11.2.10 Event: uploadConfig

The portal server can signal to the Xnet Viper to send the current configuration to the CONFIG server after it receives a hoplingBoot event. This is done by sending back an uploadConfig command in the response to the http GET call. See also paragraph 11.2.5.

The parameters sent in the uploadConfig event can be configured in the corresponding uploadConfig event file. The event file is found in the directory:

```
/config/hopling/virtual_gw/virtual_gw_0/events.
```

The following are the factory default values that are set.

```
#-------------------------------------------------------------------------+
#                                                                         |
# file: config/hopling/virtual_gw/virtual_gw_0/events/uploadConfig        |
#                                                                         |
# Configuration file for the Xnet Viper                                 |
# Hopling Technologies (c) 2004, 2005                                     |
# Ivo van Ling (support@hopling.com)                                    |
#                                                                         |
# This file contains the configuration parameters for the "getConfig"     |
# event.                                                                  |
#                                                                         |
# Last manual update : 06 April 2005                                      |
#                                                                         |
#-------------------------------------------------------------------------+
#
# These are the Hopling Technologies parameters
# Event name
#TITLE="configuration parameters for the uploadConfig event."
#START
event uploadConfig

# Additional Hopling parameters
gateway_ID $GATEWAY_ID
software_VER $SW_VERSION
platform_VER $HW_PLATFORM
macEth0 $MAC_ETH0
ipEth0 $BR_WAN0_IP
macEth1 $MAC_ETH1
ipEth1 $BR_VGW0_IP
macWlan0 $WIFI_0_MAC
ipWlan0 $WIFI_0_IP
wireless_NET $WIFI_0_SSID
```

When an uploadConfig event is generated with the above configuration for the uploadConfig event the following URL is called from the Xnet Viper:

```
http://www.hopling.nl/download_config/log.php?date=20050904193535&hopling=XnetMkI-
c20930&event=uploadConfig&gateway_ID=&software_VER=3.0.1&platform_VER=Net4511&macEth0=00:00:24:c
2:09:30&ipEth0=192.168.10.202&macEth1=00:00:24:c2:09:31&ipEth1=192.168.0.1&macWlan0=00:0c:84:01:
31:8c&ipWlan0=&wireless_NET=Hopling Technologies 0&
```

At the same time the configuration of the Xnet Viper is sent to the portal web server by POSTing the configuration data in a FORM through this URL.

For example, the contents of the file /config/hopling/hopling.conf are POSTed to the portal server like this:

```
VERSION=3.0.1
CONFIG_METHOD=auto
CONFIG_SERVER=http://www.hopling.nl
CONFIG_URL=download_config/factory_defaults.php
LOG_SERVER=http://www.hopling.nl
LOG_URL=download_config/log.php
HOST_NAME=
GATEWAY_ID=
LOCATION_ID=
SUPPLY_DNS=yes
ENABLE_AP_MON=yes
AP_DETECT=600
```

```
ENABLE_GW_MON=no
GW_DETECT=600
NTP_SERVERS=ntp.xs4all.nl%20194.109.218.162
```

The contents of the following configuration files get POSTed during this event:

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

/config/hopling/virtual_gw/virtual_gw_0/virtual_gw_0.conf
/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/hotspot.conf
/config/hopling/virtual_gw/virtual_gw_0/lan/lan_0.conf
/config/hopling/virtual_gw/virtual_gw_0/wan/wan_0.conf
/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0_0.conf
/config/hopling/virtual_gw/virtual_gw_1/virtual_gw_1.conf
/config/hopling/virtual_gw/virtual_gw_1/hotspot_mode/hotspot.conf
/config/hopling/virtual_gw/virtual_gw_1/lan/lan_1.conf
/config/hopling/virtual_gw/virtual_gw_1/wan/wan_1.conf
/config/hopling/virtual_gw/virtual_gw_1/wifi/wifi_0_1.conf
/config/hopling/virtual_gw/virtual_gw_2/virtual_gw_2.conf
/config/hopling/virtual_gw/virtual_gw_2/hotspot_mode/hotspot.conf
/config/hopling/virtual_gw/virtual_gw_2/lan/lan_2.conf
/config/hopling/virtual_gw/virtual_gw_2/wan/wan_3.conf
/config/hopling/virtual_gw/virtual_gw_2/wifi/wifi_0_2.conf
/config/hopling/virtual_gw/virtual_gw_3/virtual_gw_3.conf
/config/hopling/virtual_gw/virtual_gw_3/hotspot_mode/hotspot.conf
/config/hopling/virtual_gw/virtual_gw_3/lan/lan_3.conf
/config/hopling/virtual_gw/virtual_gw_3/wan/wan_3.conf
/config/hopling/virtual_gw/virtual_gw_3/wifi/wifi_0_3.conf
/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_0.general.conf

On Xnet Viper-II systems also:
/config/hopling/wifi_backbone/wifi_backbone_1/neighbors_1.conf
/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_1.general.conf
/config/hopling/virtual_gw/virtual_gw_0/wifi/wifi_1_0.conf
/config/hopling/virtual_gw/virtual_gw_1/wifi/wifi_1_1.conf
/config/hopling/virtual_gw/virtual_gw_2/wifi/wifi_1_2.conf
/config/hopling/virtual_gw/virtual_gw_3/wifi/wifi_1_3.conf
```

This event can only use the general event parameters. No additional parameters are available for this event.

11.2.11 Event: virusDetect

The Xnet Viper has a way of detecting worm viruses passing through the gateway. Viruses like the Nimba, Sasser and other worm viruses have a typical behavior in that they open up a large number of simultaneous TCP/IP connections to start infecting other systems. The Xnet Viper can determine the number of sessions that each user has opened per minute. For non infected user systems the number of simultaneous connections will normally not be higher than 50. However, a worm virus can easily open over 100 simultaneous TCP/IP connections. The way of detecting worm viruses works on the basis of setting a threshold for simultaneous TCP/IP connections. Once this threshold is exceeded for a particular user the Xnet Viper will signal this to the portal by generating the virusDetect event. At that point the portal server can decide what to do, either log the user out, place the user in the restricted virus queue or do nothing.

The threshold to trigger the virusDetect event is default set to 100 simultaneous TCP/IP sessions per minute. This is done using the variable `VIRUS_DETECT="100"` in the file: `/config/hopling/virtual_gw/virtual_gw_0/hotspot_mode/hotspot.conf`. When the variable is set to zero the number of simultaneous sessions will be set to unlimited.

The default value for the VIRUS_DETECT threshold can be set on a per user basis by the remote portal upon the authentication of the user. Please refer to paragraph: 10.2.4 on how to set this during authentication.

```
#@! <upload> <event> <reserved2> <reserved3> <reserved4>
#@$ <"Virtual Gateway 0: Event file for the virusDetect event">
#
# file:/config/hopling/virtual_gw/virtual_gw_0/events/virusDetect
#
# Configuration file for the Hopling Xspot
# (c) Hopling Technologies 2004, 2005, 2006
# Ivo van Ling (support@hopling.com)
#
# This file contains the configuration parameters for the "virusDetect" event.
#
# Event name
#TITLE="configuration parameters for the virusDetect event."
#START
event virusDetect

# Additional parameters
gateway_ID $CLIENT_STRING
software_VER $SW_VERSION
flavour $FLAVOUR
flavour_type $FLAVOUR_TYPE
build_nr $BUILD_NR
build_tag $BUILD_TAG
platform_VER $HW_PLATFORM
platform_TYPE $HW_TYPE
macEth0 $MAC_ETH0
wireless_NET $WIFI_0_0_SSID
vpn_server $VGW_0_VPN_SERVER
cust_MAC $CUST_MAC
cust_IP $CUST_IP
```

When a virusDetect event is generated with the above configuration for the virusDetect event the following URL is called from the Xnet Viper:

