOSTS_VIRUS="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/allowed_ho
sts.virus.conf"
ALLOWED_HOSTS_OTHER="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/allowed_ho
sts.other.conf"

#@$ <"Port black lists">
#@@ <ENABLE_BLACK_LIST_WEB>   <DROPDOWN>   <yes,no> <NONE>   <RESERVED>   <"Enable
port black list for web user group">
#@@ <PORT_BLACK_LIST_WEB>     <FILE>       <1>      <NONE>   <RESERVED>   <"List of
outgoing ports that are blocked, e.g. SUNRPC">
#@@ <ENABLE_BLACK_LIST_VOIP>  <DROPDOWN>   <yes,no> <NONE>   <RESERVED>   <"Enable
port black list for voip user group">
#@@ <PORT_BLACK_LIST_VOIP>    <FILE>       <1>      <NONE>   <RESERVED>   <"List of
outgoing ports that are blocked, e.g. SUNRPC">
#@@ <ENABLE_BLACK_LIST_VIRUS> <DROPDOWN>   <yes,no> <NONE>   <RESERVED>   <"Enable
port black list for virus user group">
#@@ <PORT_BLACK_LIST_VIRUS>   <FILE>       <1>      <NONE>   <RESERVED>   <"List of
outgoing ports that are blocked, e.g. SUNRPC">
#@@ <ENABLE_BLACK_LIST_OTHER> <DROPDOWN>   <yes,no> <NONE>   <RESERVED>   <"Enable
port black list for other user group">
#@@ <PORT_BLACK_LIST_OTHER>   <FILE>       <1>      <NONE>   <RESERVED>   <"List of
outgoing ports that are blocked, e.g. SUNRPC">

ENABLE_BLACK_LIST_WEB="yes"
PORT_BLACK_LIST_WEB="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/port_black
_list.web.conf"
ENABLE_BLACK_LIST_VOIP="yes"
PORT_BLACK_LIST_VOIP="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/port_blac
k_list.voip.conf"
ENABLE_BLACK_LIST_VIRUS="yes"
PORT_BLACK_LIST_VIRUS="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/port_bla
ck_list.virus.conf"
ENABLE_BLACK_LIST_OTHER="yes"
PORT_BLACK_LIST_OTHER="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/port_bla
ck_list.other.conf"

#@$ <"Port white lists">
#@@ <ENABLE_WHITE_LIST_WEB>   <DROPDOWN>   <yes,no> <NONE>   <RESERVED>   <"Enable
port white list for web user group">
#@@ <PORT_WHITE_LIST_WEB>     <FILE>       <1>      <NONE>   <RESERVED>   <"List of
outgoing ports that are allowed, e.g. HTTP">
#@@ <ENABLE_WHITE_LIST_VOIP>  <DROPDOWN>   <yes,no> <NONE>   <RESERVED>   <"Enable
port white list for voip user group">
#@@ <PORT_WHITE_LIST_VOIP>    <FILE>       <1>      <NONE>   <RESERVED>   <"List of
outgoing ports that are allowed, e.g. HTTP">
#@@ <ENABLE_WHITE_LIST_VIRUS> <DROPDOWN>   <yes,no> <NONE>   <RESERVED>   <"Enable
port white list for virus user group">
```

```
#@@ <PORT_WHITE_LIST_VIRUS>   <FILE>       <1>      <NONE>   <RESERVED>   <"List of
outgoing ports that are allowed, e.g. HTTP">
#@@ <ENABLE_WHITE_LIST_OTHER> <DROPDOWN>   <yes,no> <NONE>   <RESERVED>   <"Enable
port white list for other user group">
#@@ <PORT_WHITE_LIST_OTHER>   <FILE>       <1>      <NONE>   <RESERVED>   <"List of
outgoing ports that are allowed, e.g. HTTP">

ENABLE_WHITE_LIST_WEB="no"
PORT_WHITE_LIST_WEB="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/port_white
_list.web.conf"
ENABLE_WHITE_LIST_VOIP="no"
PORT_WHITE_LIST_VOIP="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/port_whit
e_list.voip.conf"
ENABLE_WHITE_LIST_VIRUS="no"
PORT_WHITE_LIST_VIRUS="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/port_whi
te_list.virus.conf"
ENABLE_WHITE_LIST_OTHER="no"
PORT_WHITE_LIST_OTHER="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/port_whi
te_list.other.conf"