```
http://www.hopling.nl/download_config/log.php?date=20050904202755&hopling=XnetMkI-
c20930&event=virusDetect&gateway_ID=&software_VER=3.0.1&platform_VER=Net4511&platform_TYPE=PRISM
WWR&macEth0=00:00:24:c2:09:30&cust_MAC=00:12:3f:15:09:62&cust_IP=192.168.0.11&wireless_NET=Hopli
ng Technologies 0
```

The virusDetect event can contain a large number of additional parameters. Below is a list of parameters that are specific for the virusDetect event that can be used to customize the virusDetect event:

virusDetect specific Parameters	Description
$CUST_MAC	The MAC address of the user's Wifi device, for example: 00:12:80:0d:45:6c
$CUST_IP	The IP address of the user's Wifi device, for example 192.168.0.11
$CUST_DHCP	The DHCP client name of the user's Wifi device if set by the operating system. For example: ivo's laptop.
$CUST_VGW	The Virtual Gateway the user is logged in to. Possible values 0 to 3 (zero to three).
$CUST_TYPE	The type of customer that is generating the virusDetect event. Possible values are: - **web**, normal user browsing the internet. - **voip**, user with a VoIP device, such as WiFi telephone. - **virus**, user that has been placed in a restricted area because of being infected by a virus. - **other**, user definable queue.
$IDLE_TIMEOUT	The setting of the idle timeout value. Default value is set to 10 minutes (600 seconds).
$IDLE_TIME	The value of the idle timer the virusDetect occurs
$SESSION_TIMEOUT	The setting of the session timeout value. Default value is set to 14400 seconds (4 hours).
$SESSION_TIME	The value of the session timer when the virusDetect timeout occurs.
$INTERIM_INTERVAL	
$SESSION_START	The UNIX system time when the user's session started. For example: 1125675940
$BYTES_UP	The number of bytes the user has sent upstream since the beginning of the session.
$BYTES_DOWN	The number of bytes the user has received since the beginning of the session
$BANDWIDTH_MAX_UP	The maximum upload speed the user is allowed to use during this session. Specified in kilobits per second.
$BANDWIDTH_MAX_DOWN	The maximum download speed the user is allowed to use during this session. Specified in kilobits per second.
$MAX_SESSIONS	Number of concurrent TCP/IP sessions per minute the user is allowed to consume
$CUR_SESSIONS	Number of concurrent TCP/IP sessions per minute the used has at the time of the virus detect event

12 Xnet call home functionality and XML interface

Using Hopling Technologies' XML-driven Auto Configuration functionality utilizes the existing infrastructure of a mobile operator to provide an effortless and rapid method for configuring devices for fast network roll-outs. Once configured, this methodology can also be effectively used to centrally manage configuration profiles for all Hopling devices in the public access network.

12.1 Xnet auto configuration description

Upon system boot the Xnet Viper will contact the operator's portal on a specific logging URL to announce the "boot" event (see chapter: 11.2.5). After the "boot" event the Xnet Viper can send the "getConfig" event (see chapter: 11.2.4). The portal server can then decide to start uploading configuration information to the Xnet Viper using XML. If no XML information is sent, the Xnet Viper will finish the boot process and become active.

However, the portal server can decide to upload configuration elements using XML to the Xnet Viper. The Xnet Viper then compares the information it received with its current configuration. If the Xnet Viper received one or more configuration elements that are different from its current configuration it will update the configuration files. After the update of the configuration files the Xnet Viper will automatically reboot and the process repeats itself.

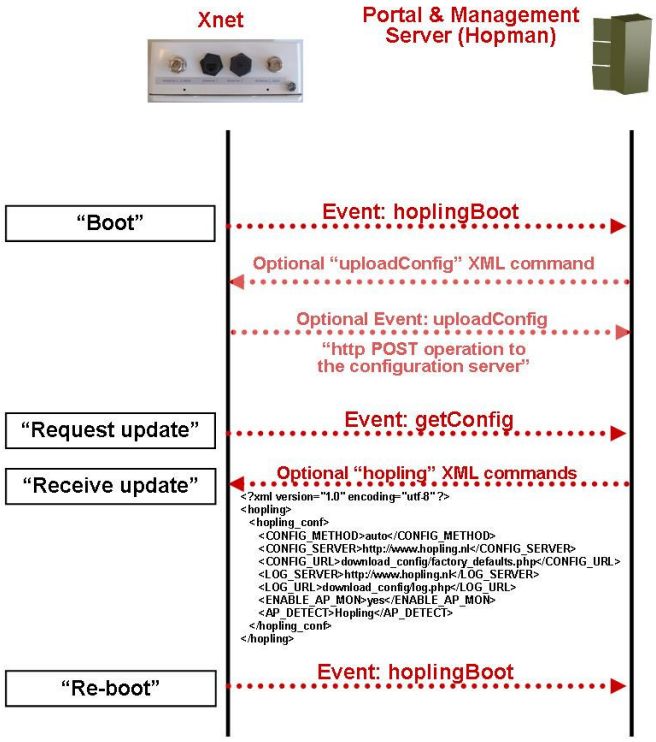


Figure 32, Xnet Viper "getConfig" boot sequence.

12.2 Xnet Viper "getConfig" XML syntax

The XML syntax for uploading information to the access controller is very simple. The XML document that is the response from the portal server should always start with the XML declaration **<?xml version="1.0" encoding="utf-8" ?>** at the top of the document. Next it should start with the root element **<hopling>**. This indicates the start of the configuration document for a Hopling Xspot/Xnet access controller. The end of the element is at the bottom of the document and is represented by the tag **</hopling>**. Inside the root element you can have one ore more elements with start and end tags following a similar pattern. Those additional elements indicate the configuration file(s) that should be updated. Between the configuration file element tags you can place the configuration parameter tags containing the values to be updated. The syntax for updating configuration files follows the directory structure of config files on the Xspot/Xnet. The `/config/hopling/` directory part is not part of the XML syntax.

A "getConfig XML document" for the Hopling access controller will generally look like:

```
<?xml version="1.0" encoding="utf-8" ?>
<hopling>
   <config_file1_name_conf>
      <PARAMETER1>value</PARAMETER1>
      <PARAMETER2>value</PARAMETER2>
      <PARAMETER3>value</PARAMETER3>
      <PARAMETER4>value</PARAMETER4>
   </config_file1_name_conf>
   <config_file2_dir>
         <config_file2_name_conf>
            <PARAMETER1>value</PARAMETER1>
           <PARAMETER2>value</PARAMETER2>
           <PARAMETER3>value</PARAMETER3>
           <PARAMETER4>value</PARAMETER4>
      </config_file2_name_conf>
   </config_file2_dir>
</hopling>
```

The files for the hotspot mode need an additional virtual gateway element <virtual_gw_0> to <virtual_gw_3> to be able to determine which virtual gateway is supposed to be updated.

Using this XML getConfig mechanism every configuration file on the access controller, with the exception of the event files, can be updated.

12.2.1.1 General files to update

The following general configuration files are available for update, where "x" stands for the Virtual Gateway number.

```
/config/hopling/hopling.conf
/config/hopling/virtual_gw/virtual_gw_x/lan/lan_x.conf
/config/hopling/virtual_gw/virtual_gw_x/wan/wan_x.conf
/config/hopling/virtual_gw/virtual_gw_x/wifi/wifi_0.general.conf
/config/hopling/virtual_gw/virtual_gw_x/wifi/wifi_0_x.conf

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

Only available on Xnet Viper-II systems:
/config/hopling/virtual_gw/virtual_gw_x/wifi/wifi_1.general.conf
/config/hopling/virtual_gw/virtual_gw_x/wifi/wifi_1_x.conf
/config/hopling/wifi_backbone/wifi_backbone_1/neighbors_1.conf
```

12.2.1.2 Files to update in Hotspot mode

For Hotspot mode the following files are available for automatic updates. There are 4 sets of files, one set for each virtual gateway. In the list below "x" can be 0 to 3 (zero to 3).

```
/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/hotspot.conf
/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/blocked_subnet_list.conf
/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/mac_access_list.conf
/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/allowed_hosts.web.conf
~~/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/allowed_hosts.other.conf~~
~~/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/allowed_hosts.virus.conf~~
~~/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/allowed_hosts.voip.conf~~
/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/port_black_list.web.conf
~~/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/port_black_list.other.conf~~
```

~~/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/port_black_list.virus.conf~~
~~/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/port_black_list.voip.conf~~
/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/port_fw.web.conf
~~/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/port_fw.other.conf~~
~~/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/port_fw.virus.conf~~
~~/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/port_fw.voip.conf~~
/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/port_white_list.web.conf
~~/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/port_white_list.other.conf~~
~~/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/port_white_list.virus.conf~~
~~/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/port_white_list.voip.conf~~

The .other.conf, .virus.conf and .voip.conf files are reserved for future use, and are not being updated yet!

12.3 Example: updating the hopling.conf file

As an example the exact syntax to update the `/config/hopling/hopling.conf` will be explained. The configuration file itself contains a number of unique configuration parameters. The names of the configuration file parameters can be used in the XML command to change the value of the parameters in the configuration file. Take a look at the contents of the /config/hopling/hopling.conf configuration file.