#@$ <"Blocked subnets">
#@@ <ENABLE_BLOCKED_SUBNET_LIST> <DROPDOWN>   <yes,no> <NONE>   <RESERVED>
<"Enable blocking subnet after being logged in">
#@@ <BLOCKED_SUBNET_LIST>        <FILE>       <1>      <NONE>   <RESERVED>   <"List
of blocked subnets">

ENABLE_BLOCKED_SUBNET_LIST="no"
BLOCKED_SUBNET_LIST="/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/blocked_su
bnet_list.conf"

#@$ <"Accounting parameters for Radius and http(s)">
#@@ <ENABLE_ACCOUNTING> <DROPDOWN>  <yes,no>             <NONE>   <RESERVED>
<"Enable accounting">
#@@ <ACCOUNTING_METHOD> <DROPDOWN>  <http,https,radius>  <NONE>   <RESERVED>
<"Accounting method">
#@@ <ACCOUNTING_SERVER> <HOST_IP>   <1>                  <NONE>   <RESERVED>
<"Server to send accounting messages to. This can be the http(s) or Radius server">
#@@ <ACCOUNTING_PORT>   <PORT>      <1>                  <NONE>   <RESERVED>
<"Port number for Radius accounting">
#@@ <ACCOUNTING_SECRET> <STRING>    <0,128>              <NONE>   <RESERVED>
<"Shared secret for the Radius accounting server">
#@@ <ACCOUNTING_URL>    <URL>       <1>                  <NONE>   <RESERVED>   <"URL
for http or https accounting">
#@@ <INTERIM_INTERVAL>  <INT>       <0,10000>            <NONE>   <RESERVED>
<"Default Accounting Interim interval in seconds.">
#@@ <LOCATION_ID>       <STRING>    <1,253>              <NONE>   <RESERVED>
<"Location id. Specific attribute according to WISPr">
#@@ <LOCATION_NAME>     <STRING>    <1,253>              <NONE>   <RESERVED>
<"Location name. Specific attributes according to WISPr">

ENABLE_ACCOUNTING="yes"
ACCOUNTING_METHOD="http"
ACCOUNTING_SERVER="updater.hopling.com"
ACCOUNTING_PORT="80"
ACCOUNTING_SECRET="testing123"
ACCOUNTING_URL="unconfigured/bas_test.php"
INTERIM_INTERVAL="60"
LOCATION_ID="Hopling_Almere"
LOCATION_NAME="Binderij_65"

#@$ <"Authentication parameters for Radius">
#@@ <AUTH_SERVER>       <HOST_IP>   <1>                  <NONE>   <RESERVED>
<"Server to send optional Radius authentication messages">
#@@ <AUTH_PORT>         <PORT>      <1>                  <NONE>   <RESERVED>
<"Port number for optional Radius authentication">
#@@ <AUTH_SECRET>       <STRING>    <0,128>              <NONE>   <RESERVED>
<"Shared secret for Radius authentication server">
#@@ <AUTH_NASID>        <STRING>    <0,253>              <NONE>   <RESERVED>   <"Set
NASID or leave empty. If empty the hostname will be used as NASID">

AUTH_SERVER="82.148.221.131"
AUTH_PORT="1812"
AUTH_SECRET="testing123"

#@$ <"Parameters for HOTSPOT user management">
#@@ <SESSION_TIMEOUT>      <INT>       <0,10000>         <NONE>   <RESERVED>
<"Default value for session time out in seconds">
#@@ <IDLE_TIMEOUT>         <INT>       <0,10000>         <NONE>   <RESERVED>
<"Default value for idle time out in seconds">
#@@ <ENABLE_BW_CONTROL>    <DROPDOWN>  <yes,no>          <NONE>   <RESERVED>
<"Enable bandwidth control">
#@@ <BANDWIDTH_MAX_UP>     <INT>       <0,2000000>       <NONE>   <RESERVED>
<"Maximum transmit rate per user (kilobits/s). Bandwidth is given in kilobits per
second">
```