```
#@! <upload> <config> <reserved2> <reserved3> <reserved4>
#@$ <"General configuration parameters for the device">
#
# File:/config/hopling/hopling.conf
#
# Configuration file for the Hopling Xspot/Xnet
# (c) Hopling Technologies 2004, 2005, 2006
# Ivo van Ling (support@hopling.com)
# Bas Muns
# Rudger van Brenk
#
# This file contains general configuration paramaters for this
# Hopling router. Specific configuration parameters, dependent on
# the mode of operation and the available wired and wireless
# interfaces can be set in the separate configuration files.
#

#@$ <"General parameters">
#@@ <VERSION>      <STRING>    <0,128>  <READ_ONLY>   <RESERVED>  <"Version of the software.
Please do not change this yourself">
#@@ <FLAVOUR_TYPE> <STRING>    <0,128>  <READ_ONLY>   <RESERVED>  <"Flavour of the settings.
Please do not change this yourself">
#@@ <FLAVOUR>      <STRING>    <0,128>  <READ_ONLY>   <RESERVED>  <"Flavour type of this
version. Please do not change this yourself">
#@@ <REL_DATE>     <STRING>    <0,128>  <READ_ONLY>   <RESERVED>  <"Release date of this
version. Please do not change this yourself">
#@@ <BUILD_NR>     <STRING>    <0,128>  <READ_ONLY>   <RESERVED>  <"Build number of this
version. Please do not change this yourself">
#@@ <BUILD_TAG>    <STRING>    <0,128>  <READ_ONLY>   <RESERVED>  <"Build tag of this version.
Please do not change this yourself">
#@@ <GPS>          <GPS>       <16,32>  <NONE>        <RESERVED>  <"GPS location of this device.
Please fill in comma seperated list of longitude: degrees,minutes,seconds,direction, latitude:
degrees,minutes,seconds,direction, and optional height (in meters). E.g.
52,20,58,N,5,10,48,E,5">

VERSION="3.1.4pre1"
FLAVOUR_TYPE="Xnet"
FLAVOUR="HSS1"
REL_DATE="Wed Apr 18 10:21:39 CEST 2007"
BUILD_NR="0980"
BUILD_TAG="development"
GPS="52,20,58,N,5,10,48,E,5"

#@$ <"Parameters for SELF PROVISIONING">
#@@ <CONFIG_METHOD>  <DROPDOWN> <auto,manual>   <NONE>   <RESERVED>   <"Config method for self
provisioning">
#@@ <CONFIG_SERVER>  <HOST_IP>  <1>             <NONE>   <RESERVED>   <"Server to use for
autoconfiguration">
#@@ <CONFIG_URL>     <URL>      <1>             <NONE>   <RESERVED>   <"URL to call to get
parameters through XML">
#@@ <HOST_NAME>      <STRING>   <0,128>         <NONE>   <RESERVED>   <"Optional HOSTNAME
parameter. If left empty then the hostname is constructed by the function of the device (Xnet,
Xspot, XspotUMTS, Xspot3G+ ) and the last 6 digits of the MAC address of eth0">
#@@ <GATEWAY_ID>     <STRING>   <0,128>         <NONE>   <RESERVED>   <"Optional GATEWAY_ID
parameter to identify the gateway">
#@@ <LOCATION_ID>    <STRING>   <0,128>         <NONE>   <RESERVED>   <"Optional LOCATION_ID
parameter to identify the location this device belongs to">
```

```
CONFIG_METHOD="manual"
CONFIG_SERVER="http://hopman.hopling-services.net"
CONFIG_URL="hopman/log.php"
HOST_NAME=""
GATEWAY_ID=""
LOCATION_ID="Hopling_Almere"

#@$ <"Parameters for UPDATING">
#@@ <UPDATE_SERVER>  <HOST_IP>  <1>             <NONE>   <RESERVED>   <"Server to use for
updating">
#@@ <UPDATE_URL>     <URL>      <1>             <NONE>   <RESERVED>   <"URL to call to get
parameters for updating">

UPDATE_SERVER="http://updater.hopling.com"
UPDATE_URL="manufacture/update.php"

#@$ <"Parameters for additional services">
#@@ <SUPPLY_DNS>              <DROPDOWN> <yes,no>  <NONE>   <RESERVED>   <"provide DNS caching">
#@@ <ENABLE_GLOBAL_STATIC_IP> <DROPDOWN>  <yes,no> <NONE>   <RESERVED>   <"Enable global static
IP">
#@@ <GLOBAL_STATIC_IP>        <IP>        <1>      <NONE>   <RESERVED>   <"An IP address which
can be used to configure this device when other methods fail">

SUPPLY_DNS="yes"
ENABLE_GLOBAL_STATIC_IP="yes"
GLOBAL_STATIC_IP="172.16.172.16"

#@$ <"Parameters for monitoring of remote access points and other devices connected to this
Hopling">
#@@ <ENABLE_AP_MON>  <DROPDOWN> <yes,no>  <NONE>   <RESERVED>  <"Enable monitoring of remote
access points and other devices connected to this Hopling">
#@@ <AP_DETECT>      <INT>      <0,10000> <NONE>   <RESERVED>  <"The amount of seconds for
reporting the devices">

ENABLE_AP_MON="no"
AP_DETECT="600"

#@$ <"Parameters for monitoring of this gateway">
#@@ <ENABLE_GW_MON>  <DROPDOWN> <yes,no>     <NONE>   <RESERVED>  <"Send a gateway detect
event">
#@@ <GW_DETECT>      <INT>      <0,10000>    <NONE>   <RESERVED>  <"The amount of seconds for
sending the gateway detect event">

ENABLE_GW_MON="no"
GW_DETECT="600"

#@$ <"Parameters for synchronizing the clock of this machine to a stable internet clock">
#@@ <NTP_SERVER>  <HOST_IP>   <1>          <NONE> <RESERVED>  <"NTP server">
#@@ <TIMEZONE>    <STRING>    <0,128>      <NONE> <RESERVED>  <"Current offset to CET (Daylight
Saving Time) time (eg. Amsterdam - 1 hour = CET)">

NTP_SERVER="pool.ntp.org"
TIMEZONE="CET-1DST"

#@$ <"Parameters for SNMP daemon">
#@@ <SNMP_ENABLE>       <DROPDOWN>  <yes,no>      <NONE>    <RESERVED>   <"Enable the SNMP
daemon on this device">
#@@ <SNMP_LOCATION>     <STRING>    <0,128>       <NONE>    <RESERVED>   <"Location of this
device">
#@@ <SNMP_CONTACT>      <STRING>    <0,128>       <NONE>    <RESERVED>   <"Contact name">
#@@ <SNMP_RO_COMMUNITY> <STRING>    <0,128>       <NONE>    <RESERVED>   <"Read only access
community string">

SNMP_ENABLE="no"
SNMP_LOCATION="default location description"
SNMP_CONTACT="someone@yourdomain.com"
SNMP_RO_COMMUNITY="public"

#@$ <"Parameters for the syslog daemon">
#@@ <SYSLOG_METHOD>     <DROPDOWN>  <local,network>   <NONE>   <RESERVED>  <"Method for
syslogging. Network method will send messages to remote server and also locally.">
#@@ <SYSLOG_SERVER>     <IP>        <1>               <NONE>   <RESERVED>  <"IP address to send
syslog message to if method = network">
#@@ <SYSLOG_PORT>       <PORT>      <1>               <NONE>   <RESERVED>  <"UDP port to send
syslog message to">

SYSLOG_METHOD="local"
SYSLOG_SERVER="127.0.0.1"
SYSLOG_PORT="514"
```

To change a number of parameters in the file the portal would send the following XML document to the access controller.

```
<?xml version="1.0" encoding="utf-8" ?>
<hopling>
   <hopling_conf>
      <CONFIG_METHOD>auto</CONFIG_METHOD>
      <CONFIG_SERVER>http://www.updated_server.nl</CONFIG_SERVER>
      <CONFIG_URL>download_config/thisisanewname.php</CONFIG_URL>
      <LOG_SERVER>http://www.hopling.nl</LOG_SERVER>
      <LOG_URL>download_config/log.php</LOG_URL>
      <ENABLE_AP_MON>yes</ENABLE_AP_MON>
      <AP_DETECT>Hopling</AP_DETECT>
   </hopling_conf>
</hopling>
```

As you can see the configuration file name (hopling.conf) is indicated with the tag <hopling_conf> and the parameters to update have the same name as the corresponding parameter in the configuration file. It is not necessary to send the complete contents of the configuration file. Only the elements that need to be updated have to be included in the XML document.

12.4 Example: updating the virtual_gw_x config file.

Below is an example of the `/config/hopling/virtual_gw/virtual_gw_0/virtual_gw_0.conf` file.

```
#
# 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 : Say "yes" to enable this interface.
#                  If "no" all other settings are ignored.
# - VGW_0_MODE   : <hopling/hotspot>
#                  "hopling": act as a node in a Hopling network
#                  "hotspot": become a local hotspot
#
VGW_0_ENABLE="yes"
VGW_0_MODE="hopling"

#
# - VGW_0_LOG_SERVER    : Server to use for logging events
# - VGW_0_LOG_URL       : URL to call to log events through XML
#
VGW_0_LOG_SERVER="http://www.hopling.nl"
VGW_0_LOG_URL="download_config/log.php"

#
# Parameters for the VPN client interface
# - VGW_0_ENABLE_VPN    : <yes/no>
# - VGW_0_VPN_TYPE      : <pptp/pppssh>
#                   If set to "pptp" the connection will be made by the
#                   Point to Point Tunnelling protocol. This will not
#                   work well through a NATed modem in case of multiple
#                   pptp connections to the same VPN server
#                   If set to "pppssh" the connection will be made by
#                   tunnelling Point-to-Point Protocol over a Secure
#                   SHell (SSH) connection. This works better with
#                   multiple NATed connections.
# - VGW_0_VPN_SERVER    : This is the hostname, or IP address for the VPN
#                   (pptp or ssh) server
# - VGW_0_VPN_NAME      : This is the user name for the VPN server.
# - VGW_0_VPN_SECRET    : This is the password for the VPN server.
# - VGW_0_VPN_LOC_IP    : This is the IP address of the local VPN tunnel
#                   The 0.0.0.0 entry needs to be replaced for a
#                   valid IP address.
# - VGW_0_VPN_REM_IP    : This is the IP address of the remote end of the VPN
#                   tunnel. The 0.0.0.0 entry needs to be replaced for a
#                   valid IP address.
```

```
#                   Both local and remote tunnel IP addresses can be set
#                   to "*" if the VPN server allocates the IP addresses
#                   dynamically (only for pptp)
# - VGW_0_VPN_ADD_ROUTE    : Set to "yes" if you want to add route(s)
#                   for the VPN interface.
# - VGW_0_VPN_ROUTE    : 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. When multiple
#                   entries are added, separate them with a space.
#
VGW_0_ENABLE_VPN="no"
VGW_0_VPN_TYPE="pppssh"
VGW_0_VPN_SSH_NAME="vpn"
VGW_0_VPN_SERVER="82.148.221.131"
VGW_0_VPN_USER="XnetMkII-c3a124"
VGW_0_VPN_SECRET="hoplingtech01"
VGW_0_VPN_LOC_IP="0.0.0.0"
VGW_0_VPN_REM_IP="0.0.0.0"
VGW_0_VPN_ADD_ROUTE="no"
VGW_0_VPN_ROUTE="192.168.199.0/255.255.255.0 192.168.200.0/255.255.248.0"

# End
```

In order to update this file, for instance to enable the VPN tunnel, the XML message should be formatted as below:

```
<virtual_gw_0>
   <virtual_gw_0_conf>
      <VGW_0_ENABLE_VPN>yes</VGW_0_ENABLE_VPN>
      <VGW_0_VPN_TYPE>pppssh</VGW_0_VPN_TYPE>
      <VGW_0_VPN_SSH_NAME>another_name</VGW_0_VPN_SSH_NAME>
      <VGW_0_VPN_SERVER>11.22.33.44</VGW_0_VPN_SERVER>
      <VGW_0_VPN_USER>XnetMkII-112233</VGW_0_VPN_USER>
      <VGW_0_VPN_SECRET>hardlyasecret</VGW_0_VPN_SECRET>
      <VGW_0_VPN_LOC_IP>10.16.0.1</VGW_0_VPN_LOC_IP>
      <VGW_0_VPN_REM_IP>10.16.0.200</VGW_0_VPN_REM_IP>
   </virtual_gw_0_conf>
</virtual_gw_0>
```

This needs to be embedded into the root elements <hopling></hopling> to make a complete XML document.

12.5 Example: updating the allowed hosts files

The update of the `/config/hopling/virtual_gw/virtual_gw_x/hotspot_mode/allowed_hosts.web.conf` file (walled garden) works a little bit different from the general configuration files. Whereas the general configuration files such as the `/config/hopling/hopling.conf` contain unique parameter names that can be used in the XML document the allowed hosts files contain multiple lines of port numbers and IP addresses. That means that the portal server needs to send the complete allowed_hosts list in order to upgrade the file. Just sending one updated line will result in the file containing only that line.

Furthermore, the system has 4 sets of allowed_hosts files, one for each Virtual Gateway that is running on the system. So the portal server needs to also include the intended Virtual Gateway in the XML document.

The syntax for the XML document for updating an allowed hosts file is:

```
<virtual_gw_0>
   <hotspot_mode>
      <allowed_hosts_web_conf>
         <comment>Examples: the HTTP and HTTPS websites of Hopling Technologies</comment>
         <entry protocol='tcp' host='www.hopling.com' port='80' />
         <entry protocol='tcp' host='82.148.221.130' port='80' />
         <entry protocol='tcp' host='www.hopling.com' port='443' />
         <entry protocol='tcp' host='82.148.221.130' port='443' />
         <comment>The DNS servers</comment>
         <entry protocol='tcp' host='194.109.6.66' port='53' />
         <entry protocol='udp' host='194.109.6.66' port='53' />
         <comment>The Hopling SSH server</comment>
         <entry protocol='tcp' host='www.hopling.nl' port='22' />
         <entry protocol='udp' host='www.hopling.nl' port='22' />
      </allowed_hosts_web_conf>
```

```
    <hotspot_mode>
</virtual_gw_0>
```

This needs to be embedded into the root elements <hopling></hopling> to make a complete XML document.

13 Upgrade procedure for Xnet Viper Systems

This chapter describes the software upgrade procedure for the Xnet Viper routers. Both indoor and outdoor Xnet versions can be upgraded to HopWARE software version 3.1.x. In order to start the upgrade to HopWARE 3.1.x the Xnet router must run HopWARE 2.3.7 or higher.

If the Xnet router is running a software version lower than 2.3.7 the software upgrade must be performed in two steps:

- First the Xnet router must be upgraded to the HopWARE version 2.3.8 (see chapter 13.1).
- After the upgrade to HopWARE 2.3.8 the Xnet router can be further upgraded to 3.1.x.

In principle the update of the software is done fully automatic and over the Internet. However, some basic knowledge of the Linux operating system is required to install and execute the "update_hopling" tool. The update procedure is as follows:

- Download the "update_hopling" tool
- Make the tool executable on the Xnet filing system
- Start "update_hopling" tool to initiate a software update.

After starting the "update_hopling" tool it will ask a number of questions about what server and passwords to use. The tool already has some sane default values built in. Pressing [ENTER] a few times will set the default values.

The "update_hopling" tool will download the latest commercial available software and install it. After the installation is complete the original router configuration is copied over to the new software and the system will reboot.

The example below uses an Xnet Mark-II, however the procedure is exactly the same for an Xnet Mark-I and Mark-II.

13.1 Upgrade HopWARE 2.1.x to HopWARE 2.3.8

This step is only required in case the Xnet node has a HopWARE version prior to version 2.3.7, only applicable for Xnet Mark-I and Xnet Mark-II series. For Xnet **Viper** series this is not necessary.

13.1.1 Download of the "update_hopling" tool

The "update_hopling" tool can be downloaded from the Hopling Technologies website. It can either be downloaded using your favorite browser or straight onto the Xnet you are trying to upgrade. In this procedure we will download straight to the Xnet.

First log in to the Xnet Viper using Secure Shell. When you are logged in set the file system of the Xnet to read/write using the command **`remount,rw`**

```
XnetMkI-c20930:~# remount,rw
```

Then download the "update_hopling" tool using the command:

```
wget "http://updater.hopling.com/download/update_hopling".
```

This will automatically download the "update_hopling" tool from the Hopling Technologies website onto the Xnet.