```
#@@ <BANDWIDTH_MAX_DOWN>   <INT>       <0,2000000>       <NONE>   <RESERVED>
<"Maximum receive rate per user (kilobits/s). Bandwidth is given in kilobits per
second">
#@@ <VIRUS_DETECT>         <INT>       <0,10000>         <NONE>   <RESERVED>
<"Number of simultaneous tcp/ip sessions per minute allowed for a single user. When
set to 0 the user is allowed an unlimited amount of sessions">
#@@ <VIRUS_ACTION>         <STRING>    <0,253>           <NONE>   <RESERVED>
<"Script to call when the virus detection is triggered">

SESSION_TIMEOUT="14400"
IDLE_TIMEOUT="600"
ENABLE_BW_CONTROL="yes"
BANDWIDTH_MAX_UP="10240"
BANDWIDTH_MAX_DOWN="10240"
VIRUS_DETECT="100"
VIRUS_ACTION="/hopling/bin/virusDetect"

#@$ <"Parameters for HOTSPOT local services">
#@@ <LOCAL_SERVICES>      <PORT>       <25>              <SPACESEP> <RESERVED>
<"Accept incoming requests to the following ports from the wireless network">

LOCAL_SERVICES="22"

# End
```

### 10.1.3 Timeout Detection

If a customer is sending traffic through the Xnet Viper, it will immediately detect a Session-Timeout. However in the case of an Idle-Timeout or an inactive subscriber Session-Timeout, the Xnet Viper will detect this with an accuracy of 10 seconds.

### 10.1.4 Interim Accounting Updates

The Xnet Viper parses the attribute Acct-Interim-Interval in an Access-Accept. If this attribute is present the Xnet Viper sends every [Acct-Interim-Interval] seconds a Radius Accounting Interim message for the specific subscriber. If this attribute is not present or equal to 0, no Interim message is sent. The precision is 10 seconds. The Xnet Viper will not send Interim messages more frequently than every 10 seconds.

## 10.2 Access Control through VPN connection

The Access Controller in the Xnet Viper can be controlled through a centralized (portal) server that is installed in the operators back office. This server sends instructions to 'open' and 'close' the firewall of the access controller through a secure VPN control channel. Currently the access controller supports two types of VPN; PPTP tunnels and PPP over SSH tunnels.

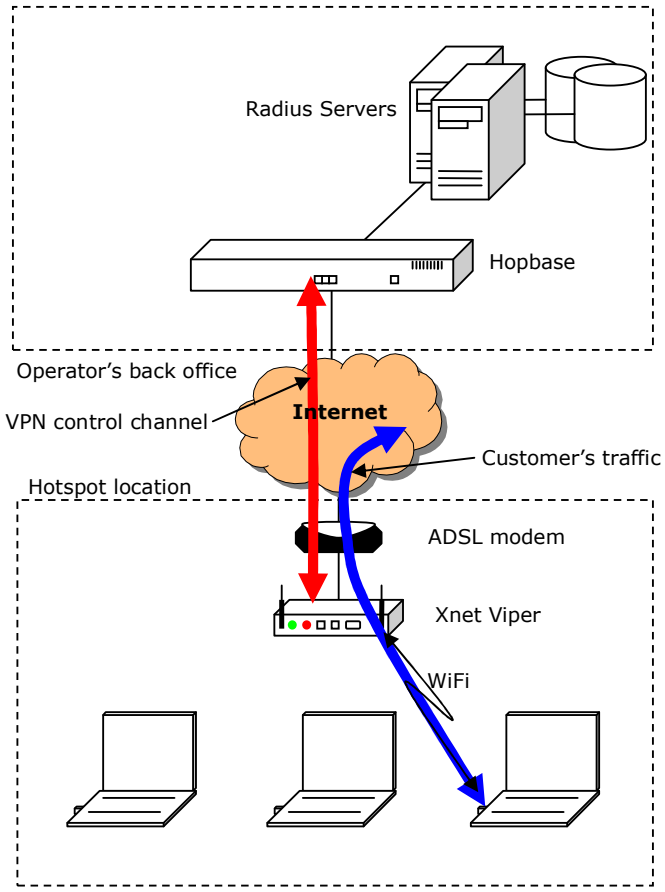



**Figure 28, Typical Hotspot with VPN control channel between back office and Xnet**

The VPN tunneling mechanism between the back office and the Xnet Viper is required for 2 reasons:

1. Security. The messages between the Xnet Viper and the back office are encrypted, either by MPPE or by SSH.
2. Bidirectional traffic between the Xnet Viper and the back office system is possible even when firewalls and NAT devices (ADSL modems) block incoming traffic.

The Xnet Viper in hotspot mode will connect to the back office servers simply by plugging it in any wired Ethernet network. The Hopling will start 'calling home' as soon as it is connected to the internet.

The first Virtual Gateway in the Xnet Viper is set to "hotspot" mode by modifying the parameter **`VGW_0_MODE`** in the file **`/config/hopling/virtual_gw/virtual_gw_0/virtual_gw.0.conf`**

As an example:

```
#@! <upload> <config> <reserved2> <reserved3> <reserved4>
#@$ <"Virtual Gateway 0: Configuration parameters">
#
# File:/config/hopling/virtual_gw/virtual_gw_0/virtual_gw_0.conf
#
# Configuration file for the Virtual Gateway interfaces
# (c) Hopling Technologies 2004, 2005, 2006
# Bas Muns
#
# This file is used to configure Virtual Gateway interface 0.
#
# Here you can specify the parameters that are unique per Virtual GW,
# and which interfaces are added to the Virtual GW.
#

#@$ <"General parameters">
#@@ <VGW_0_ENABLE>      <DROPDOWN>  <yes,no>          <NONE>   <RESERVED>  <"Enable
this interface. If disabled all other settings are ignored">
#@@ <VGW_0_MODE>        <DROPDOWN>  <hopling,hotspot> <NONE>   <RESERVED>
<"hotspot: become a local hotspot. hopling: act as an access point">

VGW_0_ENABLE="yes"
VGW_0_MODE="hotspot"

#@$ <"Log parameters">
#@@ <VGW_0_LOG_SERVER>  <HOST_IP>   <1>              <NONE>   <RESERVED>  <"Server
to use for logging events">
#@@ <VGW_0_LOG_URL>     <URL>       <1>              <NONE>   <RESERVED>  <"URL to
call to log events through XML">

VGW_0_LOG_SERVER="http://hopman.hopling-services.net"
VGW_0_LOG_URL="hopman/log.php"

#@$ <"Parameters for the VPN client interface">
#@@ <VGW_0_ENABLE_VPN>     <DROPDOWN>  <yes,no>       <NONE>      <RESERVED>
<"Enable tunneling to a VPN tunnel server">
#@@ <VGW_0_VPN_TYPE>       <DROPDOWN>  <pptp,pppssh>  <NONE>      <RESERVED>
<"VPN type. pptp: connection is made via the Point to Point Tunneling protocol.
pppssh: connection will be made by tunneling Point-to-Point Protocol over a Secure
SHell (SSH) connection">
#@@ <VGW_0_VPN_SSH_NAME>   <STRING>    <0,128>        <NONE>      <RESERVED>
<"This is the user name for the SSH server">
#@@ <VGW_0_VPN_SERVER>     <HOST_IP>   <1>            <NONE>      <RESERVED>
<"This is the hostname, or IP address for the VPN (pptp or ssh) server">
#@@ <VGW_0_VPN_USER>       <STRING>    <0,128>        <NONE>      <RESERVED>
<"This is the user name for the VPN server">
#@@ <VGW_0_VPN_SECRET>     <STRING>    <0,128>        <NONE>      <RESERVED>
<"This is the password for the VPN server">
#@@ <VGW_0_VPN_LOC_IP>     <IP>        <1>            <WILDCARD>  <RESERVED>
<"This is the IP address of the local VPN tunnel. Can be set to "*" if the VPN
server allocates the IP addresses dynamically (only for pptp method)">
#@@ <VGW_0_VPN_REM_IP>     <IP>        <1>            <WILDCARD>  <RESERVED>
<"This is the IP address of the remote end of the VPN tunnel. Can be set to "*" if
the VPN server allocates the IP addresses dynamically (only for pptp method)">
#@@ <VGW_0_VPN_ADD_ROUTE>  <DROPDOWN>  <yes,no>       <NONE>      <RESERVED>
<"Set to yes if you want to add route(s) for the VPN interface">
#@@ <VGW_0_VPN_ROUTE>      <IP_MASK>   <5>            <SPACESEP>  <RESERVED>
<"These are the IP address(es) and netmask(s) for which a route needs to be added.
It needs to be in the format IP-address/Netmask.">