```
XnetMkI-c20930:~# wget "http://updater.hopling.com/download/update_hopling"
--15:36:47--  http://updater.hopling.com/download/update_hopling
           => `update_hopling'
Resolving updater.hopling.com... done.
```

```
Connecting to updater.hopling.com[84.53.97.83]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 48,249 [text/plain]

100%[====================================>] 48,249       362.45K/s    ETA 00:00

15:36:47 (362.45 KB/s) - `update_hopling' saved [48249/48249]
```

You have now downloaded the "update_hopling" tool onto the system.

13.1.2 Make the "update_hopling" tool executable

After the file is downloaded from the web server it needs to be set to "executable". That means that the Linux operating system can run the file. This is done using the following command:
`chmod +x update_hopling`

```
XnetMkI-c20930:~# chmod +x update_hopling
```

The system is now ready to be updated.

13.1.3 Start the "update_hopling" tool

Now that the tool is downloaded and set to an executable file you can start the software update by giving the command: ./`update_hopling`.

You will be presented with a disclaimer to which you will have to answer "y" (yes) in order to start the update. All subsequent questions can be answered by just pressing [ENTER].

An example of the disclaimer:

```
XnetMkI-c20930:~# ./update_hopling

Hopling Technologies software updater version 2.20, dated 03-11-2005 starting...

+------------------------------------------------------------------------------+
|                          *** DISCLAIMER ***                                  |
| This script attempts to perform a remote software update of the              |
| Hopling Mark-I and Mark-II mesh routers.                                     |
| This script can be used to upgrade Hopling Mark-I and Mark-II routers        |
| to software version 2.3.3 or above.                                          |
| Although the original configuration files are copied and parsed              |
| by this script, no guarantees are given that ALL parameters will             |
| be copied over correctly. Please inspect each Hopling afterwards.            |
| Furthermore, if you are upgrading the software over a wireless link          |
| please be aware that link failure may result in a corrupted software         |
| image on your router.                                                        |
|                        *** END DISCLAIMER ***                                |
|                                                                              |
|                                                                              |
|      Copyright 2005 Hopling Technologies B.V. All Rights Reserved.           |
+------------------------------------------------------------------------------+
Do you wish to continue? [y/N] y

Ok, continuing with the update...
```

After answering yes to the disclaimer the "update_hopling" tool will ask for the server, username and password for the remote update server. Pressing [ENTER] will select the default values.

```
Remote update server configuration:
 - What server contains the Hopling update image? [84.53.97.83]:
 - What is your username for server 84.53.97.83? [hopling]:
 - What is your password for server 84.53.97.83? [hoplingtech01]:

Checking configuration of system HoplingMkI-c36d68:
 - Found Hopling with software version Hopling-2.1.1.

Checking server 82.148.221.131 for latest updater script.
- Found the following updater versions:
update_hopling-1.20
update_hopling-1.30
update_hopling-1.40
```

```
update_hopling-1.50
update_hopling-1.60
update_hopling-2.00
update_hopling-2.10
update_hopling-2.20
update_hopling-2.30
update_hopling-2.40
update_hopling-2.41
update_hopling-2.42
update_hopling-2.43
    -    Starting update script to update_hopling-2.43
Detected a updater with version: 2.43, we are running: 2.20
Downloading updater update_hopling-2.43... please wait
- Handing over control to new updater version: update_hopling-2.43

Hopling Technologies software updater version 2.43, dated 05-04-2006 starting...

Remote update server configuration:
- What server contains the Hopling update image? [84.53.97.83]:

- What is your username for server 84.53.97.83? [hopling]:

- What is your password for server 84.53.97.83? [hoplingtech01]:

Checking configuration of system XnetMkI-c3a1ec:
- Found software version Hopling-2.3.0.

Checking server 84.53.97.83 for latest updater script.
- Found the following updater versions:
update_hopling-1.20
update_hopling-1.30
update_hopling-1.40
update_hopling-1.50
update_hopling-1.60
update_hopling-2.00
update_hopling-2.10
update_hopling-2.20
update_hopling-2.30
update_hopling-2.40
update_hopling-2.41
update_hopling-2.42
update_hopling-2.43
Update script up-to-date.

Checking server 84.53.97.83 for updated software images.
- Found the following software versions:
0) HoplingMk-2.2.0
1) HoplingMk-2.2.1
2) HoplingMk-2.3.0
3) HoplingMk-2.3.1
4) HoplingMk-2.3.2
5) HoplingMk-2.3.3
6) HoplingMk-2.3.4
7) HoplingMk-2.3.7
8) HoplingMk-2.3.8
- What version should I get from 84.53.97.83?
Type the preceding number of the version [8]:8
Version = HoplingMk-2.3.8

- Beginning upgrade

Starting with the software update to Hopling 2.3.x settings. (case 6)
- Copying original configuration settings to backup dir.
- Setting the file system on XnetMkI-c3a1ec to read/write.
- Upgrading hopling software
- Stopping the apDetect application.
- Stopped the apDetect application.
- Downloading software version HoplingMk-2.3.8 from 82.148.221.131.
This might take a few minutes and is dependent on your download speed.
Please wait...
Download ok.
Starting md5 checksum check...
Not performing md5 checksum check: md5 file does not exist (/root/HoplingMk-2.3.8.md5)
- Updating the boot records on XnetMkI-c3a1ec.
Added Hopling_2.3.7 *
- Updating boot records complete.
- Download complete.

Updating configuration files with original settings for XnetMkI-c3a1ec.
Doing restore to factory defaults.
Restore to factory defaults completed.
Restoring old
settings.....................................................................................
.....................
- Restoring old settings complete. Successfully saved all settings.
```

```
Please wait for the Hopling to reboot...
Rebooting...

End of updater 2.43... bye

Copyright 2005 Hopling Technologies B.V. All Rights Reserved.

HoplingMkI-c36d68:~#
```

After the upgrade the Xnet will automatically perform a reboot.

13.2 Upgrade

You can only upgrade Xnet systems to HopWARE version 3.0.0 and above if you are running at least HopWARE 2.3.7. If you are running an earlier HopWARE version please refer to chapter: 13.1 on how to upgrade this first.

13.2.1 Start the "update_hopling" tool

Hopling systems running HopWARE 2.3.8 already have the "update_hopling" tool installed. In order to start the tool type: `./update_hopling-1.50`. Please not that this tool is attemptiong to connect to an old (non existent) software server. Please substitute the IP address 82.148.221.131 with **updater.hopling.com**

You will be presented with a disclaimer to which you will have to answer "y" (yes) in order to start the update. All subsequent questions can be answered by just pressing [ENTER].

An example of the disclaimer:

```
./update_hopling-1.50

Hopling Technologies software updater version 1.50, dated 15-07-2005 starting...

+------------------------------------------------------------------------+
|                        *** DISCLAIMER ***                              |
| This script attempts to perform a remote software update of the        |
| Hopling Mark-I and Mark-II mesh routers.                               |
| This script can be used to upgrade Hopling Mark-I and Mark-II routers  |
| to software version 2.2.0 or above.                          |
| Although the original configuration files are copied and parsed        |
| by this script, no guarantees are given that ALL parameters will       |
| be copied over correctly. Please inspect each Hopling afterwards.      |
| Furthermore, if you are upgrading the software over a wireless link    |
| please be aware that link failure may result in corrupted software    |
| image on your router.                                                  |
|                      *** END DISCLAIMER ***                            |
+------------------------------------------------------------------------+

Do you wish to continue? [y/N] y
```

You have to answer "y" for the updater to start.

```
Ok, continuing with the update...

Remote update server configuration:
 - What server contains the Hopling update image? [82.148.221.131]:
 - What is your username for server 82.148.221.131? [hopling]:
 - What is your password for server 82.148.221.131? [hoplingtech01]:

Checking configuration of system XnetMkI-c3a1ec:
 - Found Hopling with software version Hopling-2.3.8.

Checking server updater.hopling.com for latest updater script.
 - Found the following updater versions:
      update_hopling-1.20
      update_hopling-1.30
```

```
      update_hopling-1.40
      update_hopling-1.50
      update_hopling-1.60
      update_hopling-2.00
      update_hopling-2.10
      update_hopling-2.20
      update_hopling-2.30
      update_hopling-2.40
      update_hopling-2.41
      update_hopling-2.42
      update_hopling-2.43
 - Detected a newer updater with version: 2.43, we are running: 1.50
```

The update tool will automatically download a newer version of itself if it detects there is a new version available.

```
Downloading newer updater update_hopling-2.43... please wait
 - Handing over control to new updater version: update_hopling-2.43

Hopling Technologies software updater version 2.43, dated 05-04-2006 starting...

Checking configuration of system XnetMkI-c3a1ec:
- Found software version Hopling-2.3.8.

Checking server updater.hopling.com for latest updater script.
- Found the following updater versions:
update_hopling-1.20
update_hopling-1.30
update_hopling-1.40
update_hopling-1.50
update_hopling-1.60
update_hopling-2.00
update_hopling-2.10
update_hopling-2.20
update_hopling-2.30
update_hopling-2.40
update_hopling-2.41
update_hopling-2.42
update_hopling-2.43
Update script up-to-date.

Checking server updater.hopling.com for updated software images.
- Found the following software versions:
0) HoplingMk-2.2.0
1) HoplingMk-2.2.1
2) HoplingMk-2.3.0
3) HoplingMk-2.3.1
4) HoplingMk-2.3.2
5) HoplingMk-2.3.3
6) HoplingMk-2.3.4
7) HoplingMk-2.3.7
8) HoplingMk-2.3.8
9) HoplingMk-3.0.0
- What version should I get from updater.hopling.com?
Type the preceding number of the version [9]:9
Version = HoplingMk-3.0.0

- Beginning upgrade

- Upgrading to completely new major release.

- Get new updater.
========================================================================
 Processing device_info:
========================================================================
  Upgrade of component device_info using protocol http...
  Checking checksum of upgraded file...
  Checksum match successful...
========================================================================
 Processing flavourfs:
========================================================================
  Upgrade of component flavourfs using protocol http...
  Checking checksum of upgraded file...
```

```
  Checksum match successful...
======================================================================
 Processing kernel:
======================================================================
  Upgrade of component kernel using protocol http...
  Checking checksum of upgraded file...
  Checksum match successful...
======================================================================
 Processing rootfs:
======================================================================
  Upgrade of component rootfs using protocol http...
  Checking checksum of upgraded file...
  Checksum match successful...
======================================================================
  Create bootloader files
   title     : Xnet Version 3.0.2 HT1 (build: 0239)
   kernel    : /boot/bzImage-net45xx-3.0.2-release-0239
   arguments : console=ttyS0,19200n8
               type=Xnet
               flavour=HT1
               version=3.0.2-release-0239
======================================================================
======================================================================
   Download interim updater kernel...
======================================================================
  Upgrade of component Updater_Kernel using protocol http...
  Checksum file of Updater_Kernel not available...
Warning: LBA32 addressing assumed
Setting DELAY to 20 (2 seconds)
Added Updater_Kernel *
======================================================================
   Done...
======================================================================


Broadcast message from root (pts/0) (Thu Apr  6 13:23:01 2006):


The system is going down for reboot NOW!


- Done....

End of updater 2.43... bye

Copyright 2005 Hopling Technologies B.V. All Rights Reserved.

XnetMkI-c3a1ec:~#
```

After the upgrade the Xnet will automatically perform a reboot.

13.3 Upgrade HopWARE 3.0.x to HopWARE 3.1.x

This chapter describes the software upgrade procedure for Xnet routers running HopWARE version 3.0.x. Both indoor and outdoor versions can be upgraded.

In principle the update of the software is done fully automatic and over the Internet. Every 3.0 software version is capable of being upgraded over the Internet. This can be done from the command line interface or through the web interface.

From the command line the update of the software can be started by typing “upgrade –U hopling –P hoplingtech01”.

As an example:

```
XnetVpIV-01c822:~$ upgrade -U hopling -P hoplingtech01
 : ====================================================================
 : Prepare upgrade:
 :     Server        : http://updater.hopling.com
 :     URL           : manufacture/update.php
 :     MAC           : 00:08:a2:01:c8:22
 : ====================================================================
 : Current Software:
 :     SW_VERSION    : 3.1.2
 :     SW_FLAVOUR    : HT1
 :     BUILD NR      : 0934
 :     RELEASE DATE  : Wed Mar 21 19:06:36 CET 2007
 : ====================================================================
 :
 :
 : +-----------------------------------------------------------------------+
 : |                          *** DISCLAIMER ***                           |
 : | This script attempts to perform a remote software update of the       |
 : | Hopling Mark-I and Mark-II mesh routers.                              |
 : | This script can be used to upgrade Hopling Mark-I and Mark-II routers |
 : |                                                                       |
 : | Although the original configuration files are copied and parsed       |
 : | by this script, no guarantees are given that ALL parameters will      |
 : | be copied over correctly. Please inspect each Hopling afterwards.     |
 : | Furthermore, if you are upgrading the software over a wireless link   |
 : | please be aware that link failure may result in a corrupted software  |
 : | image on your router.                                                 |
 : |                       *** END DISCLAIMER ***                          |
 : |                                                                       |
 : |                                                                       |
 : |      Copyright 2005-2007 Hopling Technologies B.V. All Rights Reserved. |
 : +-----------------------------------------------------------------------+
 :
 : Do you wish to continue? [y/N]
y
 :
 : Ok, continuing with the update...
 : ====================================================================
 :  Available versions: (arrow is selected default)
 :
 : --> 1 ) Xnet Version 3.1.3 HT1 (build: 0966)
 :
 :  Type the number to select, or q to exit (1):
1
 : Selected version = 1
 :
 : ====================================================================
 : ====================================================================
 :  Processing device_info:
 : ====================================================================
 :   device_info: File already exists, checking hash...
 :   Upgrade of component device_info using protocol http...
 :   Checking checksum of upgraded file...
 :   Checksum match succesfull...
 : ====================================================================
 :  Processing flavourfs:
 : ====================================================================
 :   flavourfs: File already exists, checking hash...
ERR :   Checksum of flavourfs failed, retry download...
 :   Upgrade of component flavourfs using protocol http...
 :   Checking checksum of upgraded file...
 :   Checksum match succesfull...
 : ====================================================================
 :  Processing kernel:
 : ====================================================================
 :   kernel: File already exists, checking hash...
 :   Checksum match succesfull...
 :   kernel: File already exists skipping download...
 : ====================================================================
 :  Processing rootfs:
```

```
: ====================================================================
:   rootfs: File already exists, checking hash...
:   Checksum match succesfull...
:   rootfs: File already exists skipping download...
: ====================================================================
:   Create bootloader files
:    title     : Xnet Version 3.1.3 HT1 (build: 0966)
:    kernel    : /boot/zImage-ixp42x-3.1.3-release-0966
:    arguments : console=ttyS0,115200n8
:                type=Xnet
:                flavour=HT1
:                version=3.1.3-release-0966
: ====================================================================
:   Installing new config...
: ====================================================================
:    Done...
: ====================================================================
:
:
: Upgrade done, status is OK
```

After the upgrade the Xnet will have to be rebooted to make the new software version active.

Please note that the error message: "`ERR :  Checksum of device_info failed, retry download...`" is normal and does not indicate a failure to upgrade.

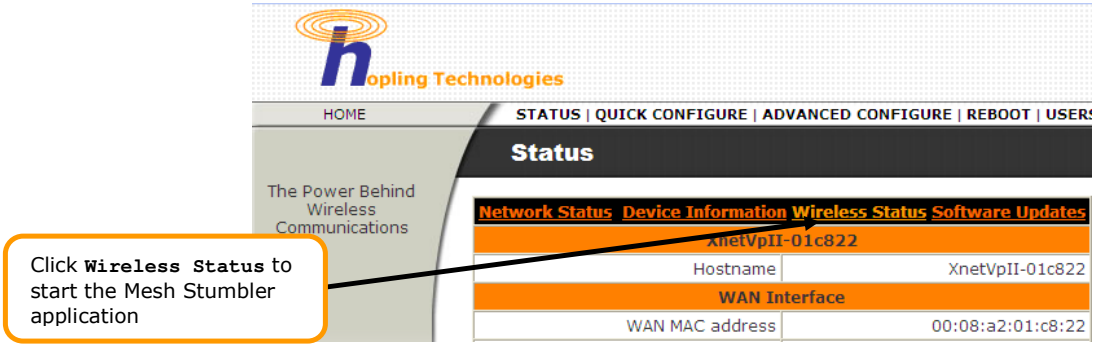
14 Testing Wireless (Mesh) Links and getting Statistics

HopWARE 3.1.x software provides several utilities to test the quality of the wireless links. It makes no difference if the Xnet nodes are being used in a Point-to-Point configuration or in a full mesh network. The underlying protocol that collects the wireless statistics of the links between each node in the network is the Hopling Discovery Protocol (HDP). Periodically (default once every 60 seconds) every Xnet node transmits an HDP packet that contains the (wireless) network statistics of that node itself.

This information can be obtained from each node to ascertain the quality of the wireless links. There are two of system tools available that will show this data to the user: the Mesh Stumbler web tool and the HDP command line tool.

14.1 Showing link statistics with Mesh Stumbler

The Mesh Stumbler tool is a flash application that is built in the web user interface of the Xnet Viper. You can start the application by clicking on the "Wireless Status" hyperlink on the Status page.



Mesh Stumbler displays wireless SSIDs, channels, whether WEP encryption is enabled and signal to noise ratio (SNR) of each radio signal that is being received on the Xnet Viper node.

When you have no flash installed in your web browser the Xnet Viper will show a semi static html page indicating the signal strength of each received node. The data can be refreshed by reloading the page (press F5).

Network Status Device Information Wireless Status Software Updates

XnetVpII-01c822

Radio 0 information Channel (MHz)

MAC address	SSID	Channel	Signal Noise Ratio
00:02:6f:33:4a:02	Hopling Technologies 0	6 (2437 MHz)	SNR 18 dB [■■■□□]
00:02:6f:08:0f:09	KPN	6 (2437 MHz)	SNR 49 dB [■■■■■]
00:02:6f:47:da:2d	vipert Elvin 69	6 (2437 MHz)	SNR 20 dB [■■■□□]
00:0c:84:01:9e:6c	MT: XspotMkI-c577d0	6 (2437 MHz)	SNR 22 dB [■■■□□]
00:0e:8e:7c:96:f6	OpenWrt	6 (2437 MHz)	SNR 12 dB [■■□□□]

Radio 1 information Channel (MHz)

MAC address	SSID	Channel	Signal Noise Ratio
00:0c:84:01:93:04	Hopling Technologies 0	36 (5180 MHz)	SNR 30 dB [■■■■□]
00:02:6f:47:da:28	vipert Elvin 69	36 (5180 MHz)	SNR 18 dB [■■■□□]

Figure 33 Mesh Stumbler as static html page, press F5 to refresh the data

The HopWARE Mesh Stumbler application shows the signal strength of all WiFi devices that are being received on that particular unit. By clicking on a specific node the details for that node are being displayed in the lower half of the screen. The screen automatically refreshes every few seconds to show the latest signal strengths.

The HopWARE Mesh Stumbler can for example be used to align two point to point antennas to give best link quality. Simply click on the far end Xnet Node and align the antenna to give maximum signal to noise ratio (SNR).

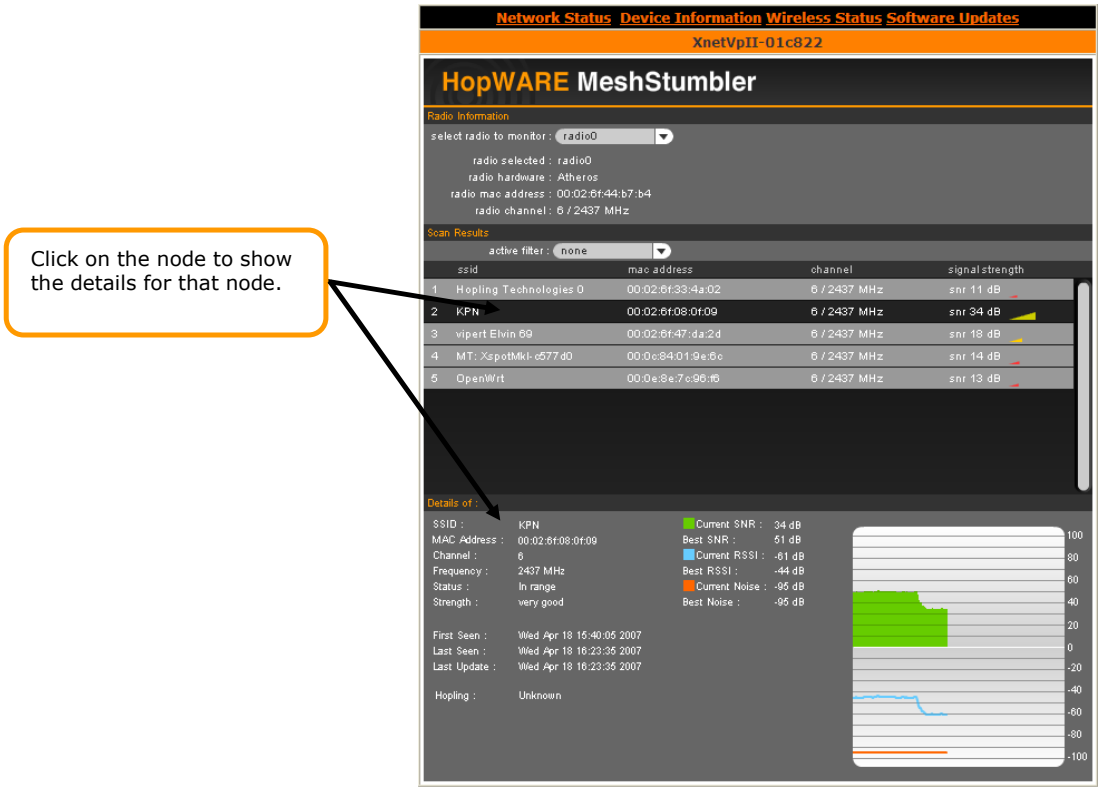


Figure 34 Mesh Stumbler as dynamic flash page data is automatically refreshed

14.2 Showing link statistics with HDP command line tool.

The **HDP** command line tool can show the signal to noise ratio of all the wireless signals being received on the Xnet Viper. Furthermore, it can also show the signal to noise ratios of ALL the radio signals being received by Xnet Viper nodes that belong to the same network. Being a command line tool it is more versatile than the flash application, at the cost of being somewhat more complicated.

To show the SNR values of this node only type **`hdp HoplingMeshSNR@0`** on the command line.

As an example:

```
XnetVpII-01c822:~$ hdp HoplingMeshSNR@0
HDP cache browser - Copyright (C) 2007 Hopling Technologies B.V. All Rights
Reserved.
```

```
Hopling Mesh SNR on peer 0: 00:02:6F:47:DA:28 on radio 1 at 5.180 GHz with 21 dB
SNR, SSID 'vipert Elvin 69', capabilities HDP & HAM (unrelated)
Hopling Mesh SNR on peer 0: 00:0C:84:01:93:04 on radio 1 at 5.180 GHz with 19 dB
SNR, SSID 'Hopling Technologies 0', capabilities HDP & HAM (lost,unrelated)
Hopling Mesh SNR on peer 0: 00:02:6F:33:4A:02 on radio 0 at 2.437 GHz with 13 dB
SNR, SSID 'Hopling Technologies 0', capabilities unknown (lost,unrelated)
Hopling Mesh SNR on peer 0: 00:02:6F:47:DA:2D on radio 0 at 2.437 GHz with 21 dB
SNR, SSID 'vipert Elvin 69', capabilities HDP (unrelated)
Hopling Mesh SNR on peer 0: 00:0E:8E:7C:96:F6 on radio 0 at 2.437 GHz with 11 dB
SNR, SSID 'OpenWrt', capabilities unknown (unrelated)
Hopling Mesh SNR on peer 0: 00:02:6F:08:0F:09 on radio 0 at 2.437 GHz with 34 dB
SNR, SSID 'KPN', capabilities unknown (unrelated)
Hopling Mesh SNR on peer 0: 00:0C:84:01:9E:6C on radio 0 at 2.437 GHz with 15 dB
SNR, SSID 'MT: XspotMkI-c577d0', capabilities unknown (unrelated)
7 records received
```

14.3 Performing a throughput test

The Xnet Viper system can test the throughput of the network, for example over a Point-to-Point link. The transmitting unit generates random packets of data that it sends to the receiving unit at the other end of the link with an application called **`walltx`**. The data packects are received on the other end of the link by another application called **wallrx**. Together the applications will show the throughput of the link in Megabits per second.

Performing a link test is started by giving the command **`wallrx`** (the data receiving application) on one end of the link and **`walltx`** (the data sending application) on the other side of the link.

To start the application on one end of the link:

```
XnetVpII-01c823:~$ wallrx
wallrx: waiting for data on port TCP 1500
20.1571 Mbits/sec
22.3034 Mbits/sec
23.0325 Mbits/sec
 connection closed by client
wallrx: waiting for data on port TCP 1500
```

To start the application on one end of the link:

```
XnetVpII-01c822:~$ walltx 192.168.18.89 -s 1 -b 30000
2.4907 Mbits/sec
24.1971 Mbits/sec
23.6990 Mbits/sec
23.6990 Mbits/sec
22.2045 Mbits/sec
22.7027 Mbits/sec
22.4536 Mbits/sec
21.7064 Mbits/sec
22.2045 Mbits/sec
23.4499 Mbits/sec
23.9480 Mbits/sec
23.2008 Mbits/sec
22.7027 Mbits/sec
22.2045 Mbits/sec
```

Be careful! Running a throughput test can be performed while the system carries user data, but the test overhead reduces the links data capacity. It is better to run these tests while the system is idle.

15 Frequently asked questions and gotcha's

This paragraph describes some frequently asked questions from people installing and using the Xnet Viper. This list is by no means complete. It will be constantly updated when we receive more questions.

Q: I installed the Xnet Viper and have extended the Ethernet cable using a number of Ethernet extension leads and Ethernet through connectors. The total cable length is over 40 meters. We now see the Hopling cycle through SSID "Hopling Technologies" and the SSID we configured ourselves.

A: This Hopling is probably constantly rebooting because the DC voltage for the system is too low. Once the system is booted and the wireless card is activated the power drop across the Ethernet is so large that the Hopling system will not work correctly. This will be noticed by the watchdog timer, who will automatically reboot the system.

The Xnet Viper is powered using power over Ethernet technology. The power supply of the Xnet Viper is delivering 48Volts/DC, which is injected into the Ethernet cable. If you use standard cat5e Ethernet cabling the average voltage drop per meter is about 0.1Volt. You can use a cable up to 100 meters in length before the power drop across it becomes so large that things stop working. However, connecting standard Ethernet cables together using Ethernet through connectors will degrade performance considerably and is therefore not advised.

Q: I replaced the standard configuration file with one of my own. The Xnet Viper still boots, but it looks it is stuck in the network "Hopling Technologies". Also I can not log in anymore. What is wrong?

A: The Xnet Viper uses the configuration files to set most customer specific parameters of the system. By replacing this file with something else the Hopling will boot with the parameters as specified in this new file. However, if for some reason the file is corrupt or unreadable, the Hopling reverts to a default configuration.

You can still log into the system using SSH via both the wireless and wired IP addresses or through the serial (console) port.

Q: I replaced the standard `/config/hopling/hopling.conf` file with one of my own. Something went wrong as the system now boots into the default configuration. How do I restore normal operation?

A: The Xnet Viper uses the `/config/hopling/hopling.conf` file to set most customer specific parameters of the system. If you have other Hoplings Xnet systems up and running you can copy a working file from this Xnet Viper onto the dead system. Also make sure that the file permissions are set correctly. If you are unsure please ask your reseller.

Example file permissions for file in the `/config/hopling/` directory,

```
XnetMkII-c3a124:/config/hopling$ ls -l
-rwxr-xr-x    1 root     root          3361 Mar 31 17:10 hopling.conf
-rw-r--r--    1 root     root           135 Mar 31 17:10 hw_type.conf
drwxr-xr-x    6 root     root          4096 Mar 31 17:10 virtual_gw
drwxr-xr-x    2 root     root          4096 Mar 31 17:10 webconfig
drwxr-xr-x    4 root     root          4096 Mar 31 17:10 wifi_backbone
```

Q: How do I see the IP addresses on my system?

A: The network configuration can be seen using the command `ifconfig`. If you log into the Xnet Viper using SSH type: `ifconfig br_wan0 [ENTER]`

As an example;

```
HoplingMkI-c36c74:~# ifconfig br_wan0
br_wan0   Link encap:Ethernet  HWaddr 00:00:24:C3:6D:68
          inet addr:192.168.1.170  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::200:24ff:fec3:6d68/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7789 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3002 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1089721 (1.0 MiB)  TX bytes:416175 (406.4 KiB)

HoplingMkI-c36c74:#
```

In this case the system is using IP address 192.168.1.170 with a netmask of 255.255.255.0 on the wired Ethernet port.

16 Appendix A: using the Xnet vi Editor

A text editor is a program used to edit files which contain text, such as C programs or system configuration files. While there are many such editors available for Linux, the only editor which you are guaranteed to find on any UNIX system is **vi** – the "visual editor". Vi is not the easiest editor to use, nor is it very self-explanatory. However, because it is so common in the UNIX world it is used by Hopling Technologies to edit configuration files. Please remember when using commands that vi is case-sensitive, so whether a letter is upper-case or lower-case **does** matter.

16.1.1 Two Modes of the vi Editor

Before you begin working with the vi editor, you should know that there are two modes of operation. These modes are known as *command mode* and the *insert mode*.

When you start up vi, you are in *command mode*. This mode is used to move through text, search for words or save a file, etc. This mode covers everything except inserting text. Insert mode is only for inserting text into a file.

Using **i**, **I**, **a**, **A**, **cw**, **o**, **O**, or **R** will place you into *insert mode* from *command mode*.

IMPORTANT!! Use the [Escape] key to return to *command mode* from *insert mode*. If you are not sure which mode you are in, hit the escape key to be sure to be in *command mode* again.

If the keys you are pressing are not achieving the results they should, you may be in the wrong mode, or you may have accidentally pressed the [CapsLock] key. The little green light on the Caps Lock key should not be lit (if such a light exists on your keyboard).

Sometimes you may hit [Escape] to switch to *command mode*, and find that the words INSERT MODE still appear at the bottom left corner of the window (as it does when in INSERT MODE with some setups). If this happens, press [Escape] again to be sure you are actually in *command mode*. If the words still appear in the lower left corner of the window, you may want to "refresh" the screen by pressing the [Control] and [l] keys at the same time. (That is the lower-case letter "l" in case you were not certain.) Now, if you are not in *insert mode*, the words stating otherwise will disappear from your screen.

16.1.2 Moving Around Within Text in Command Mode

[←] [↓] [↑] [→]	Move through text: left, down, up and right
[Control] [f]	Move forward one screen
[Control] [b]	Move backward one screen
[Control] [d]	Move half a screen down
[Control] [u]	Move half a screen up
[G]	Move to end of file
[1] [G]	Move to beginning of file
[6] [5] [G]	Move to line 65 in the file
[$]	Move to end of file
[0]	Move to beginning of line
[b]	Move to beginning of current word
[e]	Move to end of current word
/myword	Forward to any existing occurrence of <myword>
?myword	Backwards to any existing occurrence of <myword>
[n]	Next occurrence of <myword> in the search direction
[N]	Next occurrence of <myword> in the opposite direction as the search

16.1.3 Moving commands

You can use the arrow keys to move around the document. In addition, you can use the `h`, `j`, `k`, and `l` commands to move the cursor left, down, up and right respectively. This comes in handy when (for some reason) the arrow keys are not working correctly. The `w` command moves the cursor to the beginning of the next word; the `b` moves it to the beginning of the previous word.

16.1.4 Editing commands

`x`	Deletes current character.
`dd`	Deletes current line.
`dw`	Deletes the current word.
`d)`	Deletes the rest of the current sentence.
`P`	Puts back text from the previous delete

16.1.5 Saving files and quitting `vi`

To quit `vi` without making changes to the file use the command :q!. When you type the ":", the cursor will move to the last line on the screen. In this mode, certain extended commands are available. One of them is `q!`, which quits `vi` without saving. The command `:wq` saves the file and then exits `vi`. The command `ZZ` is equivalent to `:wq`.

:w	Writes the file (saves it) while remaining in the file
:w new_file_name	Saves the current file under a new name
:wq	Writes the file and quits the `vi` session, closing the file
ZZ	Writes the file and quits the vi session, closing the file (same as :wq)
:q	Quit when you have *not* changed a file
:q!	Really quit – without saving any changes

17 Appendix B: Regulatory information

17.1.1 FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 26 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

This equipment marketed in USA is restricted by firmware to only operate on 2.4 GHz channel 1-11, and 5 GHz channel 36, 40, 44 and 48.

17.1.2 IC (Industry Canada) Statement

Operation for this device is subject to the following two conditions:

(1) this device may not cause interference and
(2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 10.31 dBi at 2.4 GHz and 9.21 dBi at 5 GHz.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding.
(Equipment (or its transmit antenna) that is installed outdoors is subject to licensing).