VGW_0_ENABLE_VPN="yes"
VGW_0_VPN_TYPE="pppssh"
VGW_0_VPN_SSH_NAME="vpn"
VGW_0_VPN_SERVER="vpn1.hopling-services.net vpn2.hopling-services.net"
VGW_0_VPN_USER="00:08:a2:01:c8:22"
VGW_0_VPN_SECRET="hoplingtech01"
VGW_0_VPN_LOC_IP="192.168.160.23"
VGW_0_VPN_REM_IP="192.168.160.5"
VGW_0_VPN_ADD_ROUTE="yes"
VGW_0_VPN_ROUTE="192.168.160.0/255.255.240.0"

#@$ <"Parameters for the NOC interface">
#@@ <VGW_0_ENABLE_NOC>  <DROPDOWN>  <yes,no>    <NONE>              <RESERVED>
<"Enable NOC interface mechanism">
#@@ <VGW_0_NOC_TYPE>    <DROPDOWN>  <picopoint> <NONE>              <RESERVED>
<"NOC interface mechanism">
#@@ <VGW_0_NOC_AUTH>    <DROPDOWN>  <ip,ssl>    <NONE>              <RESERVED>
<"NOC authentication mechanism. ip: the IP list VGW_0_ENABLE_NOC_IP will be used as
allowed NOC servers. ssl: the certificate in VGW_0_ENABLE_NOC_CERT and
VGW_0_ENABLE_NOC_CACERT will be used to authenticate the NOC server">
```

```
#@@ <VGW_0_NOC_PORT>    <PORT>      <1>         <NONE>               <RESERVED>
<"Port number the NOC will use for controlling user authentication">
#@@ <VGW_0_NOC_IP>      <IP>        <5>         <SPACESEP|WILDCARD>  <RESERVED>
<"IP addresses of NOC portals allowed on this port. Multiple IP addresses can be
added separated by a space. Leave empty to allow any IP on the NOC port">
#@@ <VGW_0_NOC_CERT>    <FULLURL>   <1>         <WILDCARD>           <RESERVED>
<"URL of the certificate to use when using NOC_AUTH mechanism ssl">
#@@ <VGW_0_NOC_CACERT>  <FULLURL>   <1>         <WILDCARD>           <RESERVED>
<"URL of the certificate authority (CA) to use when using NOC_AUTH mechanism ssl">
#@@ <VGW_0_NOC_NASID>   <STRING>    <0,128>     <NONE>               <RESERVED>
<"The NASID to use in the radius authentication messages. Note: Radius accounting
and athentication settings can be found in hotspot_mode/hotspot.conf file">

VGW_0_ENABLE_NOC="no"
VGW_0_NOC_TYPE="picopoint"
VGW_0_NOC_AUTH="ip"
VGW_0_NOC_PORT="8043"
VGW_0_NOC_IP="193.67.189.182"
VGW_0_NOC_CERT="https://www.hopling.com/xyz/hopling.cert"
VGW_0_NOC_CACERT="https://www.hopling.com/xyz/hopling_ca.cert"

# End
```

When Virtual Gateway 0 in Xnet Viper is set to “hotspot” mode then the Xnet Viper will have a firewall setup between the wireless interface and the rest of the network. The firewall stops all customer traffic until it is specifically instructed to open a hole for that specific customer. This is done on the basis of IP and MAC address of the customer. That means that nobody can get any further than the wireless interface on the Xnet Viper until instructed by a central server.

### 10.2.1 Setting up the VPN tunnel between Xnet and Back Office

You have to instruct the Hopling to open up the firewall for each individual customer. You can open and close the firewall remotely by sending the appropriate commands through a VPN tunnel. This VPN tunnel will have to be setup between each Virtual Gateway in the Xnet Viper and the machine you use to send the "open" and "close" commands in the back office. Normally this machine would be the Hopbase in combination with the Hoptun.

So in order for this to work you will have to have a management VPN tunnel to each Xnet Viper. You can specify to use a VPN tunnel in the file

`/config/hopling/virtual_gw/virtual_gw_0 virtual_gw.0.conf.`

Set the parameter **`VGW_0_ENABLE_VPN`** (near the bottom of the file) to "yes".

Example for Hopling Technologies VPN server:

```
#@$ <"Parameters for the VPN client interface">
#@@ <VGW_0_ENABLE_VPN>     <DROPDOWN>  <yes,no>       <NONE>      <RESERVED>
<"Enable tunneling to a VPN tunnel server">
#@@ <VGW_0_VPN_TYPE>       <DROPDOWN>  <pptp,pppssh>  <NONE>      <RESERVED>
<"VPN type. pptp: connection is made via the Point to Point Tunneling protocol.
pppssh: connection will be made by tunneling Point-to-Point Protocol over a Secure
SHell (SSH) connection">
#@@ <VGW_0_VPN_SSH_NAME>   <STRING>    <0,128>        <NONE>      <RESERVED>
<"This is the user name for the SSH server">
#@@ <VGW_0_VPN_SERVER>     <HOST_IP>   <1>            <NONE>      <RESERVED>
<"This is the hostname, or IP address for the VPN (pptp or ssh) server">
#@@ <VGW_0_VPN_USER>       <STRING>    <0,128>        <NONE>      <RESERVED>
<"This is the user name for the VPN server">
#@@ <VGW_0_VPN_SECRET>     <STRING>    <0,128>        <NONE>      <RESERVED>
<"This is the password for the VPN server">
#@@ <VGW_0_VPN_LOC_IP>     <IP>        <1>            <WILDCARD>  <RESERVED>
<"This is the IP address of the local VPN tunnel. Can be set to "*" if the VPN
server allocates the IP addresses dynamically (only for pptp method)">
#@@ <VGW_0_VPN_REM_IP>     <IP>        <1>            <WILDCARD>  <RESERVED>
<"This is the IP address of the remote end of the VPN tunnel. Can be set to "*" if
the VPN server allocates the IP addresses dynamically (only for pptp method)">
#@@ <VGW_0_VPN_ADD_ROUTE>  <DROPDOWN>  <yes,no>       <NONE>      <RESERVED>
<"Set to yes if you want to add route(s) for the VPN interface">
#@@ <VGW_0_VPN_ROUTE>      <IP_MASK>   <5>            <SPACESEP>  <RESERVED>
<"These are the IP address(es) and netmask(s) for which a route needs to be added.
It needs to be in the format IP-address/Netmask.">
```

```
VGW_0_ENABLE_VPN="yes"
VGW_0_VPN_TYPE="pppssh"
VGW_0_VPN_SSH_NAME="vpn"
VGW_0_VPN_SERVER="vpn1.hopling-services.net vpn2.hopling-services.net"
VGW_0_VPN_USER="00:08:a2:01:c8:22"
VGW_0_VPN_SECRET="hoplingtech01"
VGW_0_VPN_LOC_IP="192.168.160.23"
VGW_0_VPN_REM_IP="192.168.160.5"
VGW_0_VPN_ADD_ROUTE="yes"
VGW_0_VPN_ROUTE="192.168.160.0/255.255.240.0"
```

- VGW_0_VPN_SERVER is the public IP address of the VPN server. In this case it is the public IP address of the Hopling Technologies VPN server.
- VGW_0_VPN_SECRET is the password for the VPN user. As username normally the hostname of the Hopling is sent.

So in this example when logging in the Hopling would try to log in with username: XnetMKII-c3a124 and password: hoplingtech01.

### 10.2.2 Hopling control messages between Xnet and back office

Between the Xnet Viper and the back office, control messages are exchanged using HTTP GET. Browser redirect messages from the Xnet Viper to the back office are sent through the internet using https and control messages from the back office to the Xnet Viper are sent through the secure VPN tunnel.

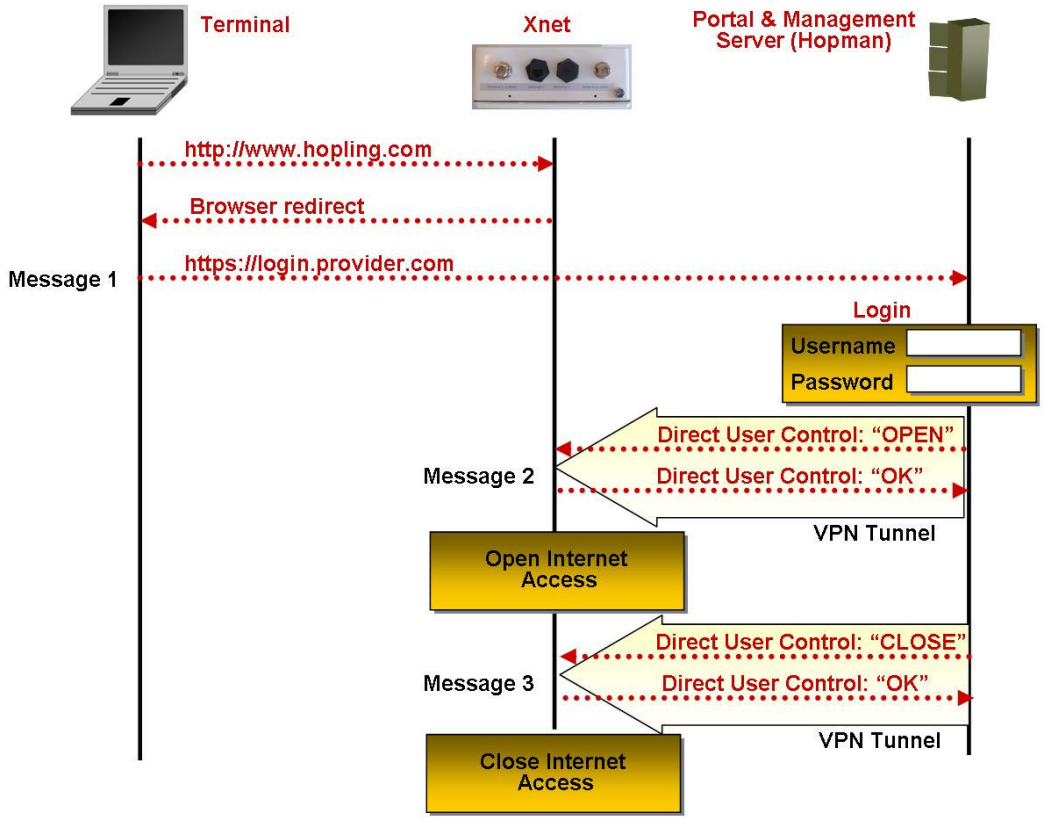



**Figure 29, HTTP message exchange between Xnet Viper and back office**

### 10.2.3 Browser redirect message (message 1)

1. When a customer opens the browser and attempts to surf to any http or https website, the Hopling redirects the browser to a specific portal page: the so-called portal push page.

2. The Hopling adds its own query string in the redirection operation. This query string contains the following information:

| | |
|---|---|
| - cust_MAC | is the MAC address of the customer's laptop, desktop or PDA. |
| - cust_IP | is the IP address of the customer's laptop, desktop or PDA. |
| - cust_URL | the original URL the customer intended to visit. |
| - gateway_ID | the unique gateway ID. For the Xnet Viper-IV this will be XnetVpIV-c36c74, where c36c74 are the last 6 octets of the first Ethernet port of the device. |
| - gateway_VER | the software version the gateway is running. |
| - tunnel_IP | the IP address of the VPN tunnel end point on the Xnet Viper-I. |

For example, the Xnet Viper redirects the customer's browser to the web portal of Hopling Technologies with the following link:

```
https://82.148.221.131/remote_login/hopling_default.php?cust_MAC=00:02:2D:42:4B:1C&c
ust_IP=192.168.0.11&cust_URL=http%3A%2F%2Fwww.google.com%2F&gateway_ID= XnetVpIV-
c36c74&gateway_VER=3.0.1&tunnel_IP=10.16.0.15
```

The query string of the redirect message is configurable through the "redirect" event file. Please see chapter 11.2.9 for a description of all parameters that can be sent in the redirect event.

The query string can be used in the back office or web portal to determine which Xnet Viper the customer is connected to and what website the customer intended to visit.

### 10.2.4 User Authentication (message 2)

1. After the customer is successfully logged in on the portal page, the back office executes an HTTP GET to the requesting Xnet Viper by calling the URL: http://tunnel_ip/authorizeUser.php through the VPN tunnel.

2. The actual HTTP IP traffic for the GET command is directed over the VPN tunnel, running between the Xnet Viper and the back office.

3. In message 1, the VPN tunnel IP address of the requesting Xnet Viper-I was included, which can be used to call the Xnet Viper-I over the VPN tunnel.

4. Message 2 must contain the following mandatory information:

| | |
|---|---|
| - tunnel_IP | is the IP address of the VPN tunnel end point on the Hopling. |
| - action | can be either "**open**" or "**close**". |
| - cust_MAC | is the MAC address of the customer's device. |
| - cust_IP | is the IP address of the customer's device. |

Message 2 may contain the following optional parameters: