



Nivis Versa Router 1100

Titan - User Guide

Version 1.2

Table of Contents

1	Introduction.....	4
1.1	Document purpose.....	4
1.2	Audience.....	4
1.3	Abbreviations and acronyms.....	4
2	The Versa Router™ VR1100 “Titan” Overview and Key Features	5
2.1	About the Versa Router™ 1100 “Titan”.....	5
2.2	Platform architecture	5
2.3	The Edge Router Functional Features	8
2.4	Package content	10
2.4.1	Versa Router VR1100 Titan US	10
2.4.2	Versa Router VR1100 Titan US OEM	11
3	Getting Started	12
3.1	Power up the Versa Router™ 1100 Titan	12
3.2	Configure the SIM card.....	15
3.3	Verify the Cell backhaul starts up properly	16
3.4	Verify the Cell backhaul works using NMS	16
3.5	Verify the Cell backhaul works using the cell IPv4 accessible from the PC.....	16
3.6	Configure the PC static IP address to access the Edge Router	17
3.7	Optional: Ensure the Edge Router is accessible from PC over ETH	19
3.8	Versa Router™ 1100 Titan US hardware description	20
3.8.1	General product view	20
3.8.2	Versa Router™ 1100 Titan US.....	21
3.8.3	Versa Router™ 1100 Titan US OEM.....	22
3.8.4	Connectors, buttons, LEDs.....	23
3.8.5	The Titan “Reset to Default” button.....	26
3.8.6	Power supply specifications	26
3.9	The Edge Router (Versa Router™ 1000 Quark and Versa Router™ 1100 Titan) Software	27
4	Upgrading the Edge Router (Versa Router™ 1000 Quark and Versa Router™ 1100 Titan) components	75
4.1	Overview.....	75
4.2	Upgrading the Edge Router Transceiver firmware using Edge Router web interface	75
4.3	Upgrading the Edge Router Transceiver firmware using Edge Router /admin/ interface	75
4.4	Upgrading the Edge Router software using Edge Router web interface	75
4.5	Upgrading the Edge Router using Edge Router /admin/ interface	75

4.6	Upgrading the Edge Router software using Cloud-based NOC website	75
4.7	Upgrading the Edge Router website using Edge Router /admin/ interface.....	75
5	Configuring the Edge Router (Versa Router™ 1000 Quark and Versa Router™ 1100 Titan)	76
5.1	Overview.....	76
5.2	Accessing the configuration interface on Edge Router	76
5.3	Enable/disable DTLS on the Edge Router	77
5.4	Change the DTLS Certificate / pre-shared Key	78
5.4.1	Overview.....	78
5.4.2	Change the DTLS Key/Certificate.....	78
5.5	Change the PANA Certificate / pre-shared Join Key.....	80
5.5.1	Change the PANA Certificate.....	80
5.5.2	Change the pre-shared Join Key	81
5.6	Change the Network ID	82
5.7	Set-up Edge Router - Cloud-Based NOC communication.....	83
5.7.1	Add Edge Router in the Cloud-Based NOC Whitelist.....	83
5.7.2	Set-up Edge Router and NMS communication using VPN [RECOMMENDED]	85
5.7.3	[Alternate] Set-up Edge Router / NMS plain-text communication (Use for lab tests only)	91
6	Use Cases.....	95
6.1	Setting the PC-to-device communication using Edge Router in transparent mode	95
6.1.1	PC-to-device IPv6 communication for Windows user, VPN based.....	95
6.1.2	PC-to-device IPv6 communication for Windows user, non-VPN based	99
6.1.3	PC-to-device IPv6 communication for Linux user, VPN based	101
6.1.4	PC-to-device IPv6 communication for Linux user, non-VPN based.....	105
7	Troubleshooting	108
	Appendix A: List of Standards Supported in the Smart Object Platform	109
	Appendix B: FCC and IC Compliance Information	110

1 Introduction

1.1 Document purpose

This user guide describes the usage of Versa Router™ 1100 Titan, the outdoor version of Nivis Edge Router for Internet of Things and Smart Object technology, including hardware and software installation, configuration, use of the Network and Application Monitoring Tool and connection to Cloud-based NOC/NMS Website.

1.2 Audience

This document is intended for the users of the Versa Router™ 1100 Titan and more generally, to the users of NMS.

1.3 Abbreviations and acronyms

Versa Router™ 1000 Quark	The Versa Router™ 1000 Quark is comprised of the Phytec-designed and built phyCORE-AM335x, with “Smart Object” attached for the Transceiver.
Versa Router™ 1100 Titan	The Versa Router™ 1100 Titan is comprised of the Phytec-designed and built phyCORE-AM335x, with “Smart Object” attached for the Transceiver, along with RF amplifier, battery backup, ability to detect and report tamper and power outage, outdoor enclosure and 3G cell connectivity
VR1000	Short name for Versa Router™ 1000 Quark
VR1100	Short name for Versa Router™ 1100 Titan
Quark	Short name for Versa Router™ 1000 Quark
Titan	Short name for Versa Router™ 1100 Titan
Edge Router	Short name for Versa Router™ 1000 Quark or Versa Router™ 1100 Titan
Versa Router	Short name for Versa Router™ 1000 Quark or Versa Router™ 1100 Titan
phyCORE-AM335x	Phytec-designed and built board based on AM335x processor
Network and Application Monitoring Tool	Windows-based monitoring and management tool supplied by Nivis that will allow the end user to evaluate the performance of the Smart Object network
Smart Object	Nivis-built, manufactured, and sold MK60DN512ZVMC10 + MC12311CHN Radio Module
NMS	Network Management System – centralized management system allowing management of multiple networks controlled by VR1000 or VR1100

The document will use the term **Edge Router** when referring to either Versa Router™ 1100 Titan **or** Versa Router™ 1000 Quark – describing functionality that is common to both Routers.

2 The Versa Router™ VR1100 “Titan” Overview and Key Features

2.1 About the Versa Router™ 1100 “Titan”

The Versa Router™ 1100 Titan plays the same role and inherits all of the functional features of Versa Router™ 1000 Quark, packing additional features on top of Quark's.

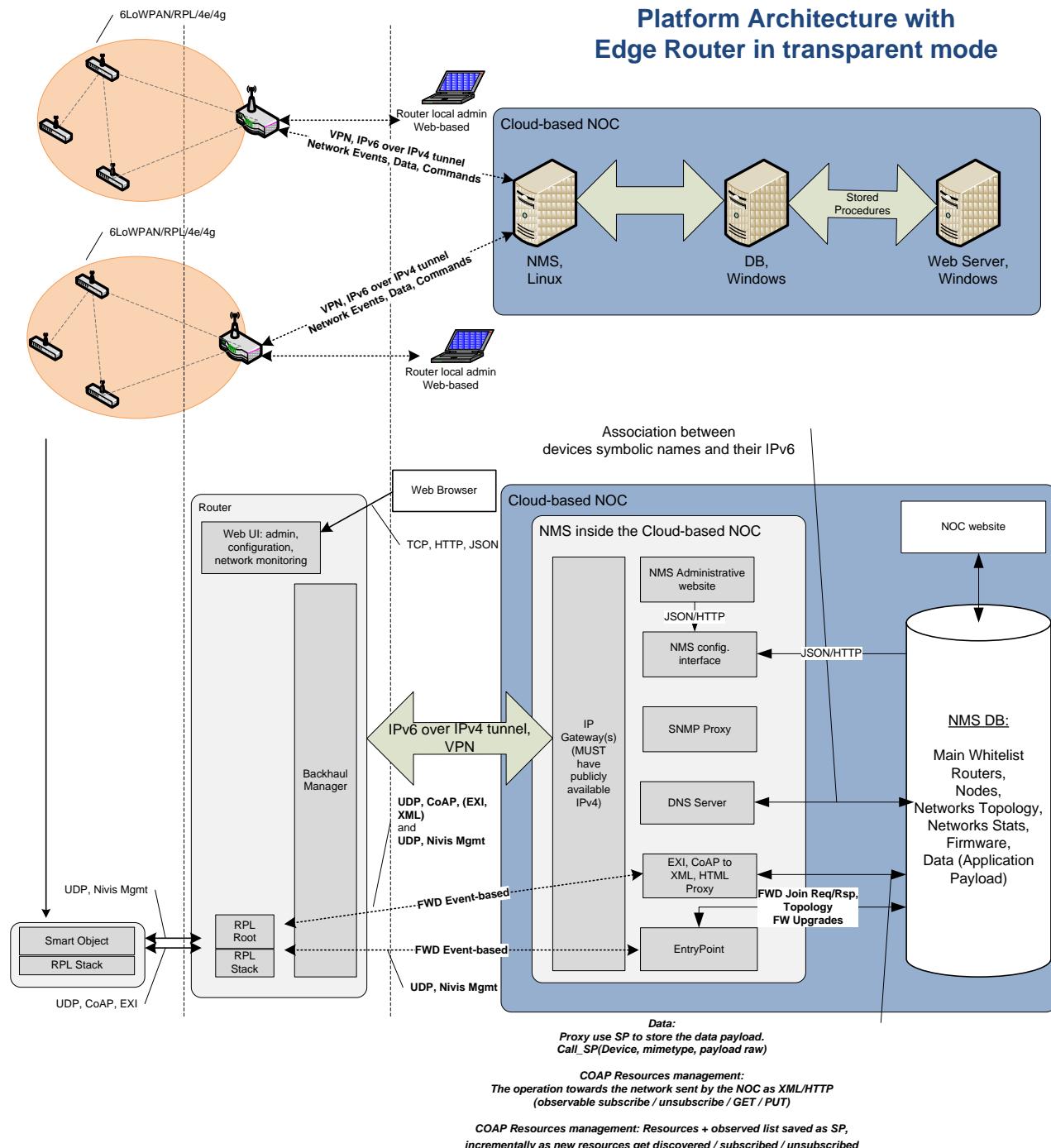
NOTE For a more detailed description of the Versa Router™ 1100 Titan hardware platform, please consult section [Versa Router™ 1100 Titan US hardware description](#)

2.2 Platform architecture

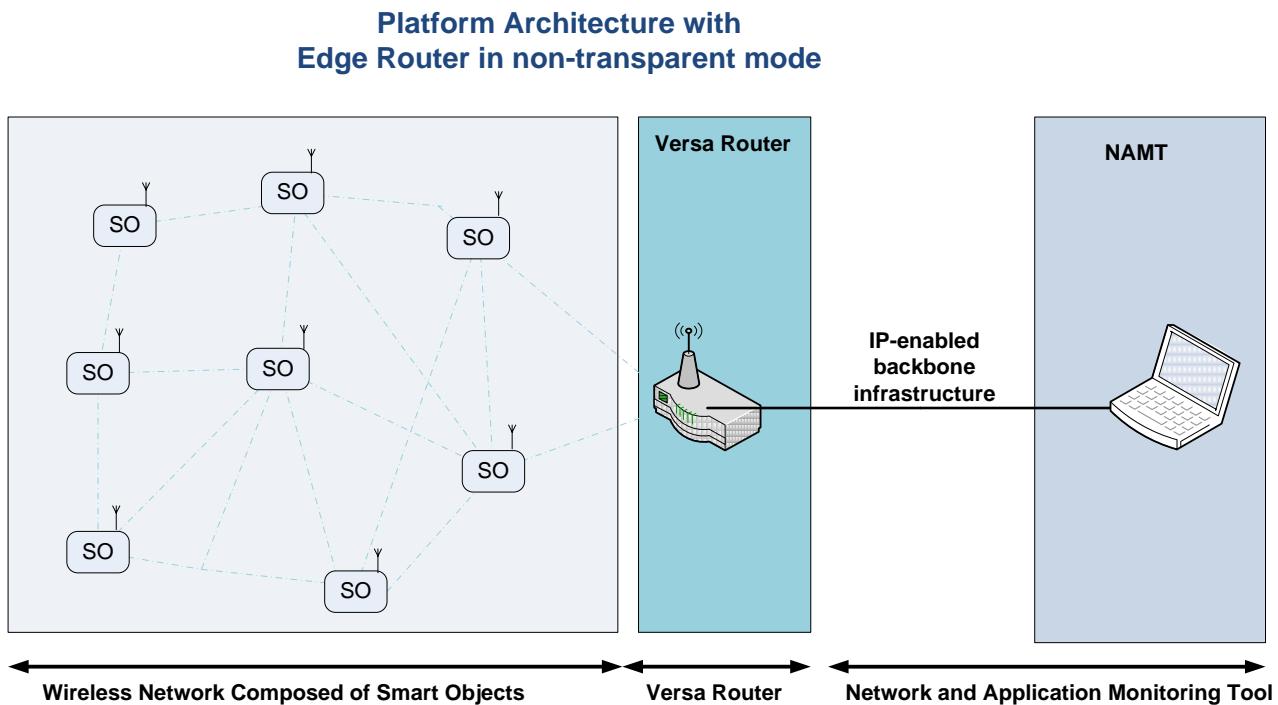
There are two possible architectures:

- With Edge Router running in “transparent” mode, used for real-life deployments. This is the normal operating topology.
- With Edge Router running in “non-transparent” mode, used for evaluation purposes. This is to be used only in laboratory

The platform architecture for Edge Router running in “transparent” mode is illustrated in the image below.



The platform architecture for Edge Router running in “non-transparent” mode is illustrated in the image below.



NOTE The NAMT uses a large amount of bandwidth for its operation. Do not connect to Versa Router™ 1100 Titan, on top of a low bandwidth or low data limit cellular data link.

The NAMT is currently not designed to handle networks larger than 500 nodes. Do not attempt to use NAMT with Titans controlling networks in excess of 500 nodes.

2.3 The Edge Router Functional Features

The Edge Router is the network entity responsible for arbitrating and managing the WLAN formed of Smart Objects. It also mitigates between the WLAN and entities present on the backbone infrastructure (such as the NAMT). The functional features of the Edge Router are described in the table below, separating the features common to VR1000 Quark and VR1100 Titan by the features specific to VR1100 Titan.

Functional Feature	Notes
Supports connectivity between the Smart Object WLAN and entities residing on the Internet.	A good example is the PC that hosts the Network and Application Monitoring Tool (NAMT).
Provides central arbitration for the WLAN formed of Smart Objects by acting as a MAC WLAN coordinator.	This is accomplished through the distribution of an 802.15.4e-compliant network maintenance slotframe.
Collects network and communication diagnostics sent by Smart Objects, such as: 1. Channel statistics 2. Neighbor-related statistics 3. Routing (RPL) -related information such as the topology of the network	Network- and communication-related statistics and parameters are displayed in the NAMT.
Acts as the link layer security manager and the termination of hop-to-hop security.	
Acts as an extraction point for application-related as well as management parameters. Parameters are extracted utilizing HTTP requests and methods via a COAP/HTTP proxy.	
Host a web server for router administration: management of network profiles, whitelist, configuration parameters, and network configuration of the Router	
VR1000 Quark: Can store application layer payloads for up to 24 hours for up to 500 Smart Objects with a reporting interval of 5 minutes . Historical data can be retrieved from HTTP/COAP Proxy using XML over HTTP requests.	Values specific for VR1000 Quark See below the storage capabilities of VR1100 Titan
Allows management for application-related parameters: <ul style="list-style-type: none"> • Allows extraction of the most recent as well as historical COAP resources, translating to XML if necessary • Allows observation of (subscription to) COAP-observable resources on the devices • Allows getting and setting of the reporting interval for observable resources 	

The features below are VR1100 Titan specific, features on top of VR1000 Quark features	VR1100 Titan specific features below
Has IP65 enclosure allowing outdoor operation	
Provides 3G cellular backhaul	Verified in US with AT&T and Emnify (MVNO)
Amplified RF, 30 dB/1W	LOS range 2.2 km / 1.35 miles
Support up to 4000 Smart Objects in RF mesh network	
Has a battery backup allowing continuous operation after the main power failed	At least 8 hours; up to 24 hours depending on operating conditions
Can store application layer payloads for at least 1 year for up to 4000 Smart Objects with a reporting interval of 6 hours . Historical data can be retrieved from HTTP/COAP Proxy using XML over HTTP requests.	
SD-card for extended storage and data/configuration back-up/restore in another unit	<p>Extended storage: Allow storing at least 1 year of CoAP data from up to 4000 Smart Objects with a reporting interval of 6 hours.</p> <p>Configuration and data back-up and restore: allow fast and simple replacement of a broken Titan: just move the SD-card to another Titan and power on the new Titan; the network will join to the new Titan and data gathering will resume automatically, no other configuration necessary.</p>
Tamper detection and reporting	
Power fail/restore detection and reporting	

2.4 Package content

2.4.1 Versa Router VR1100 Titan US

The **Versa Router VR1100 Titan US** package includes the components listed below.

Component	Quantity	Picture
Versa Router™ 1100 Titan (Pictured here with antenna mounted. The Titan is shipped with antenna un-mounted and wrapped separately)	1	
Antenna	1	
Mounting brackets	2	

2.4.2 Versa Router VR1100 Titan US OEM

The **Versa Router VR1100 Titan US OEM** package includes the components listed below.

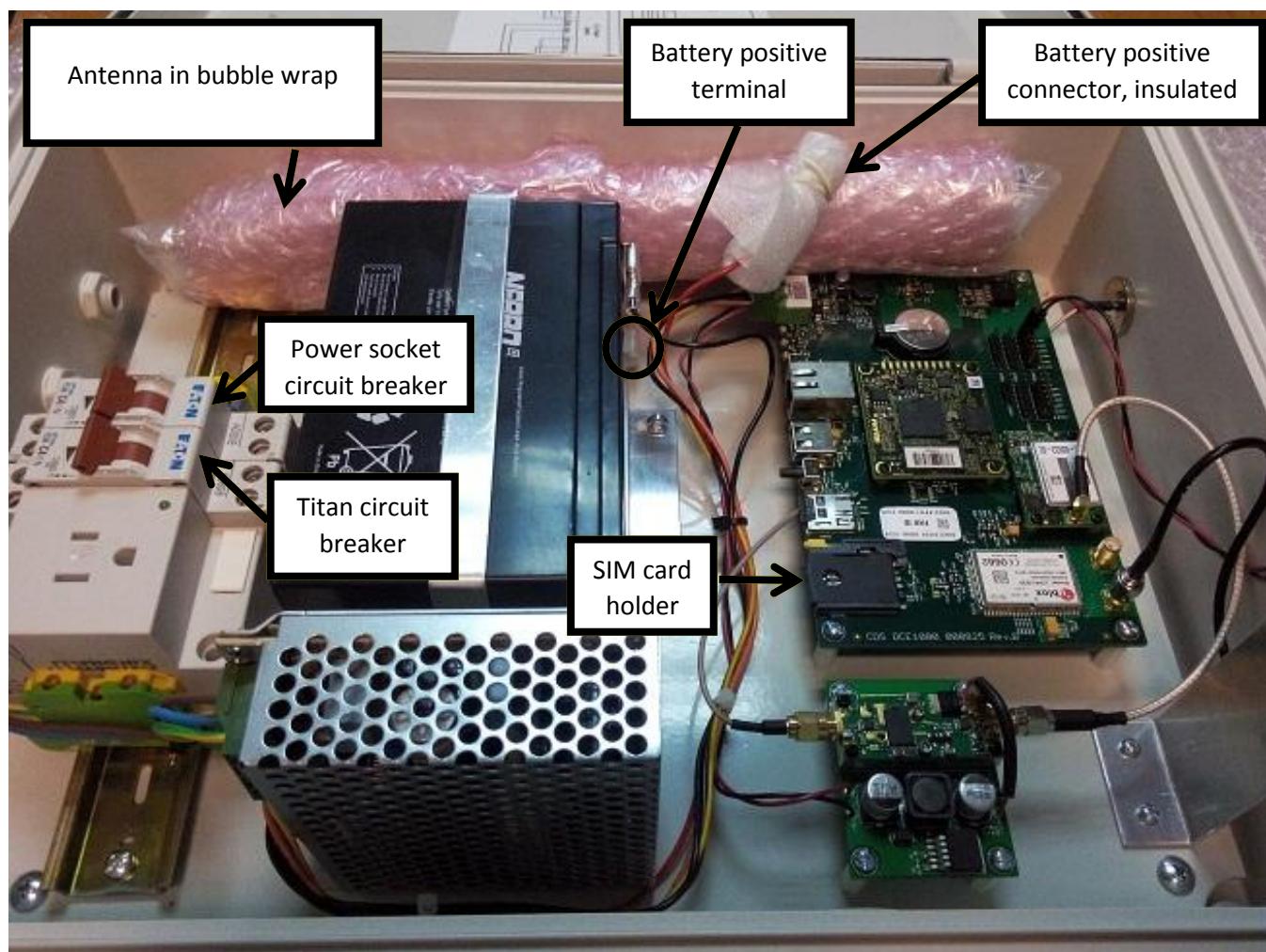
Component	Quantity	Picture
Versa Router™ 1100 Titan board	1	 A photograph of the Versa Router VR1100 Titan US OEM printed circuit board. It is a green board with various electronic components, including a central chip, capacitors, resistors, and connectors. A small white label with a red logo is visible on the left side.
RF Amplifier with associated power supply	1	 A photograph of the RF Amplifier with its associated power supply. It is a small green circuit board with two black SMA connectors at the bottom and some surface-mount components.
RF cable between Titan Radio and RF Amplifier	1	 A small icon or placeholder image showing a simple wire or cable segment.

3 Getting Started

3.1 Power up the Versa Router™ 1100 Titan

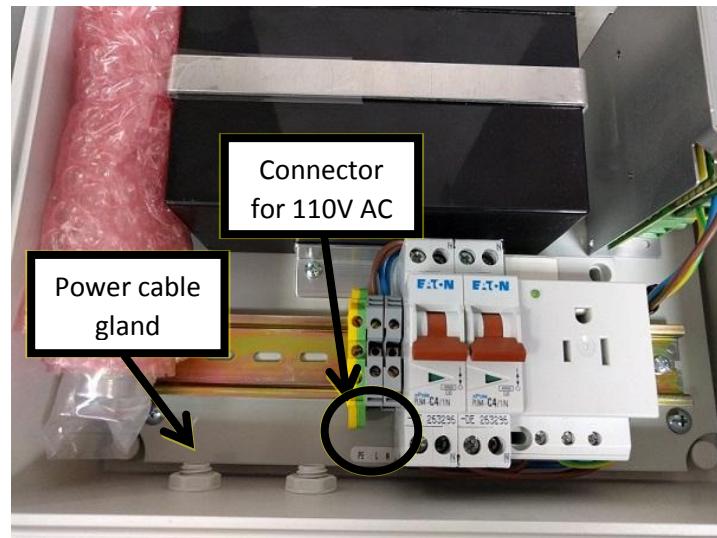
The following steps are to be executed exactly in the order listed below.

1. Take the Titan out of the box and out of the protective bubble wrap.
2. Open Titan case. The Titan is delivered with:
 - a. Antenna bubble wrapped and placed inside Titan enclosure
 - b. Battery positive connector disconnected from battery and insulated
 - c. Both automated circuit breakers switched to "OFF" position.

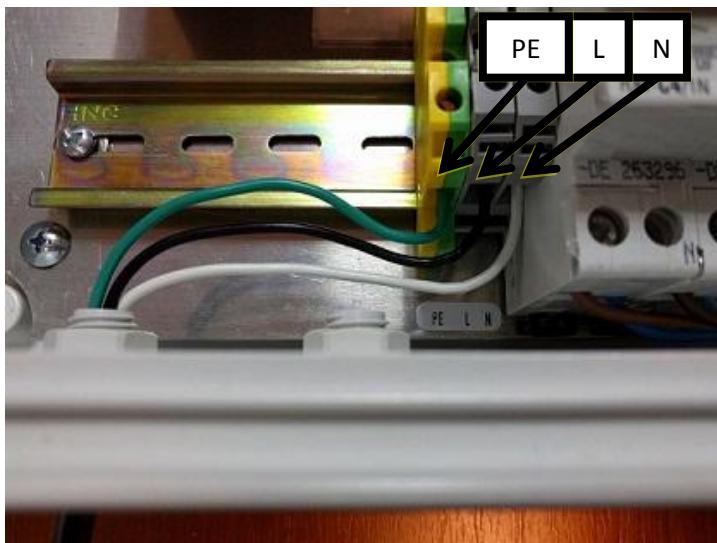


3. Take Antenna out of Titan enclosure

- Pass the power cable (max 6.5 mm / 0.256 inch) through one of the cable glands (recommend the one farthest to the circuit breakers, as it makes connecting the power easier)



- Make sure the power cable is not connected to the mains at this point!**
- Connect the power cable PE/L/N wires as indicated in the label below the connectors



- Optional** while in the lab but mandatory at deployment: unwrap the RF antenna and mount it on top of the enclosure.
- Optional**, if necessary: connect the ETH connector to Titan. This option is available only in the laboratory as it will keep the enclosure lid open; there is no provision to take the ETH cable out of the enclosure with the lid closed.

Optional while in the lab but mandatory at deployment: install an standard format SIM card (active, with data plan associated, details in the section

9. Configure the SIM card below)
10. Unwrap the battery positive connector can connect it to the battery positive terminal.
This action will start up on the Titan and power on the RF amplifier; several LED's on the Titan board will light up as well as a LED on the RF amplifier. At this point Titan draws power from the battery.
11. Connect the power cable to the mains (110 VAC) then switch the circuit breakers into "ON" position. At this point Titan draws power from the mains, and the battery gets charged from the mains.
12. **Titan is fully powered on now.**

NOTE Titan is delivered without a mains power plug/power connector, as the method to connect to the mains depend on the local conditions and the utility. The utility should use an appropriate connection cord and connection solution to the mains find appropriate, with the restriction that the power cable diameter must not exceed **6.5 mm / 0.256 inch** – that is the inner diameter of the power cable gland.

NOTE Any mechanical operation involving Titan SIM card, SD-card, RF/Cell Antennae, ETH cable must be performed with Titan **fully powered off** (Titan disconnected from mains **and** battery positive connector disconnected from battery)

3.2 Configure the SIM card

In order to use the 3G backhaul, a properly configured SIM card is necessary. The SIM card is NOT provided.

See below the steps for a properly configured SIM card.

1. Acquire a SIM card (standard format) associated with a data plan. The monthly data volume depends on the number of nodes and data acquisition frequency.
2. Activate the SIM card (cell carrier dependent procedure, not described here)
3. Get from the cell carrier the settings associated with the data plan: (APN, user, password, etc. for carrier-specific MCC/MNC)
4. In case the SIM card is delivered with PIN active: Disable the PIN associated with the SIM card. Use one of the alternatives below:
 - Use a phone to disable PIN
 - Use Titan /admin/ UI section [Edit Versa Router™ 1100 Titan SIM Settings \[Titan ONLY\]](#).
5. Titan is delivered preconfigured with a set of APN/user/pass for US cell carriers. If the APN/user/pass for carrier-specific MCC/MNC are not already configured, or are improperly configured on Titan: Configure the cell carrier settings (APN/user/pass matching the carrier-specific MCC/MNC), see section [Edit Versa Router™ 1100 Titan GPRS provider – Titan ONLY](#) below.
6. **Make sure the Titan is powered off.** Power it off if necessary: disconnect Titan from mains **and** disconnect battery positive connector from battery
7. Insert the SIM into the SIM card holder
8. At this point the Titan and its SIM card are properly configured for cell backhaul.
9. Recommended action: verify the 3G backhaul starts up and works properly, as described in the section below.

NOTE It is **strongly** recommended to use a data plan with **full unrestricted internet access** (all ports including ports below 1024, TCP/UDP/ICMP)

3.3 Verify the Cell backhaul starts up properly

1. This section only checks whether the cell connectivity is **stable** (meaning SIM was properly configured with an active data plan). It does **not** check whether the Titan is **accessible** over cellular link or whether Titan **can access** the NMS.
2. Power off Titan
3. Remove Titan ETH connection
4. Make sure a properly configured and activated SIM card is inserted in titan SIM slot
5. Power on Titan
6. Wait for about 2-3 minutes for Titan to boot up
7. Check whether Titan “WEB” blue LED is solid on – and stay on for more than a minute without turning off.

3.4 Verify the Cell backhaul works using NMS

1. Have available and running a NMS instance
2. Have Titan connected over ETH
3. Power on Titan
4. Set Titan in “transparent” mode, connecting it to the instance mentioned above
5. Power off Titan
6. Remove Titan ETH connection
7. Make sure a properly configured and activated SIM card is inserted in titan SIM slot
8. Power on Titan
9. Check whether Titan is accessible from the NMS Web interface

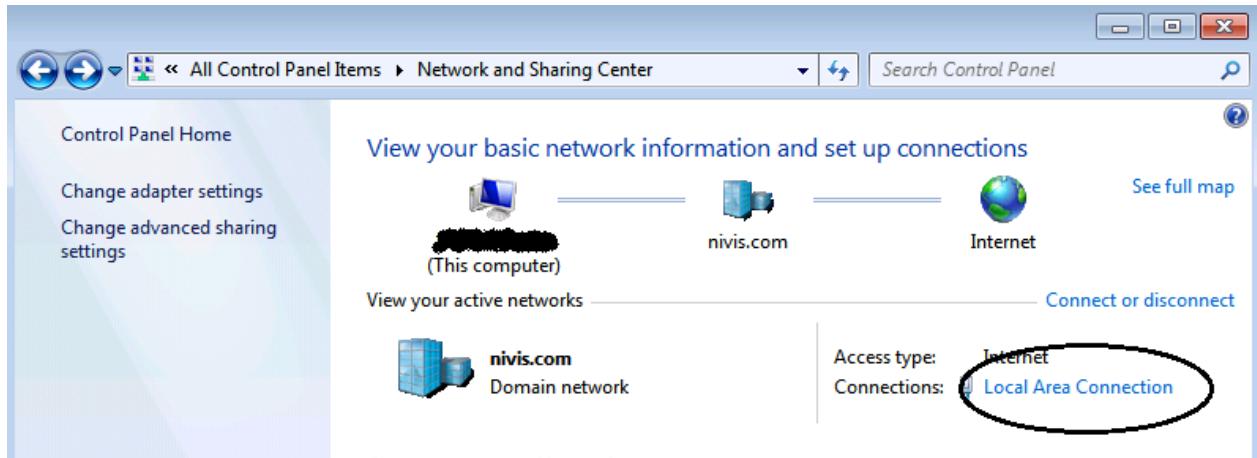
3.5 Verify the Cell backhaul works using the cell IPv4 accessible from the PC

1. The procedure below works ONLY if the cell provider has assigned an IPv4 accessible from the PC to the SIM card.
 - o One case is when the IPv4 associated with the SIM card is accessible from the Internet.
 - o Another case is when the PC itself has an IPv4 provided by a cell modem using a SIM card in the same private IP class as SIM on Titan.
2. Power off Titan
3. Remove Titan ETH connection
4. Make sure a properly configured and activated SIM card is inserted in titan SIM slot
5. Power on Titan
6. Check whether Titan Web interface is accessible using the cell provider-assigned IP4

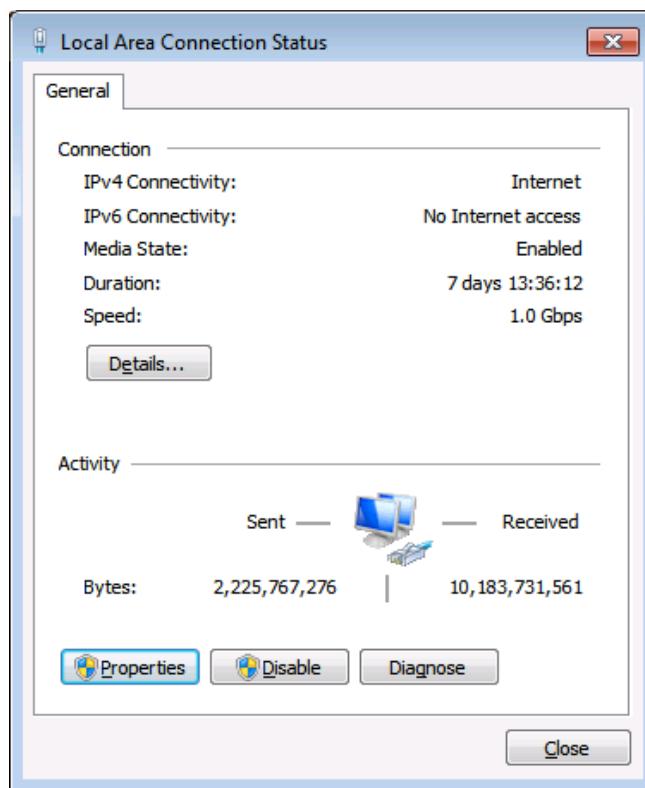
3.6 Configure the PC static IP address to access the Edge Router

Step-by-step instructions for Windows 7:

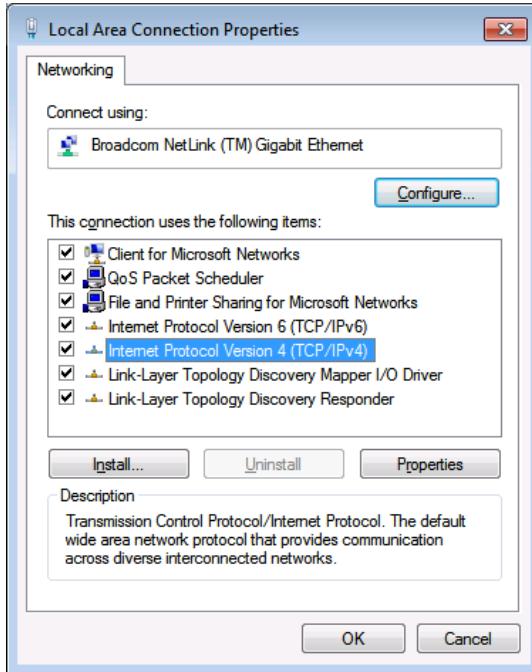
1. Open **Control Panel**→**Network and Sharing Center** and click on **Local Area Connection**.



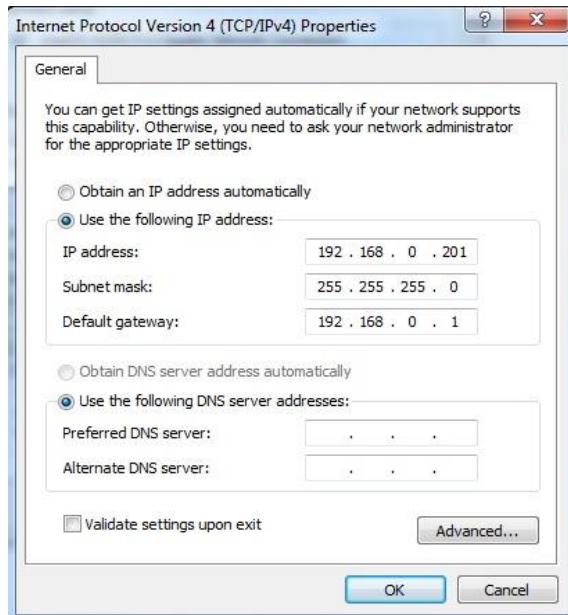
2. Click on **Properties**.



3. Click on **Internet Protocol Version 4 (TCP IPv4)** and then click on **Properties**.



4. Enter **IPv4: 192.168.0.201, Subnet Mask: 255.255.255.0, Default Gateway 192.168.0.1.** (NOTE Any other available IPv4 EXCEPT 192.168.0.101/192.168.0.1 can be used as PC IPv4).



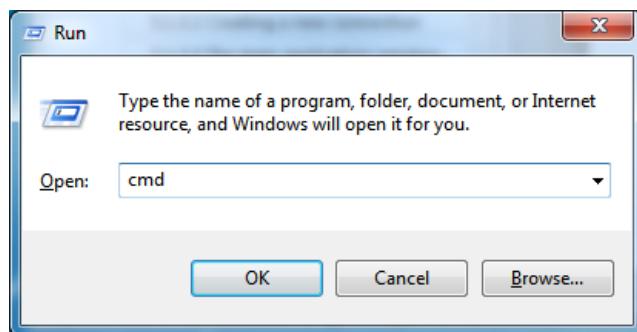
5. Check **Validate settings upon exit.**

6. Click **OK**.

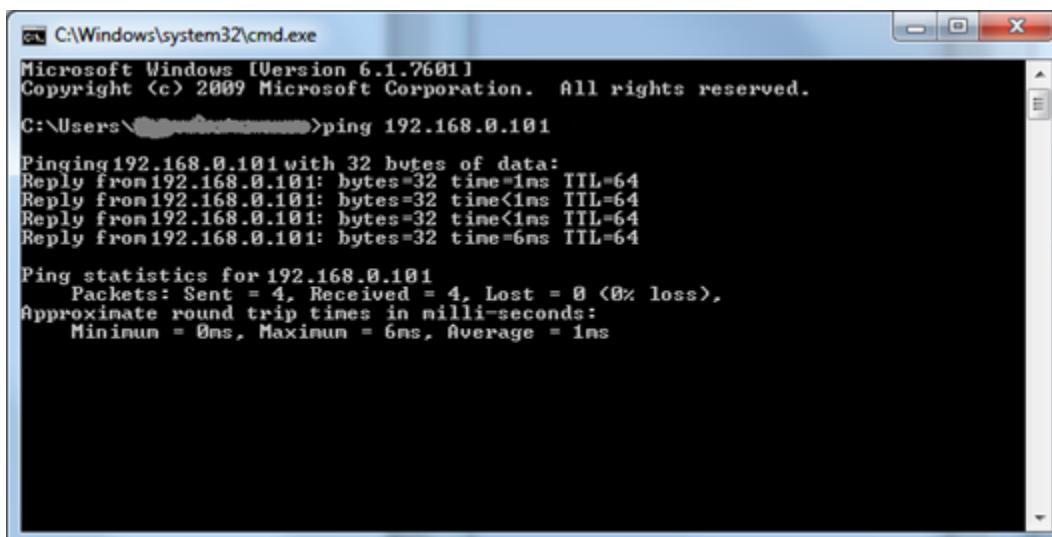
3.7 Optional: Ensure the Edge Router is accessible from PC over ETH

Use ping to verify Edge Router connectivity from the PC:

1. Click **Start**, **Run**, and type **cmd**.



2. Type **ping 192.168.0.101**. The expected result is shown below.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\[REDACTED]>ping 192.168.0.101

Pinging 192.168.0.101 with 32 bytes of data:
Reply from 192.168.0.101: bytes=32 time=1ms TTL=64
Reply from 192.168.0.101: bytes=32 time<1ms TTL=64
Reply from 192.168.0.101: bytes=32 time<1ms TTL=64
Reply from 192.168.0.101: bytes=32 time=6ms TTL=64

Ping statistics for 192.168.0.101
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

3.8 Versa Router™ 1100 Titan US hardware description

3.8.1 General product view

The Versa Router™ 1100 **Titan** is running on Phytec designed and built phyCORE-AM335x, built around the AM335x processor with the functionality of a network router, same as the Versa Router™ 1000 **Quark**. The **Titan** packs more memory and flash space and runs at a higher frequency compared to **Quark**.

The Versa Router™ 1100 **Titan** requires only a 3G SIM card and a power cord connected to the mains 110 VAC in order to run the hardware. The power cord is not provided. The Smart Object's wireless connection is established via the on-board amplified radio connected to the antenna connector on the case.

See the VR1100 datasheet on the Nivis website www.nivis.com for additional details.

3.8.2 Versa Router™ 1100 Titan US

The standard version includes the OEM version enclosed in an IP65 enclosure, adding battery back-up and power supply RF antenna, 3G antenna, plus accessories – circuit breakers, power socket. See below an image of VR1100 Titan US with enclosure lid open:

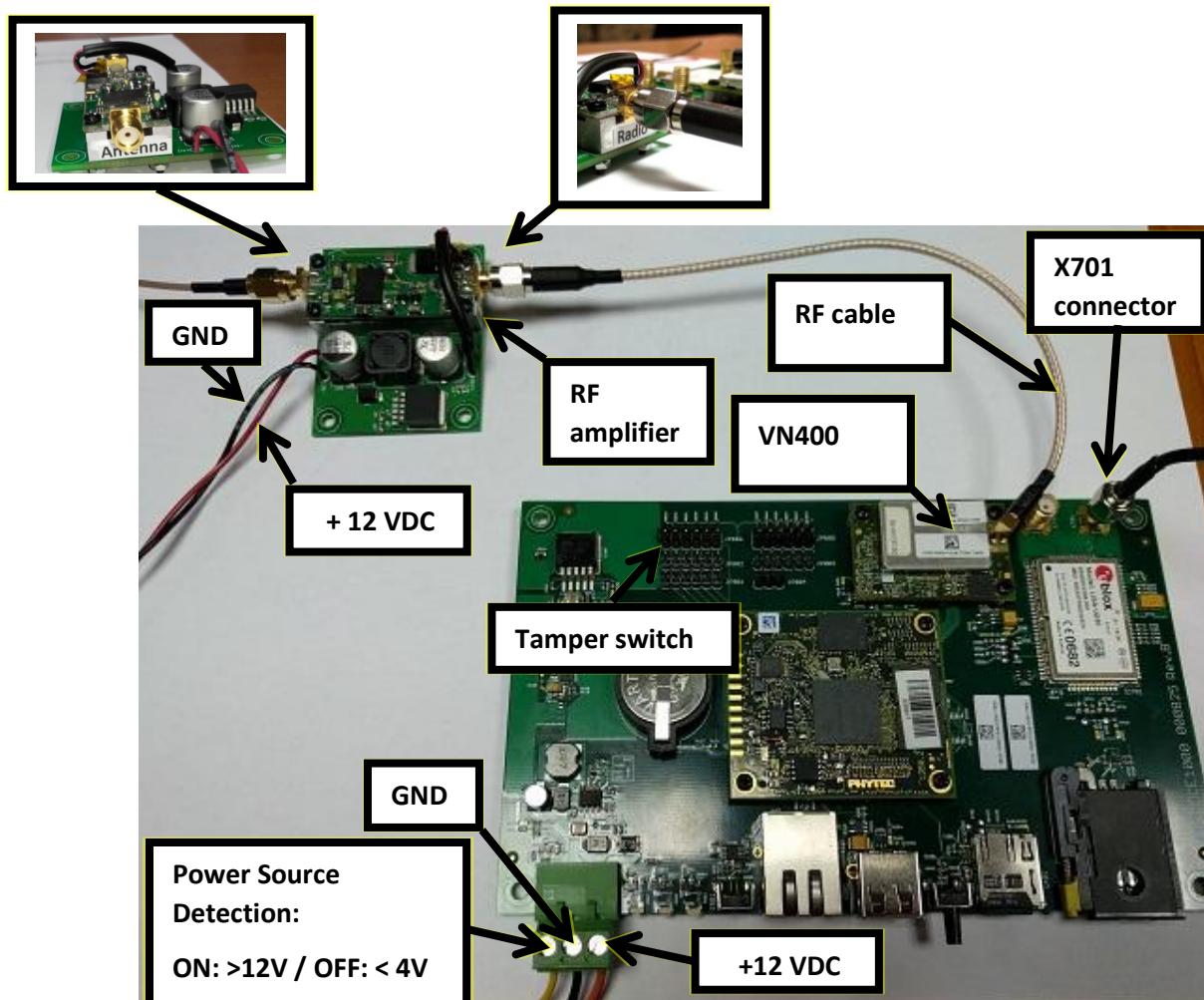


3.8.3 Versa Router™ 1100 Titan US OEM

The VR1100 Titan US OEM version includes the Titan board with VN400 radio on it, the RF amplifier and the RF cable to connect the VN400 radio to the amplifier:



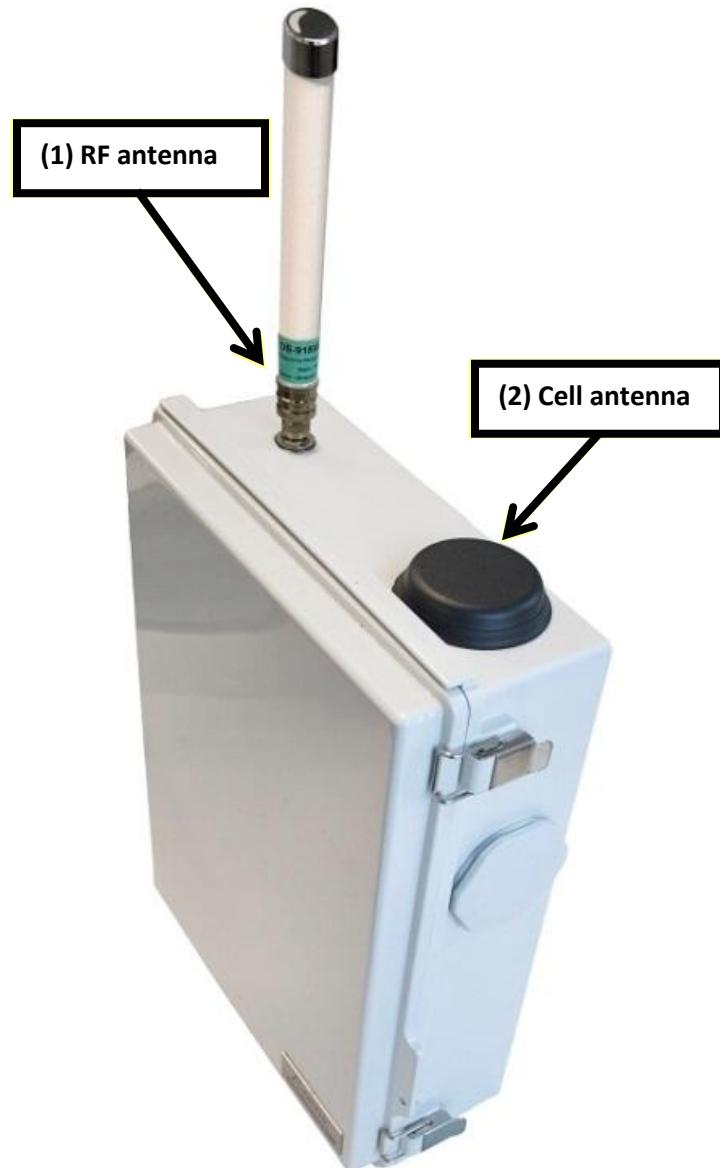
The VR1100 Titan OEM fully connected:



3.8.4 Connectors, buttons, LEDs

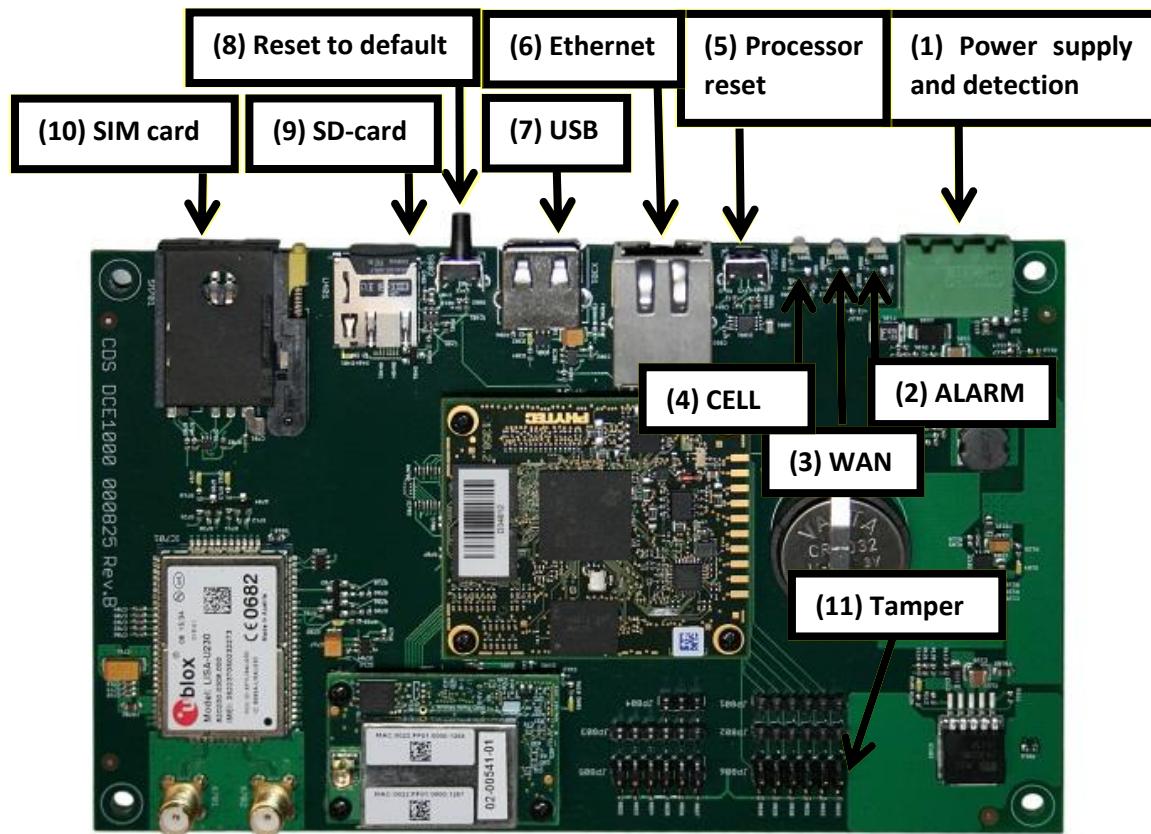
On the Titan enclosure is the antenna connector (1). The antenna is shown connected in the picture below.

Titan is delivered with cell antenna (2) already mounted. There user should not operate the cell antenna.



There are no LED/Buttons accessible on the Titan enclosure.

Inside of enclosure, the following LED's, buttons and connectors are available:



The green connector (1) in the left is for power supply connection.

There are 3 main LEDs on the Titan board next to the power supply connection: "ALARM", "WAN", and "CELL".
The other two secondary LEDs are the ETH link/activity LEDs

The "ALARM" LED (2, red) lights solid on when the SD-card is not detected or is malfunctioning.

The "ALARM" LED (2, red) is blinking while the board is in the process of reset to factory defaults.

The "WAN" LED (3, green) lights solid on when there is a NAMT or a browser connected to the Versa Router™ 1100 Titan.

The "CELL" LED (4, blue) lights solid on when the cell link is established.

To the left is the RJ-45 connector (6) for WLAN connectivity.

Next there is the USB connector. The USB currently has no functionality for Titan.

Next to the left there is the "Reset to Defaults" button (6). It serves to reset the settings to the factory defaults.
See the following section for additional details.

To the left there is the SD-card holder. It must have a working SD-card at all times.

NOTE Titan does NOT function without a properly working SD-card

Next to the SD-card holder there is the SIM holder.

NOTE Titan needs an active SIM card, with an active data plan associated, and with PIN disabled in order to activate the cell backhaul link. It also requires coverage from the SIM card provider for the same purpose.

On titan board, amplifier or power supply there are several other LED's. They have no functional significance for Titan user. It is not in the scope of this document to describe the rest of the LED's on Titan main board, power amplifier or power supply.

3.8.5 The Titan “Reset to Default” button

If the Titan network settings (for example, the IP) are lost or if for any reason the configuration becomes non-functional, you can use the “Reset to defaults” button to reset all application configurations and Quark Network configurations.

To do this, press and hold the “Reset to Defaults” button (located inside the enclosure, position 8 in the picture above). Keep the button pressed for up to 10 seconds, until the “ALARM” LED (2, red) starts blinking. At that time, the Titan connectivity settings and the application configuration are reset to factory defaults. The LED will keep blinking for 10 seconds, and then the board will perform a reboot.

A “Reset to default” action will reset the following setting to their factory default value:

- IPv4 settings
- All Application settings
- OpenVPN/DTLS certificates/configurations
- Communication profiles, including Vendor Network ID

A “Reset to default” action will NOT reset the license files existing on Titan.

NOTE After the reboot, the Titan IPv4 network configuration will be: IPv4 **192.168.0.101**, network mask **255.255.255.0**, gateway **192.168.0.1**.

3.8.6 Power supply specifications

VR1100 Titan needs a power supply of 85 – 264 VAC 50/60Hz or 120 – 370VDC, max 35W (normal consumption is 5.5W). Max power cable diameter 0.256 inch/ 6.5 mm – that is the inner diameter of the power cable gland

VR1100 OEM needs a power supply 12 VDC, max 2.6A on the green connector (1 in the image above).

NOTE Any mechanical operation involving Titan SIM card, SD-card, RF/Cell Antennae, ETH cable must be performed with Titan **fully powered off** (Titan disconnected from mains **and** battery positive connector disconnected from battery)

3.9 The Edge Router (Versa Router™ 1000 Quark and Versa Router™ 1100 Titan) Software

The software features described below are inherited by Versa Router™ 1100 **Titan** from Versa Router™ 1000 **Quark** and are available on both Versa Router™ 1000 **Quark** and Versa Router™ 1100 **Titan**, unless otherwise noted. Any features available on **Titan** only are marked clearly below.

3.9.1.1 *HTTP-COAP proxy*

The HTTP-COAP proxy is a translator from HTTP to COAP and a proxy for COAP resources.

The client apps can query directly the COAP resources on the Smart Objects using COAP; however, this is not recommended, as it may exceed with ease the bandwidth available.

We recommend sending the queries as XML on top of HTML. The proxy on the Edge Router will serve the resource from the cache or query the SO if necessary; at the same time, it will translate from COAP to HTTP. If configured, the proxy will subscribe to observable resources on the Smart Objects, further reducing the bandwidth requirements.

Advantages of using a HTTP – COAP proxy against interrogating the Smart Objects directly include:

- Controllable bandwidth requirements
- Reduced bandwidth requirements ensured through use of caching on the proxy
- Reduced bandwidth requirements ensured through use of subscription to observable resources from the proxy
- Fast development by using XML/HTTP

3.9.1.1.1 *COAP – HTTP proxy interface description*

The proxy interface allows a client application to list the observable resources, get the device list and topology, and observe resources (including the configuration of the resources observed).

3.9.1.1.2 HTTP status codes

The CoAP – HTTP status code translation is performed according to the following table.

CoAP Code	HTTP Status Code
65	201 Created
66	204 No Content
67	304 Not Modified
68	204 No Content
69	200 OK
128	400 Bad Request
129	401 Unauthorized
130	400 Bad Request
131	403 Forbidden
132	404 Not Found
133	405 Method Not Allowed
134	406 Not Acceptable
140	412 Precondition Failed
141	413 Request Entity Too Large
143	415 Unsupported Media Type
160	500 Internal Server Error
161	501 Not Implemented
162	502 Bad Gateway
163	503 Service Unavailable
164	504 Gateway Timeout
165	505 HTTP Version Not Supported

While most HTTP status codes returned are a direct translation from the CoAP corresponding response code, there are several error codes that may be sent by the proxy.

HTTP Request	HTTP Error Code	Details
Any request	504 Gateway Timeout	The request could not be handled in the configured time interval. Response string: "Gateway Timeout"
	501 Not Implemented	The request could not be parsed. Response string: "Can't parse Http request"
	400 Bad Request	The HTTP request is not valid and therefore cannot be handled. Response string: "Invalid request"
Device resource request	501 Not Implemented	The request could not be sent over the CoAP interface at this time. Response string: "Can't SendRequestToCoap"
		The requested resource could not be created locally. Response string: "Can't AddReqRspResource"
	502 Bad Gateway	Decoding error. Response string: "Can't convert Coap response to Http response, Xml failed"
	409 Conflict	A <i>no-cache</i> HTTP request was made for an observed resource. Requests for observed resources may not bypass the cache and such a request should not be attempted. Response string: "Can't bypass cache for an observed resource"
	504 Gateway Timeout	There was no response from the CoAP interface in the configured timeout interval. Response string: "Gateway Timeout"
		Another request for the same resource was already made and has not yet been answered. Response string: "Another request for this resource was sent before"
		An observable resource is in the subscribing process, and thus a new request for the resource will not be made and data will only be available once the subscription is established. Response string: "Resource is in subscription process"
Observe resources	400 Bad Request	The XML observation request was badly formed. Response string: "Invalid query"

HTTP Request	HTTP Error Code	Details
request		The individual observable element request was badly formed. Response string: "Observing resources request is bad formed"
		The XML observation request is not a PUT request. Response string: "Request is bad formed, invalid method, it should be PUT"
		The XML observation request content type is invalid. Response string: "Request is bad formed, invalid content type, it should be application/xml"
		The XML observation request content is invalid. Response string: "Request is bad formed, invalid Xml content." Response string: "Request is bad formed, error processing Xml Observation List elements" Response string: "Request is bad formed, Xml Observation List invalid finish"
Storage data retrieval request	400 Bad Request	The request query has invalid or conflicting elements. Response string: "Storage-data-get request is bad formed"
Device list request	400 Bad Request	The device list search query is badly formed. Response string: "Invalid query"

3.9.1.1.3 Communicating with HTTP CoAP Proxy

If the HTTP Client is a web-browser, the HTTP client has to manually set the proxy configuration, by setting the Proxy IP to the value of Edge Router IP, and the port to 9999.

EXAMPLE:

Considering CoAP server [2001::1:101]

Considering Edge Router (HttpCoapProxy): 10.32.0.160, listens by default on TCP port 9999

The client web browser must be configured for "Manual proxy configuration":

HTTP Proxy: 10.32.0.160 Port: 9999

3.9.1.1.4 Resources

HTTP query: http://resources

HTTP response:

```
<?xml version='1.0' encoding='utf-8'?>
<!DOCTYPE ResourceList [
<!ELEMENT ResourceList (CoAPResource)>
<!ELEMENT CoAPResource (Value)>
<!ELEMENT Value (#PCDATA)>
<!ATTLIST Value Name CDATA #IMPLIED>
<!ATTLIST Value Type CDATA #IMPLIED>
]>
<ResourceList>
    <CoAPResource>
        <Value Name='IPv6Addr' Type='BinHex'>...</Value>
        <Value Name='CoRELinkFormat' Type='String'>...</Value>
    </CoAPResource>
    <CoAPResource>
        <Value Name='IPv6Addr' Type='BinHex'>...</Value>
        <Value Name='CoRELinkFormat' Type='String'>...</Value>
    </CoAPResource>
    <CoAPResource>
        <Value Name='IPv6Addr' Type='BinHex'>...</Value>
        <Value Name='CoRELinkFormat' Type='String'>...</Value>
    </CoAPResource>
    ...
</ResourceList>
```

3.9.1.1.5 Device list

HTTP query: http://device-list(?search*)

Where search can be: MAC=HHHHHHHHHHHH or IPv6Addr=HHHHHHHHHHHHHHHHHHHHHHHHHHHH

HTTP response:

```
<?xml version='1.0' encoding='ascii'?>
<!DOCTYPE DeviceList [
<!ELEMENT DeviceList (Device)>
<!ELEMENT Device (Value)>
<!ELEMENT Value (#PCDATA)>
<!ATTLIST Value Name CDATA #IMPLIED>
<!ATTLIST Value Type CDATA #IMPLIED>
]>

<DeviceList>
    <Device>
        <Value Name='MAC' Type='BinHex'>...</Value>
        <Value Name='IPv6Addr' Type='BinHex'>...</Value>
        <Value Name='DeviceType' Type='Number'>...</Value>
        <Value Name='Status' Type='Number'>...</Value>
        <Value Name='LastComm' Type='Number'>...</Value>
        <Value Name='LastRegistration' Type='Number'>...</Value>
    </Device>
    <Device>
        <Value Name='MAC' Type='BinHex'>...</Value>
        <Value Name='IPv6Addr' Type='BinHex'>...</Value>
        <Value Name='DeviceType' Type='Number'>...</Value>
        <Value Name='Status' Type='Number'>...</Value>
        <Value Name='LastComm' Type='Number'>...</Value>
        <Value Name='LastRegistration' Type='Number'>...</Value>
    </Device>
    ...
</DeviceList>
```

NOTES

- LastComm – UTC time in seconds (since 1970) – time when last message (network or APP) was received from device
- LastRegistration - UTC time in seconds (since 1970) – time when last DAO message was received from device
- DeviceType: { 0:Any; 1:TypeNMS; 2:reserved; 3:TypeER; 4:reserved; 5:reserved; 6:TypeEndpointRPL; 7:TypeRplRoot; 8:TypeRplLocalEndpointIfUp; 9:TypeRplLocalEndpointIfDown; 10:TypeRplEndpointOnBattery; 11: TypeRplSimEndpoint}

3.9.1.1.6 Topology

HTTP query: http://topology

HTTP response:

```
<?xml version='1.0' encoding='ascii'?>
<!DOCTYPE Topology [
<!ELEMENT Topology (Device)>
<!ELEMENT Device (Value, Parents)>
<!ELEMENT Parents (Parent)>
<!ELEMENT Parent (Value)>
<!ELEMENT Value (#PCDATA)>
<!ATTLIST Value Name CDATA #IMPLIED>
<!ATTLIST Value Type CDATA #IMPLIED>
]>
```

```
<Topology>
  <Device>
    <Value Name='MAC' Type='BinHex'>...</Value>
    <Value Name='IPv6Addr' Type='BinHex'>...</Value>
    <Parents>
      <Parent>
        <Value Name='MAC' Type='BinHex'>...</Value>
        <Value Name='IPv6Addr' Type='BinHex'>...</Value>
        <Value Name='ExpirationTime' Type='Number'>...</Value>
        <Value Name='PathSequence' Type='BinHex'>...</Value>
        <Value Name='PathControl' Type='BinHex'>...</Value>
        <Value Name='Preferred' Type='Bool'>...</Value>
      </Parent>
      <Parent>
        <Value Name='MAC' Type='BinHex'>...</Value>
        <Value Name='IPv6Addr' Type='BinHex'>...</Value>
        <Value Name='ExpirationTime' Type='Number'>...</Value>
        <Value Name='PathSequence' Type='BinHex'>...</Value>
        <Value Name='PathControl' Type='BinHex'>...</Value>
```

```
<Value Name='Preferred' Type='Bool'>...</Value>
</Parent>
...
</Parents>
</Device>
...
</Topology>
```

3.9.1.1.7 Resource requests

An HTTP request for a target resource is translated into a CoAP request and then sent to the appropriate device.

The HTTP method (GET/PUT/POST/DELETE) is translated in the equivalent CoAP method.

The HTTP options are, when possible, translated into CoAP options. Otherwise they are ignored, with the exception of the cache-control options (“***Pragma: no-cache***” / “***Cache-Control: no-cache***”), which may be used to indicate cache bypass to the proxy itself and otherwise has no CoAP equivalent.

The HTTP payload is translated as CoAP payload.

HTTP request: http://[device_ipv6]/resource_path(?cmd=*)

where the optional cmd query may be as per device specification.

HTTP response:

- If the request was successful, the response will contain the device response and the corresponding [HTTP status codes](#).
- If the request could not be sent for any reason, the response will contain an appropriate status and an informative message.

EXAMPLE

http://[2001::1:101]/

http://[2001::1:101]/app/ptm

3.9.1.1.8 Observing resources

3.9.1.1.8.1 Overview

HttpCoapProxy Observation List - list of resources ([device ipv6 addr]/resource_path) which were processed by HttpCoapProxy for putting under observation.

HttpCoapProxy Observation Cache - list of resources which are put under observation by HttpCoapProxy at current moment, with their corresponding responses.

3.9.1.1.8.2 Get observation list

HTTP query : `http://observe-resources-get(?search*)`

where search can be: MAC=HHHHHHHHHHHHHH or IPv6Addr=HHHHHHHHHHHHHHHHHHHHHHHHHHHHHH

HTTP response:

List of resources which are put under observation by `HttpCoapProxy` at that moment.

This is actually the `HttpCoapProxy` Observation List in XML format.

```
<ObservationList>

    <Resource>
        <Value Name='DeviceMAC' Type='BinHex'>...</Value>
        <Value Name='DeviceIPv6Addr' Type='BinHex'>...</Value>
        <Value Name='UriPath' Type='String'>...</Value>
        <Value Name='State' Type='String'>...</Value>
    <Value Name='PubPeriod' Type='Number'>...</Value>
    </Resource>

    <Resource>
        <Value Name='DeviceMAC' Type='BinHex'>...</Value>
        <Value Name='DeviceIPv6Addr' Type='BinHex'>...</Value>
        <Value Name='UriPath' Type='String'>...</Value>
        <Value Name='State' Type='String'>...</Value>
    <Value Name='PubPeriod' Type='Number'>...</Value>
    </Resource>

    ...
</ObservationList>
```

NOTES

The “State” field can take the following values:

- “Started”
- “Can't send request”
- “Device not in Device List”
- “Waiting for response from device”
- “Device didn't respond during timeout”
- “Resource doesn't exist”
- “Resource is not observable”
- “Subscribed”
- “Unsubscribed”

The PubPeriod field value is a number that describes the publication period set by the user for that observed resource. If “0”, it means that publication period for that resource is the default one, set by the device, and can be found in the ResourceDiscovery report (<http://resources>). If not “0”, it means that the publication period was explicitly set by the user to that value.

3.9.1.1.8.3 Enable observation for target resource

HTTP query: http://observe-resources-set?enable=1&device=device_ipv6_addr&path=resource_path

HTTP response:

- If the request is well formed, a 200 "OK" "Observation request for SUBSCRIPTION passed forward" message will be retrieved to the client. This is a sign that the request was processed and HttpCoapProxy will subscribe for observing the specified resource.
- If the request is not well formed, a 400 "Bad Request" response will be retrieved.

Every time a client makes a request for a resource, http://[device ipv6 addr]/resource_path, HttpCoapProxy will look for it in its Observation Cache:

- If it is found, it will be retrieved to the client, and it means that the resource is observable and that the client or another client made an earlier request to put it under observation.
- If that resource does not exist in the HttpCoapProxy Observation Cache, the normal flow will be followed: Send Coap request, wait for Coap response, translate to Http, and send back to Http client.

NOTE

http://observe-resourcesset?enable=1&device=device_ipv6_addr&path=resource_path &pb=publish_time can be used to determine the observed resource to be publish every "publish_time" seconds.

A successful request will result in assigning the observation state "Started" for the target resource (see description in [Get observation list](#)). Once a resource is in the "Subscribed" state, it is assumed that periodic notifications will be received for it, often enough so that the proxy will always have valid cached data available (data is valid for a max-age interval as indicated by the CoAP notification, or until newer data is received). If the max-age time interval passes and there are no new notifications, the CoAP subscription may be automatically renewed depending on the configurable option ALLOW_RESUBSCRIPTION_ON_TIMEOUT (option is set to NO by default, meaning subscription is NOT renewed).

3.9.1.1.8.4 Disable observation for target resource

HTTP query: http://observe-resources-set?disable=1&device=device_ipv6_addr&path=resource_path

HTTP response:

- If the request is well formed and the resource is found in the Observation List, a 200 "OK" "Observation request for UNSUBSCRIPTION passed forward" message will be retrieved to the client. This is a sign that the request was processed and the HttpCoapProxy will unsubscribe from observing specified resource.
- If the request is well formed, but the resource is not found in the Observation List, a 200 "OK" "Observation request for UNSUBSCRIPTION wasn't passed forward, maybe resource is not in observation list" message will be retrieved to client.
- If the request is not well formed, a 400 "Bad Request" response will be retrieved.

3.9.1.1.8.5 Set observation for multiple resources

HTTP PUT query: http://observe-resources-set-xml

Where query content is an XML file with following format:

```
<ObservationListSet>

    <Resource>
        <Value Name='DeviceIPv6Addr' Type='BinHex'>...</Value>
        <Value Name='UriPath' Type='String'>...</Value>
        <Value Name='Action' Type='String'>...</Value>
    </Resource>

    <Resource>
        <Value Name='DeviceIPv6Addr' Type='BinHex'>...</Value>
        <Value Name='UriPath' Type='String'>...</Value>
        <Value Name='Action' Type='String'>...</Value>
    </Resource>

    ...
</ObservationListSet>
```

NOTE

Action - is a string which defines the type of action that HttpCoapProxy should take on the specified resource (Enable – set as observable, HttpCoapProxy will subscribe for that resource, Disable – unset, HttpCoapProxy will unsubscribe from observing that resource)

HTTP response :

- If XML file is well formed then a 200 "OK" "XML observation list processed" will be sent back to client;
- If XML file is not well formed, 400 "Bad Request" response will be retrieved.

3.9.1.1.8.6 Retrieving data history

HTTP query: http://storage-data-get/(?device=device_ipv6_addr&since=time_since&until=time_until&oldest/newest=N/path=resource_path)

- Query may specify “device”
- Query may specify “since”, “until”, both of them or none.
- If query specified device one of “oldest”, “newest” queries may be specified.
- Query may specify a “path” containing a target resource path.

HTTP response:

- If request is well formed, HttpCoapProxy will retrieve an XML with history data which is stored for *device_ipv6_addr* device, from *time_since* and until *time_until*; *time_since* and *time_until* must be specified in UNIX timestamp format. If both “since” and “until” queries are missing, will be retrieved an XML with all history data which is stored for *device_ipv6_addr* device; this initial XML report will contain a number of X records. If “oldest” query is specified, the XML report will contain only first *N* records from X (or X if *N* >X), which represent the oldest records from the initial report. If “newest” query is specified, the XML report will contain only last *N* records from X (or X if *N* >X), which represent the newest records from the initial report;
- If path is specified, the proxy will perform a search using the provided path filter.
- If no *device_ipv6_addr* is provided, the proxy will provide the history for the entire storage.
- If no *device_ipv6_addr* is provided, “oldest” and “newest” queries do not apply.
- If storage for *device_ipv6_addr* device doesn’t exist, “Storage not found” response will be retrieved;
- If request is not well formed, 400 “Bad Request” response will be retrieved, with the information “Storage-data-get request is bad formed”.

Each record from the response XML has the following form:

```
<Record>
  <uriPath>Path</uriPath>
  <e t="timestamp"><Application v="value"/></e>
</Record>
```

If device is provided, the response XML will have the following form:

```
<DataRetrieving>
  <Record>
    <uriPath>path</uriPath>
    <e t="timestamp"><Application v="value"/></e>
  </Record>
  ...
  <Record>
```

```
<uriPath>path</uriPath>
<e t="timestamp"><Application v="value"/></e>
</Record>
</DataRetrieving>
```

If device is not provided, the response will have the following form:

```
<DataRetrieving>
<Device uriHost=device_ip>
    <Record>
        <uriPath>path</uriPath>
        <e t="timestamp"><Application v="value"/></e>
    </Record>
    ...
    <Record>
        <uriPath>path</uriPath>
        <e t="timestamp"><Application v="value"/></e>
    </Record>
<Device>
...
<Device uriHost=device_ip>
    <Record>
        <uriPath>path</uriPath>
        <e t="timestamp"><Application v="value"/></e>
    </Record>
    ...
    <Record>
        <uriPath>path</uriPath>
        <e t="timestamp"><Application v="value"/></e>
    </Record>
<Device>
</DataRetrieving>
```

EXAMPLES of requests

<http://storage-data-get/?device=2001::3&since=1358438082&until=1358438277>

<http://storage-data-get/?device=2001::3&since=1358438082&until=1358438277&oldest=5>

<http://storage-data-get/?device=2001::3&newest=10>

<http://storage-data-get/?device=2001::3& path=/app/sw>

<http://storage-data-get/?path=/app/sw>

<http://storage-data-get/>

EXAMPLE of a record in response XML:

```
<Record>
  <uriPath>/app/sw</uriPath>
  <e t="1358831522"><Sw v="1"/></e>
</Record>
```

3.9.1.2 Configuration and administration of the Edge Router

3.9.1.2.1 Overview

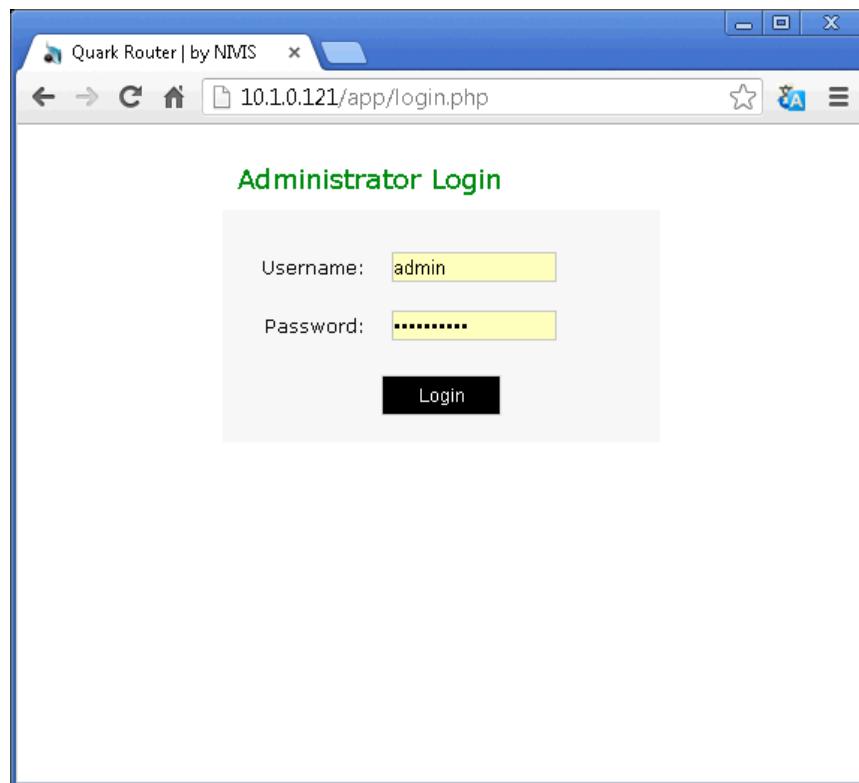
Web-based administration is the *preferred* method for administration/configuration of the Edge Router. It requires a web browser and the IP of the Edge Router.

The Versa Router™ 1000 **Quark** must be connected to the local LAN and then powered on.

The Versa Router™ 1100 **Titan** must be powered on and either connected to the local LAN or connected to 3G cell.

The IPv4 of the Edge Router must be accessible from the PC where the browser is running.

The administration website for the Edge Router can be accessed by pointing a web browser to the Edge Router IP.



Login with username: **admin** and password: **adminadmin**.

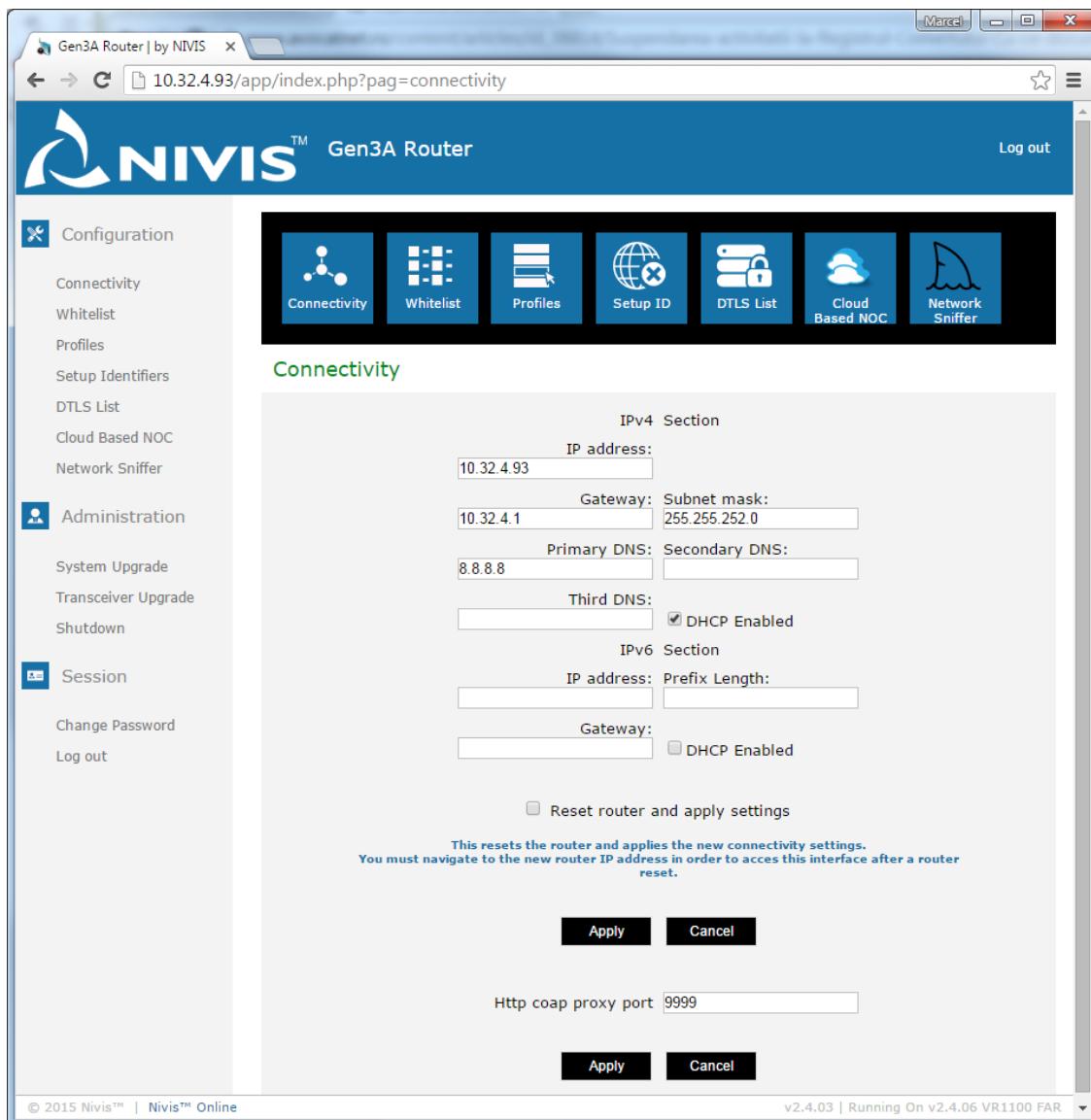
After login, the website shows the configuration/connectivity page.

All of the website pages are accessible through the left-hand menu.

All of the pages of the current section are available through the metro-style menu at top of the page.

3.9.1.2.2 Configuring the Edge Router Connectivity settings

Click on **Connectivity** in the **Configuration** section.



The screenshot shows the NIVIS Gen3A Router web interface. The left sidebar has sections for Configuration (Connectivity, Whitelist, Profiles, Setup Identifiers, DTLS List, Cloud Based NOC, Network Sniffer), Administration (System Upgrade, Transceiver Upgrade, Shutdown), and Session (Change Password, Log out). The main content area is titled 'Connectivity'. It contains two sections: 'IPv4 Section' and 'IPv6 Section'. In the IPv4 section, fields include IP address (10.32.4.93), Gateway (10.32.4.1), Subnet mask (255.255.252.0), Primary DNS (8.8.8.8), Secondary DNS (empty), Third DNS (empty), and a checked checkbox for DHCP Enabled. In the IPv6 section, fields include IP address (empty), Prefix Length (empty), Gateway (empty), and an unchecked checkbox for DHCP Enabled. Below these sections is a note: 'This resets the router and applies the new connectivity settings. You must navigate to the new router IP address in order to access this interface after a router reset.' At the bottom are 'Apply' and 'Cancel' buttons, and a field for 'Http coap proxy port' set to 9999.

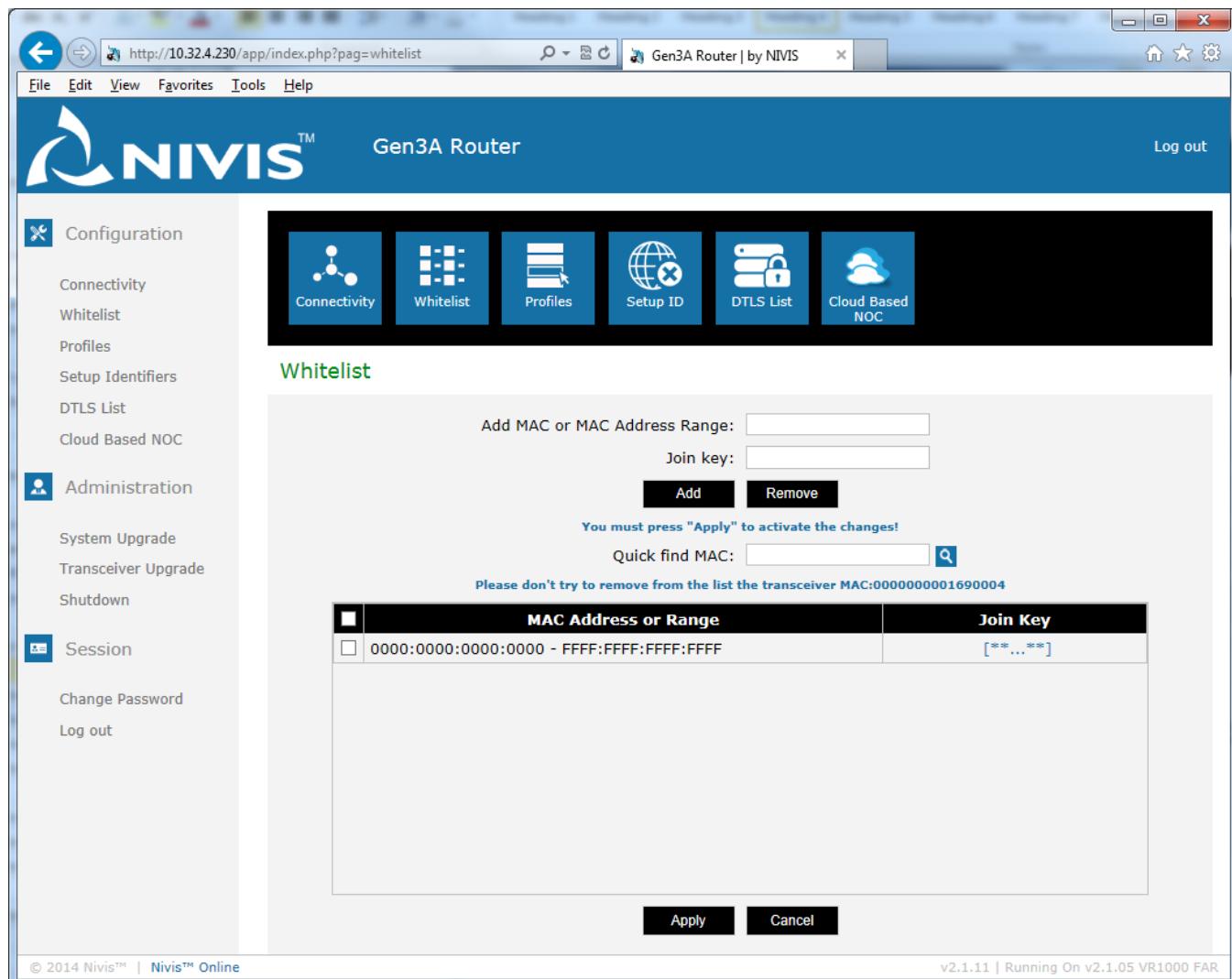
This allows the user to choose between statically allocated IPv4/IPv6 and dynamically allocated IPv4/IPv6 (by DHCP) for the Edge Router; set the static IPv4/IPv6, network mask, gateway, and DNS; and change the HTTP/COAP Proxy port.

WARNING: This page is for advanced users only – do not use it unless you know precisely how to configure the network. Any invalid values may render the router dysfunctional, or may cause difficult-to-trace malfunctions.

NOTE Make sure you are not causing IP conflicts when you make changes.

3.9.1.2.3 Configuring the Edge Router Whitelist

Click on **Whitelist** in the **Configuration** section.



The screenshot shows the Gen3A Router web interface with the URL <http://10.32.4.230/app/index.php?pag=whitelist>. The left sidebar has sections for Configuration (Connectivity, Whitelist, Profiles, Setup Identifiers, DTLS List, Cloud Based NOC), Administration (System Upgrade, Transceiver Upgrade, Shutdown), and Session (Change Password, Log out). The main content area is titled "Whitelist". It contains fields for "Add MAC or MAC Address Range:" and "Join key:", with "Add" and "Remove" buttons. A note says "You must press "Apply" to activate the changes!". Below is a table with one entry:

	MAC Address or Range	Join Key
<input type="checkbox"/>	0000:0000:0000:0000 - FFFF:FFFF:FFFF:FFFF	[**...**]

Buttons at the bottom are "Apply" and "Cancel".

The whitelist is the list with devices accepted in the network and their respective join keys. Devices are specified by their MAC addresses. There are two ways to specify the whitelist: by specifying each MAC individually or by using a MAC range.

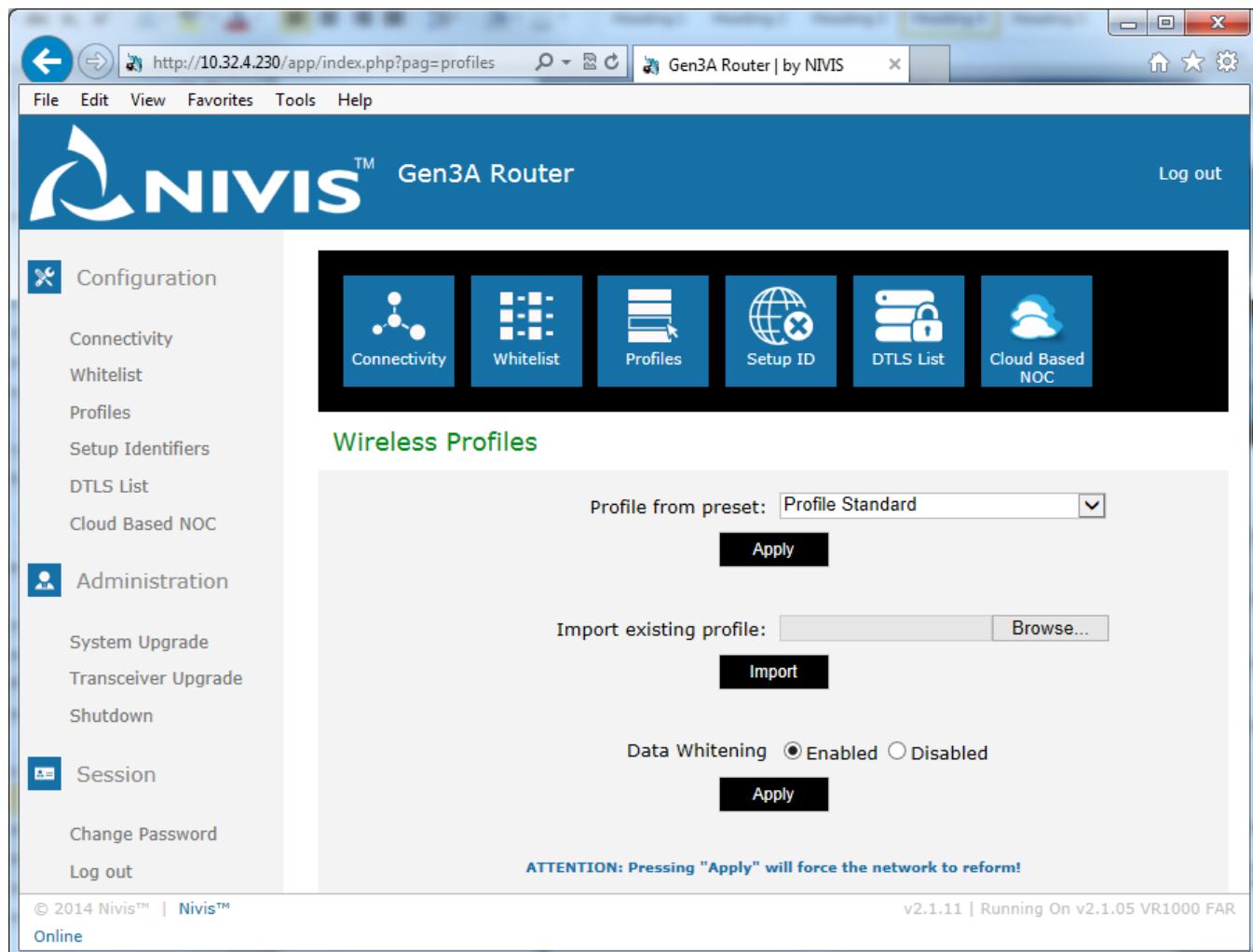
WARNING The Transceiver MAC must be present always in the whitelist, with the default join key set at Production.

The user is NOT allowed to remove the Transceiver MAC from the whitelist.

The user is NOT allowed to modify the Transceiver join key in the whitelist.

3.9.1.2.4 Configuring the Edge Router Profiles

Click on **Profiles** in the **Configuration** section.



The screenshot shows the NIVIS Gen3A Router web interface. The left sidebar has sections for Configuration (Connectivity, Whitelist, Profiles, Setup Identifiers, DTLS List, Cloud Based NOC), Administration (System Upgrade, Transceiver Upgrade, Shutdown), and Session (Change Password, Log out). The main content area is titled "Wireless Profiles". It includes a dropdown menu "Profile from preset: Profile Standard" with an "Apply" button, a "Import existing profile:" field with a "Browse..." button and an "Import" button, and a "Data Whitening" section with radio buttons for "Enabled" (selected) and "Disabled". At the bottom, there is a warning: "ATTENTION: Pressing "Apply" will force the network to reform!". The footer shows copyright information: "© 2014 Nivis™ | Nivis™ Online" and "v2.1.11 | Running On v2.1.05 VR1000 FAR".

This allows switching between “Demo” setup (small network: up to 10 devices, fast join), “Standard” setup (average network size: up to 100 devices, average join), “Large” setup (large network size, up to 500 devices). This also enables users to load a custom profile file.

The **Versa Router™ 1100 Titan** has two more profile available: extra-large (up to 1000 devices) and huge (up to 4000 devices)

On this page, the user can also enable/disable the “Data whitening” feature.

NOTE Use only Nivis-provided profile files. Do not edit Nivis-provided profile files.

3.9.1.2.5 Configuring the Edge Router Identifiers

Click on **Setup Identifiers** in the **Configuration** section.



The screenshot shows the NIVIS Gen3A Router configuration interface. The left sidebar contains navigation links for Configuration, Connectivity, Whitelist, Profiles, Setup Identifiers, DTLS List, and Cloud Based NOC. Under Administration, there are links for System Upgrade, Transceiver Upgrade, and Shutdown. Under Session, there are links for Change Password and Log out. The main content area is titled "Setup Identifiers for 10.32.4.230". It displays fields for FAR ID (":00fa:0230") and FAR ID on RF (":00fa:0231"). Below these are fields for Pan ID (230) and Vendor Network ID (230), each with a checkbox for "Based on FAR ID". A field for Hopping Sequence ID (230) also has a "Based on FAR ID" checkbox. A note at the bottom states "To activate these settings you must reboot your router." with "Apply" and "Cancel" buttons. The footer includes copyright information (© 2014 Nivis™ | Nivis™ Online) and system details (v2.1.11 | Running On v2.1.05 VR1000 FAR).

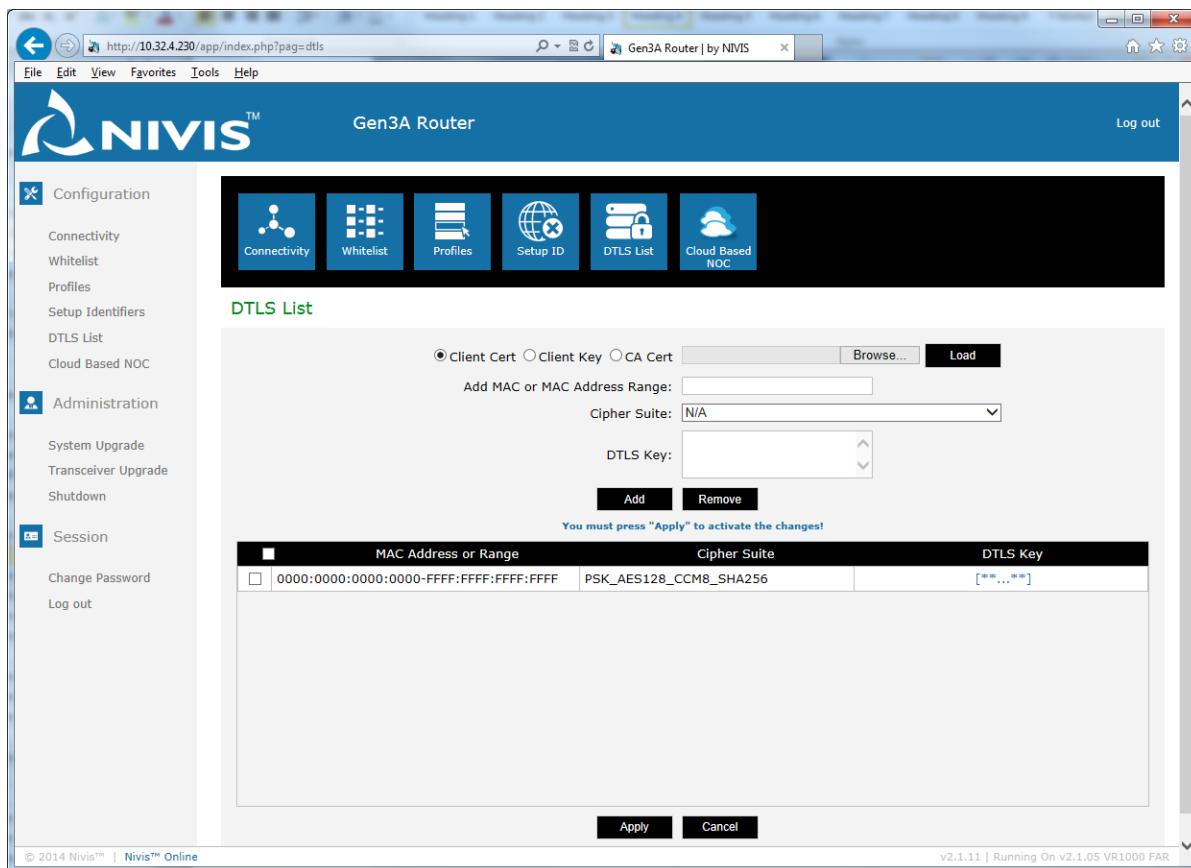
The default setup identifiers need to be changed **only** if you have several collocated networks/Quarks or Titans. In this case, each collocated Edge Router must have its own unique set of identifiers.

For ease of configuration, use the “Based on FAR ID” checkbox where available.

WARNING Do not change the variables FAR ID and FAR ID on RF under any circumstance.

3.9.1.2.6 Configuring the Edge Router DTLS list

Click on **DTLS List** in the **Configuration** section.



	MAC Address or Range	Cipher Suite	DTLS Key
<input type="checkbox"/>	0000:0000:0000:FFFF:FFFF:FFFF:FFFF	PSK_AES128_CCM8_SHA256	[***...***]

On this page, the user can load certificates and configure the DTLS list.

User actions available on this page:

- **Load:** The user will select one of the three radio buttons (ClientCert, ClientKey, or CA Cert), will choose a local .pem file, and then will load the certificate on the router.
- **Add:** The Mac, Cipher Suit, and DTLS Key fields will be validated and a new entry will be added to the table.
- **Remove:** The rows with the checkbox checked will be removed.
- **Apply:** The changes will be saved on the router.
- **Cancel:** The pending changes will be removed and the table will be reloaded from the router.
- **Select from table** (by clicking in the checkbox or on the row): The selected MAC Address or Range will be loaded in the textbox from above; the corresponding Cipher Suite will be loaded in the drop down list from above; and the DTLS key will not be loaded. Also, the selected device details will be bolded in the table.
- **Update:** If the user will edit the loaded data (or input a new key), the Add button will be renamed Update and will trigger the update in the table.

Keys will be used only if the Cipher Suite is one of the following:

- PSK_NULL_SHA256
- PSK_AES128_CCM_SHA256
- PSK_AES128_CCM8_SHA256

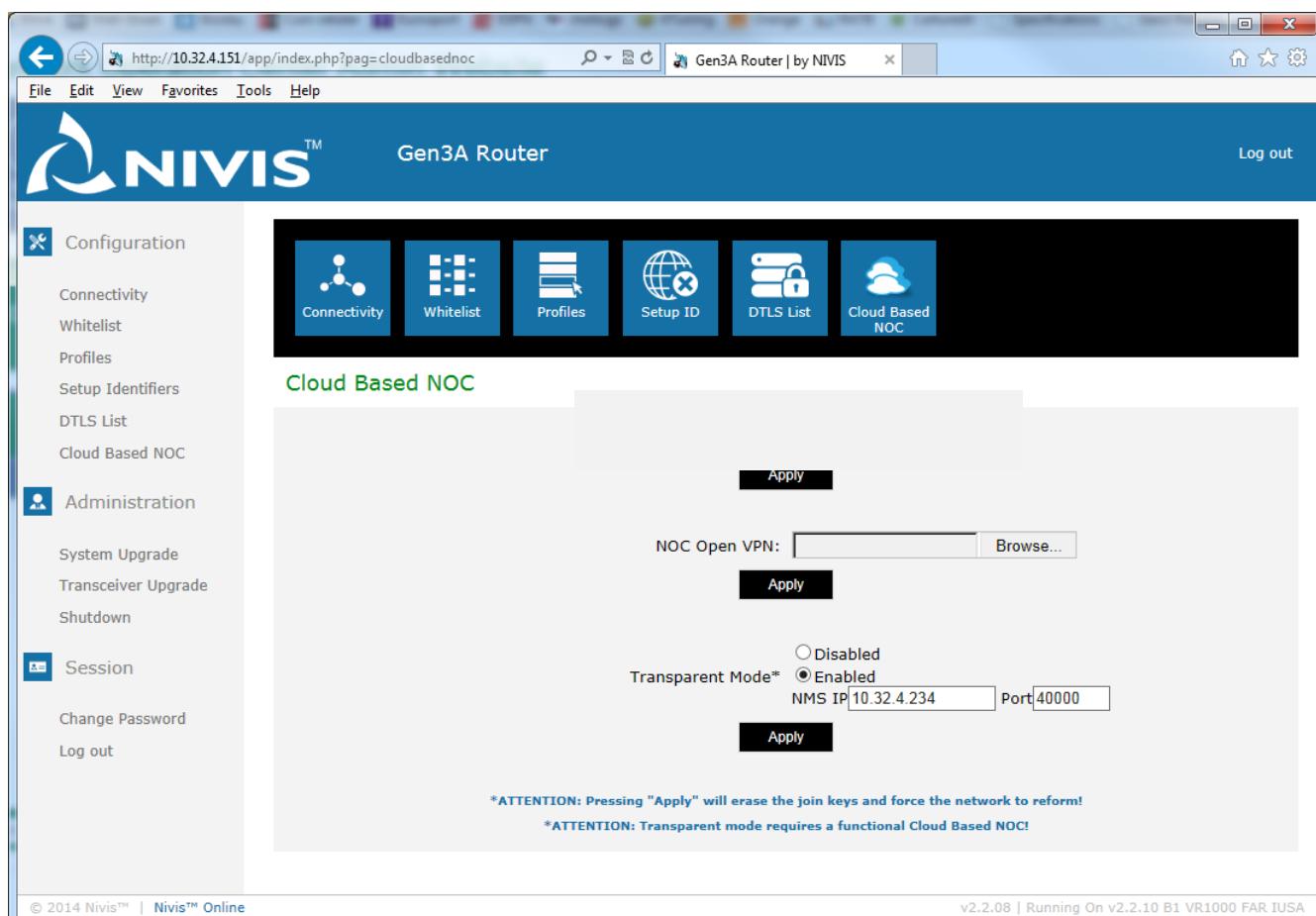
The Cipher Suite “ECDHE_ECDSA_AES128_CCM8_SHA256” uses a Certificate, not a Key.

The Cipher Suite “N/A” does not use a Key or Certificate.

3.9.1.2.7 Configuring the Edge Router Transparent Mode - connection to Cloud-Based NOC

- The Edge Router can be configured through Edge Router website to work in two different modes:
 - Standalone gateway
 - Router connected to the NMS (transparent mode enabled)
- When operating as a standalone gateway, the Edge Router is offering the following functionalities:
 - Resource directory
 - HTTP-CoAP Proxy
 - Data caching and storage
 - Support for nodes firmware upgrade
 - Support for NAMT for network monitoring, management, configuration, topology view, etc
- When operating connected to Nivis NMS the functionalities above move to the NMS and are no longer available on the Edge Router
- Main common functionalities:
 - Border router for 6lowpan/RPL network, WPAN coordinator
 - IP Routing
 - Name service (DNS)

Click on “Cloud Based NOC” link in “Configuration” section. This link is available only for routers with “Cloud Based NOC” capability.



The screenshot shows the NIVIS Gen3A Router configuration interface. The left sidebar contains navigation links for Configuration (Connectivity, Whitelist, Profiles, Setup Identifiers, DTLS List, Cloud Based NOC), Administration (System Upgrade, Transceiver Upgrade, Shutdown), and Session (Change Password, Log out). The main content area is titled "Gen3A Router" and "Cloud Based NOC". It features a toolbar with icons for Connectivity, Whitelist, Profiles, Setup ID, DTLS List, and Cloud Based NOC. Below the toolbar, there is a "Cloud Based NOC" section with an "Apply" button. Further down, there is a "NOC Open VPN:" field with a "Browse..." button, another "Apply" button, and a "Transparent Mode*" section with radio buttons for "Disabled" and "Enabled" (which is selected). Below that, there are fields for "NMS IP" (10.32.4.234) and "Port" (40000), followed by another "Apply" button. At the bottom, there are two warning messages: "*ATTENTION: Pressing "Apply" will erase the join keys and force the network to reform!" and "*ATTENTION: Transparent mode requires a functional Cloud Based NOC!". The footer of the page includes copyright information ("© 2014 Nivis™ | Nivis™ Online") and system details ("v2.2.08 | Running On v2.2.10 B1 VR1000 FAR IUSA").

User actions available on this page:

- Upload NOC Open VPN certificates.
- Set transparent mode ON (for this the NMS IP and Port are required) or OFF.

When transparent mode is ON, the user cannot do the following actions:

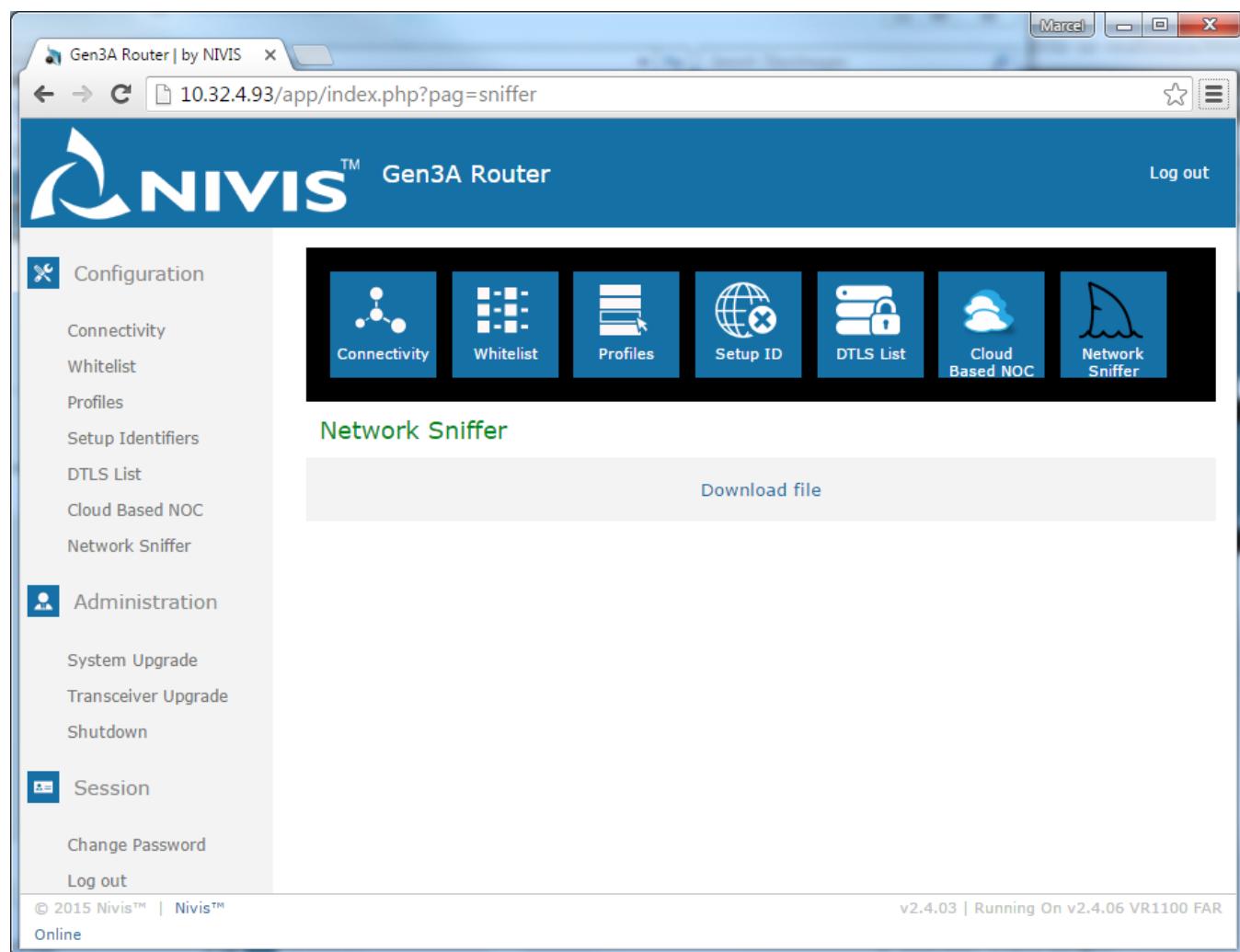
- Modify whitelists in “Whitelists” page.
- Modify DTLS lists in “DTLS List” page.
- Load certificates in “DTLS List” page.

3.9.1.2.8 Downloading the Network Sniffer settings

User actions available on this page:

- Download the settings to use on Network Sniffer.

The settings will configure the Network Sniffer to be able to monitor the network controlled by current Titan.

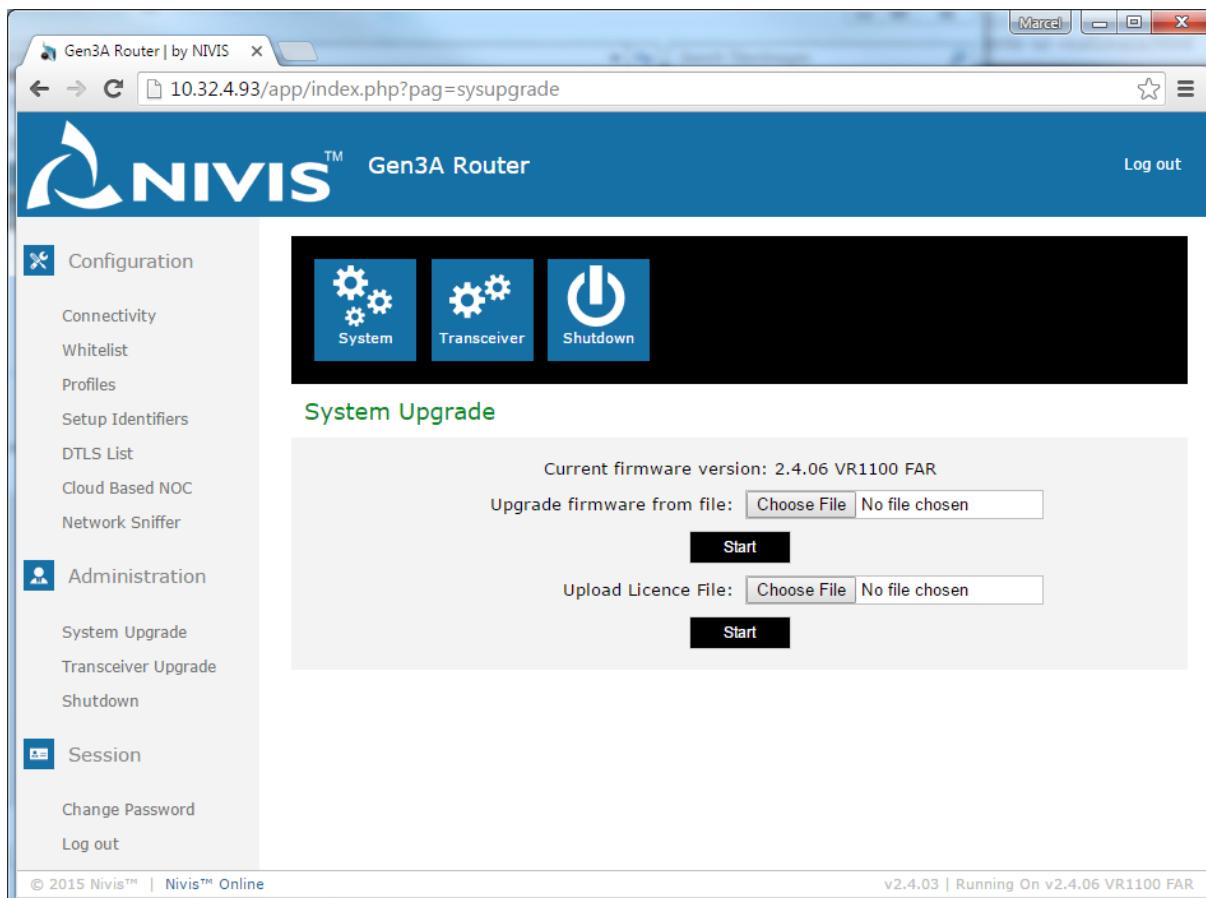


The screenshot shows the Gen3A Router web interface. At the top, there is a navigation bar with a back button, forward button, refresh button, address bar containing "10.32.4.93/app/index.php?pag=sniffer", and a search icon. To the right of the address bar are user-specific icons for "Marcel" and standard window control buttons. The main header features the NIVIS logo and the text "Gen3A Router". On the right side of the header is a "Log out" link. Below the header, a sidebar on the left contains several menu items under three categories: Configuration, Administration, and Session. Under Configuration, the "Network Sniffer" item is highlighted. Under Administration, the "System Upgrade" item is highlighted. Under Session, the "Change Password" and "Log out" items are listed. The main content area has a dark blue header with several icons: Connectivity (a network graph), Whitelist (a grid of squares), Profiles (a database table), Setup ID (a globe with a red X), DTLS List (two stacked boxes with a lock), Cloud Based NOC (a cloud icon), and Network Sniffer (a fish icon). Below this header, the "Network Sniffer" section is titled "Network Sniffer" in green. It contains a single button labeled "Download file". At the bottom of the page, there is a footer with copyright information: "© 2015 Nivis™ | Nivis™ Online" on the left and "v2.4.03 | Running On v2.4.06 VR1100 FAR" on the right.

WARNING The settings will match only the network joined to this Titan. In order to monitor a different network controlled by a different Titan, a new set of settings must be downloaded from the other Titan and loaded into the Network Sniffer

3.9.1.2.9 Upgrading the Edge Router Software

Click on **System Upgrade** in the **Administration** section.



User actions available on this page:

- Upload and activate a Titan or Quark software file.
- Upload a new license file

Browse to the Nivis-provided software archive file, and then click **Start**.

The upgrade process takes several minutes. At the end of the process, the board will restart, rendering the Edge Router and the Edge Router Website unavailable for up to several minutes.

WARNING The Titan and Quark software files are NOT interoperable. Do NOT upload a Titan Software file into a Quark, or a Quark software files into a Titan.

Browse to the Nivis-provided software license file, and then click **Start**.

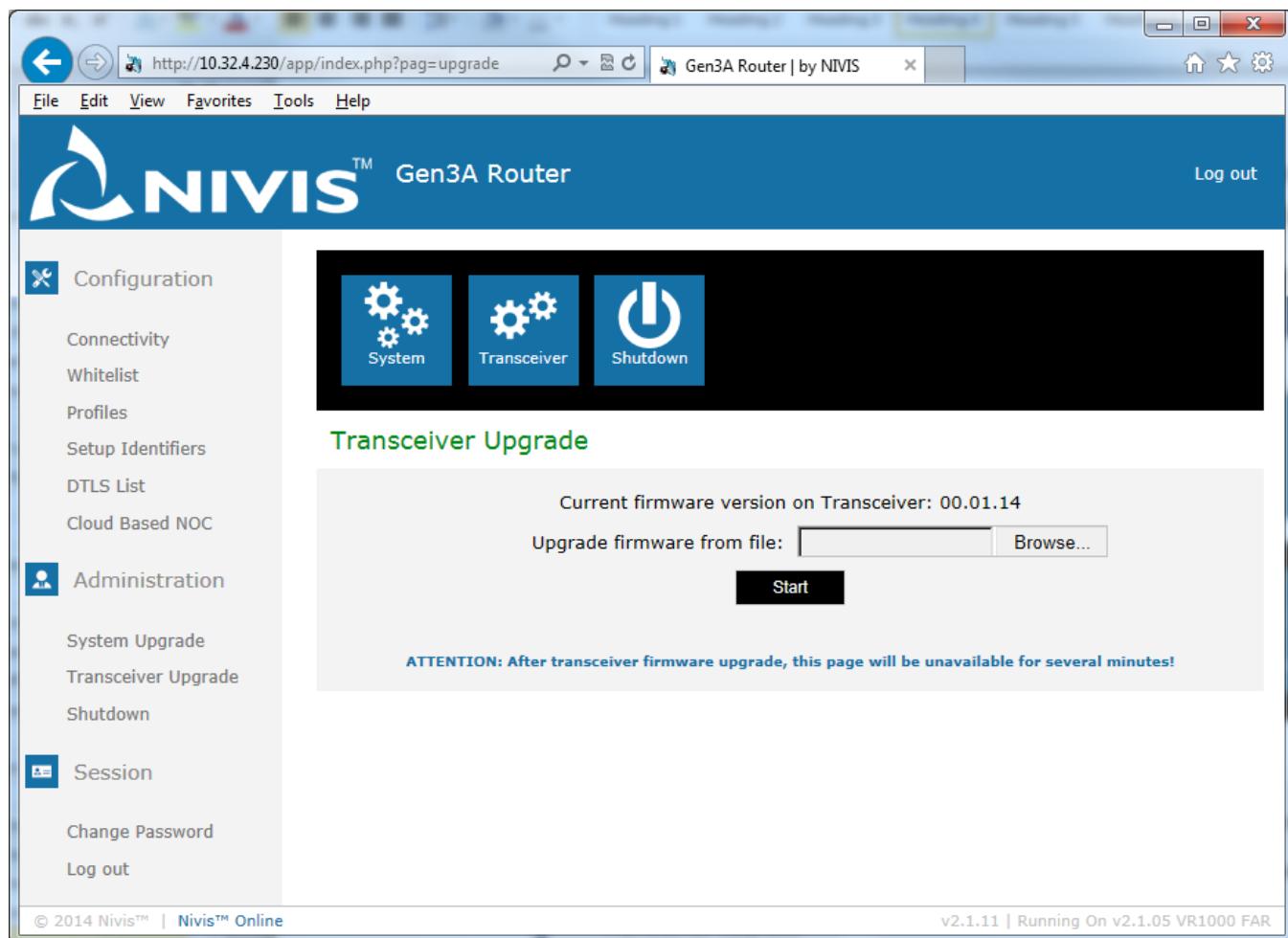
NOTE The Edge Router is delivered pre-loaded with an appropriate license file. No user action is necessary.

This feature is provided for the future, to allow customizing the features/number of nodes, possibly for a different price.

3.9.1.2.10 Upgrading the Edge Router Transceiver

The radio on the Edge Router (the Transceiver) is upgraded separately from the main Edge Router software.

Click on **Transceiver Upgrade** in the **Administration** section.



The screenshot shows the NIVIS Gen3A Router web interface. The left sidebar contains navigation links for Configuration, Administration, and Session. The main content area has a title "Transceiver Upgrade". It displays the current firmware version (00.01.14) and a field to "Upgrade firmware from file:" with a "Browse..." button. A "Start" button is below the file input. A warning message at the bottom states: "ATTENTION: After transceiver firmware upgrade, this page will be unavailable for several minutes!"

User actions available on this page:

- Upload and activate a Titan or Quark Transceiver firmware file.

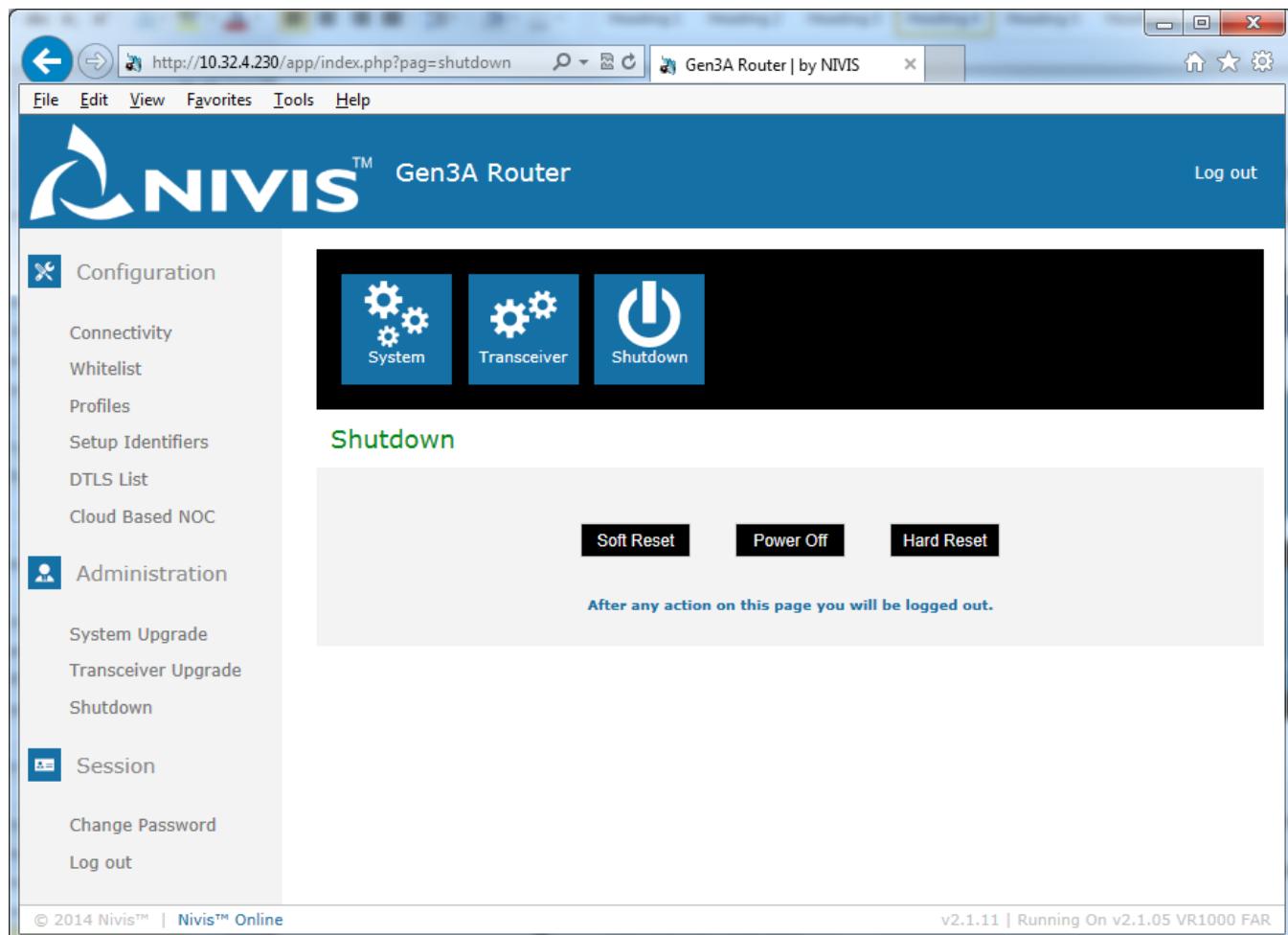
Browse to the Nivis-provided firmware file, and then click **Start**.

The upgrade process takes up to a minute. At the end of the process, the Transceiver will restart, beginning a full rejoin of the network.

3.9.1.2.11 Shutting down the Edge Router

The administration page allows the user to perform a soft reset (restarting the apps), hard reset (rebooting the board), or power off procedure (graceful shutdown).

Click on **Shutdown** in the **Administration** section, and then choose the desired shutdown type.



The screenshot shows the Gen3A Router administration interface. The left sidebar contains navigation links for Configuration, Administration, and Session. Under Administration, the Shutdown link is selected. The main content area has a blue header bar with the NIVIS logo and 'Gen3A Router'. Below this is a large black button labeled 'Shutdown' with three icons: 'System' (two gears), 'Transceiver' (two gears), and 'Shutdown' (a power button). The word 'Shutdown' is written in green below the button. At the bottom of the content area, there are three buttons: 'Soft Reset', 'Power Off', and 'Hard Reset'. A note at the bottom states: 'After any action on this page you will be logged out.'

User actions available on this page:

- Soft Reset – restart the Titan applications – without rebooting the board
- Power Off – shut down Titan – graceful shutdown, must be performed before powering off Titan (power source disconnect)
- Hard Reset – reboot HW the Titan board.

WARNING Before removing the Edge Router power, you **MUST** perform a graceful shutdown (click on **Power Off**). Failure to do so may render the Edge Router non-functional.

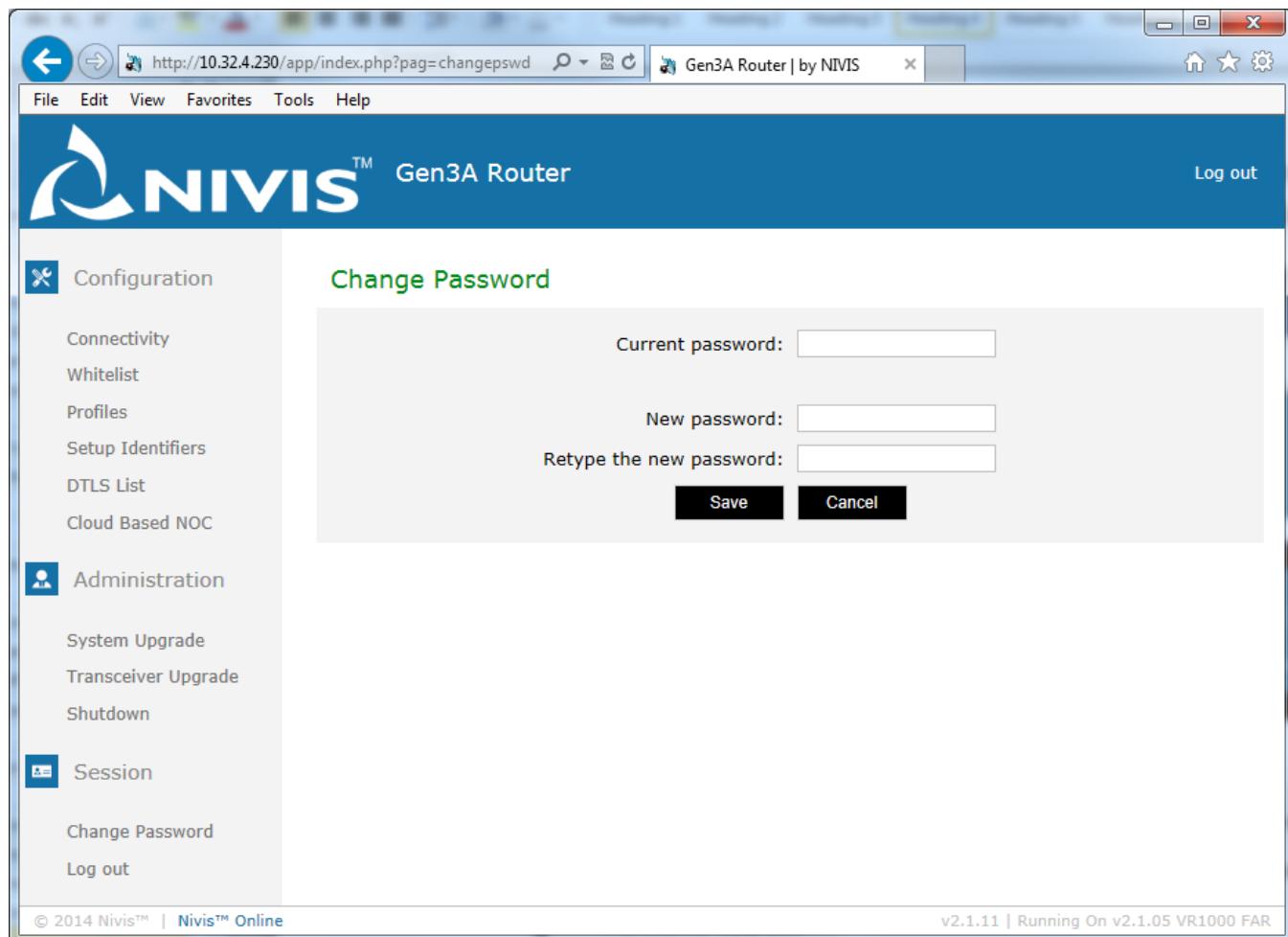
3.9.1.2.12 Changing the Edge Router Website password

The administration page allows users to change the Edge Router Website password.

User actions available on this page:

- Change the Website user password

Click on **Change Password** in the **Session** section. Type the old password and new password, re-type the new password, and click **Save**.



The screenshot shows a web browser window for the 'Gen3A Router | by NIVIS' at the URL <http://10.32.4.230/app/index.php?pag=changepwd>. The left sidebar has sections for Configuration (Connectivity, Whitelist, Profiles, Setup Identifiers, DTLS List, Cloud Based NOC), Administration (System Upgrade, Transceiver Upgrade, Shutdown), and Session (Change Password, Log out). The main content area is titled 'Change Password' and contains fields for 'Current password', 'New password', and 'Retype the new password', with 'Save' and 'Cancel' buttons. The top right of the page shows 'Log out'.

3.9.1.2.13 Logging out

User actions available on this page:

- Log out from the Website

Click on **Log Out** in the **Session** section to log out of the website.

3.9.1.3 Web-based Administration /admin/

The web-based administration /admin/ interface is the secondary method that can be used to administer/configure the Edge Router. It requires a web browser and the IP of the Edge Router.

The Versa Router™ 1000 **Quark** must be connected to the local LAN and then powered on.

The Versa Router™ 1100 **Titan** must be powered on and connected to the local LAN or to 3G cellular network.

The IPv4 of the Edge Router must be accessible from the PC where the browser is running.

The administration website for the Edge Router can be accessed by pointing a web browser to the Edge Router IP.

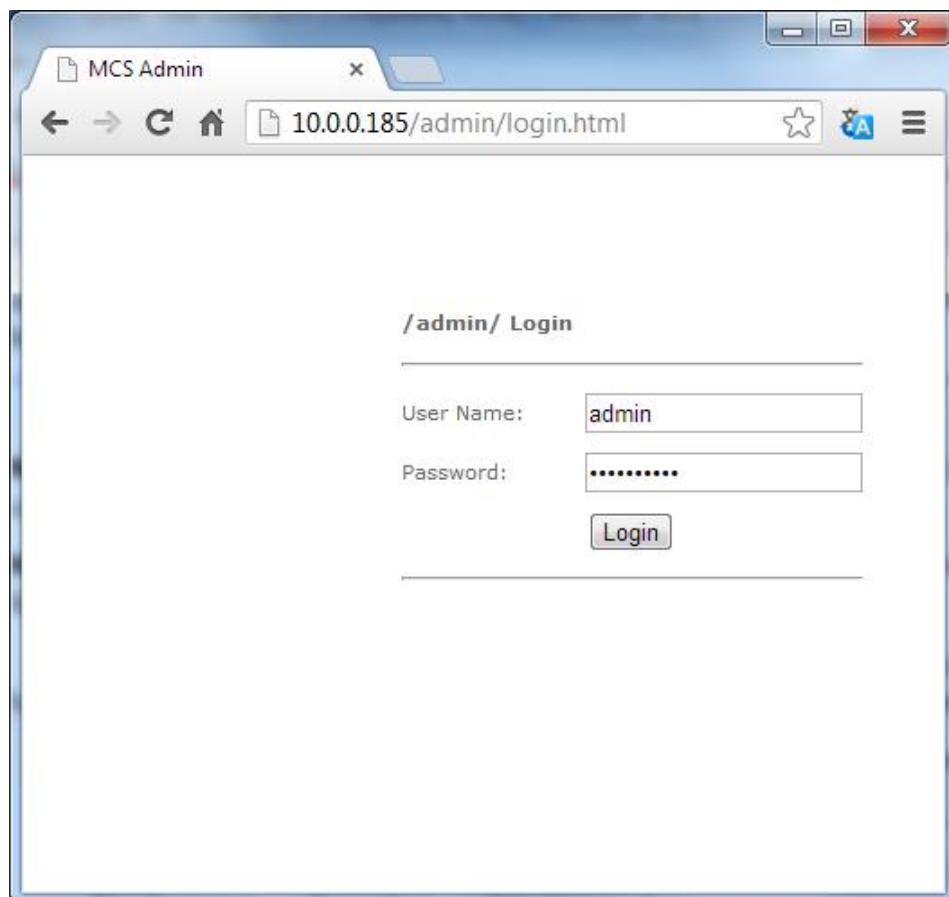
NOTES

The /admin/ interface is for advanced users only. Do not use this method unless instructed by a Nivis representative.

Depending on the firmware running on the Edge Router, more or fewer features may be available than described herein.

All web administration tasks require login. The login step is presented here only once. All of the following /admin/ related sections will require it.

1. Navigate to the following URL: http://<ER_IP>/admin where<ER_IP> is replaced by the Edge Router IP.

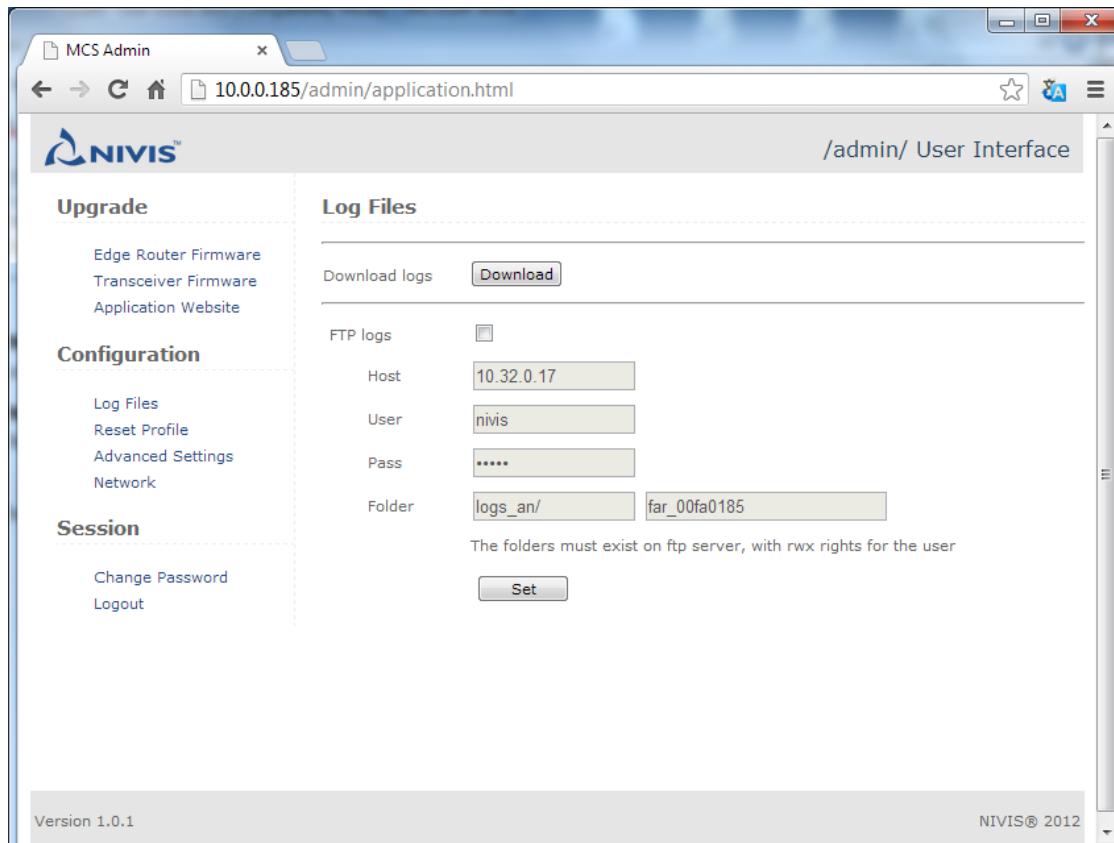


2. Type the following credentials in the input fields

- User: **admin**
- Password: **adminadmin**

3. Click **Login**.

The following page appears, allowing access to various tasks. By default, the **Log Files** link is selected.



NOTE

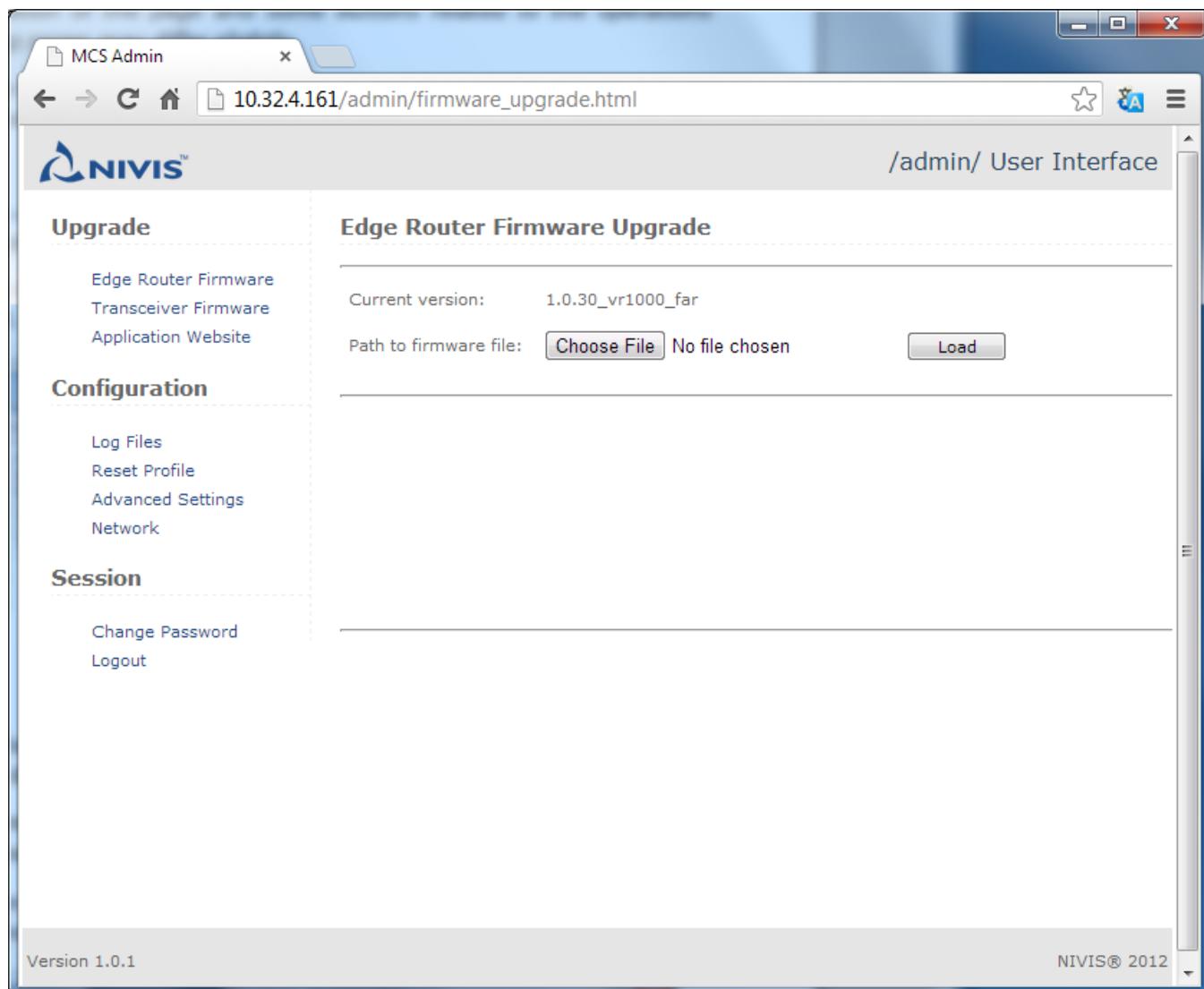
Depending on the web browser you are using to log into the Edge Router Administration, the graphical representation of the page and some buttons related to the operations described in the following pages may differ slightly.

For instance, the button **Choose File** in Google Chrome and Apple Safari is the same as the button **Browse** in Mozilla Firefox and Internet Explorer.

3.9.1.3.1 Upgrade Edge Router Software

This function is used to upgrade the Edge Router SW when an update is provided by Nivis.

1. Click **Edge Router Firmware**. The following screen shows the version currently installed.



The screenshot shows the 'Edge Router Firmware Upgrade' page within the NIVIS MCS Admin interface. The left sidebar contains links for 'Upgrade' (Edge Router Firmware, Transceiver Firmware, Application Website) and 'Configuration' (Log Files, Reset Profile, Advanced Settings, Network). The main panel displays the current version as '1.0.30_vr1000_far'. It includes a file input field 'Path to firmware file:' with a 'Choose File' button, a status message 'No file chosen', and a 'Load' button. At the bottom of the page, there are links for 'Change Password' and 'Logout'. The footer indicates 'Version 1.0.1' and 'NIVIS® 2012'.

2. Click **Browse** to locate and select new firmware file, then click **Load** (the version must be different from the previous one).
3. Wait until the firmware is activated. This process will take few minutes. Do not power-cycle the board or interrupt the upgrade processing any other way.

During the upgrade, the process log is displayed. When the operation is complete, the screen should look similar to the screen capture below.

Operation complete.

Log results:

```
+ ./web_upgrade.sh
Stopping modules
Announce to stop modules: watchdog.sh
killall watchdog.sh
Module watchdog.sh ended OK
All modules ended OK
Announce to stop modules: RplBridge RplRoot RemoteAccess SNMP_Agent DNS_Server NMS_EntryPoint HttpCoapPr
killall RplBridge RplRoot RemoteAccess SNMP_Agent DNS_Server NMS_EntryPoint HttpCoapProxy sys_monitor.sh
Module RplBridge ended OK
Module RplRoot ended OK
Module RemoteAccess ended OK
 625 ?      S1    7:06 ./SNMP_Agent
29997 ?     S     0:00 ./SNMP_Agent
Module DNS_Server ended OK
17644 ?      S1    0:51 ./NMS_EntryPoint
29999 ?     S     0:00 ./NMS_EntryPoint
Module HttpCoapProxy ended OK
Module sys_monitor.sh ended OK
Module log_watcher.sh ended OK
Module SNMP_Agent ended OK
17644 ?      S     0:51 ./NMS_EntryPoint
29999 ?     S     0:00 ./NMS_EntryPoint
17644 ?      S     0:51 ./NMS_EntryPoint
29999 ?     S     0:00 ./NMS_EntryPoint
Module NMS_EntryPoint ended OK
All modules ended OK
Validate DB '/jffs/nivis/far/tmp/EntryPoint.db3' against '/jffs/nivis/far/activity_files/EntryPoint_Fixt
Move DB to BackupDB /jffs/nivis/far/tmp/EntryPoint.db3 -> /jffs/nivis/far/activity_files/EntryPoint.db3
== STARTING ACT_OUT ===
activate.sh --fw_file /jffs/nivis/far/tmp/upgrade_web/an_bin_1.0.11_b1_p1025twr_far_lg.tgz
SetActive firmware: fw_file=/jffs/nivis/far/tmp/upgrade_web/an_bin_1.0.11_b1_p1025twr_far_lg.tgz fw_ver=
SetActive [an_bin_1.0.11_b1_p1025twr_far_lg]
SetActive firmware [an_bin_1.0.11_b1_p1025twr_far_lg] done. Restart in 30sec.
ER_RESULT=SUCCESS
```

NOTES

Contact Nivis support if the upgrade operation does not succeed.

For faster rejoin: power-cycle all Smart Object devices after performing an Edge Router firmware upgrade

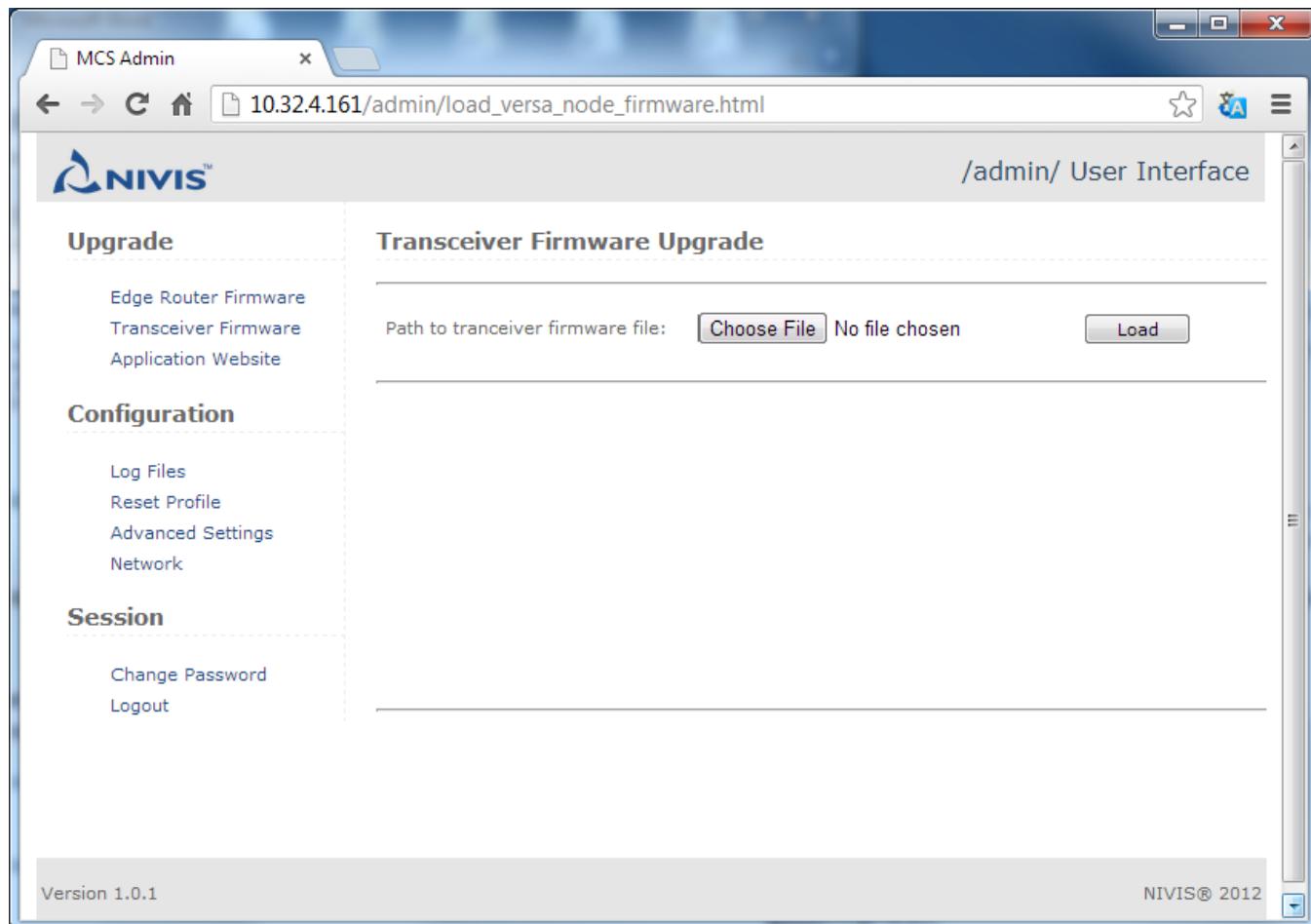
Wait about 5 minutes before attempting to connect the NAMT to the Edge Router.

WARNING The Titan and Quark software files are NOT interoperable. Do NOT upload a Titan Software file into a Quark, or a Quark software files into a Titan.

3.9.1.3.2 Upgrade Edge Router Transceiver firmware

This function is used to upgrade the Edge Router transceiver firmware when an update is provided by Nivis.

1. Click **Transceiver Firmware**. The following screen appears.



2. Click **Browse** to locate and select a new firmware file then click **Load** (the version must be different from the previous one).
3. Wait until the firmware is activated. This process will take few minutes. Do not power-cycle the board or interrupt the upgrade processing any other way.

After the upgrade, the process log is displayed.

NOTES

Contact Nivis support if the operation does not succeed.

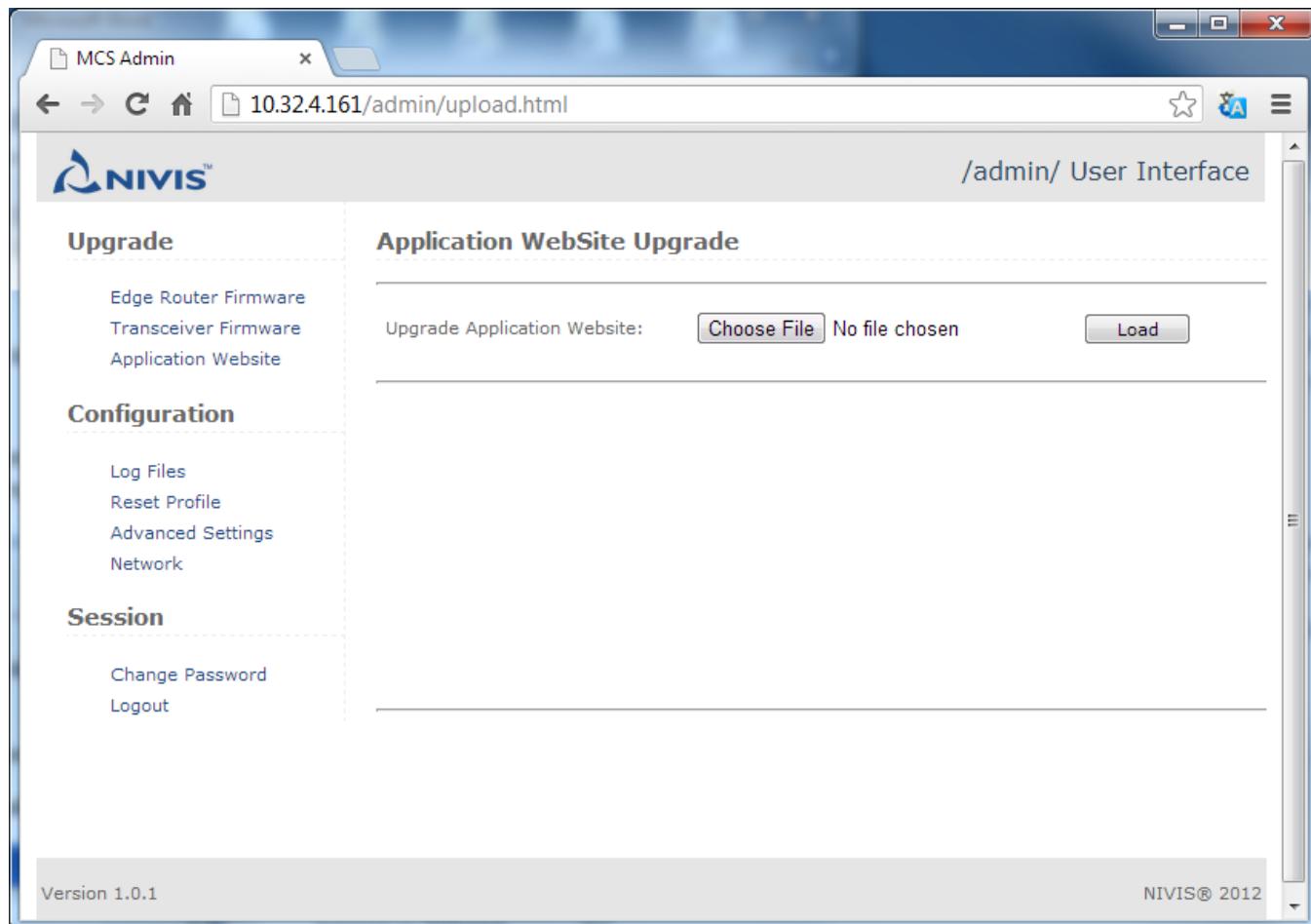
For faster rejoin: power-cycle all Smart Object devices after performing an Edge Router firmware upgrade

Wait about 5 minutes before attempting to connect the NAMT to the Edge Router.

3.9.1.3.3 Upgrade the Edge Router Website

This function is used to upgrade the Edge Router website when an update is provided by Nivis.

1. Click **Application Website**. The following screen appears.



2. Click **Browse** to locate and select new firmware file, then click **Load** (the version must be different from the previous one).
3. Wait until the website is activated. This process will take few minutes. Do not power-cycle the board or interrupt the upgrade processing any other way.

After the upgrade, the process log is displayed.

NOTES

Contact Nivis support if the operation does not succeed.

For faster rejoin: power-cycle all Smart Object devices after performing an Edge Router firmware upgrade

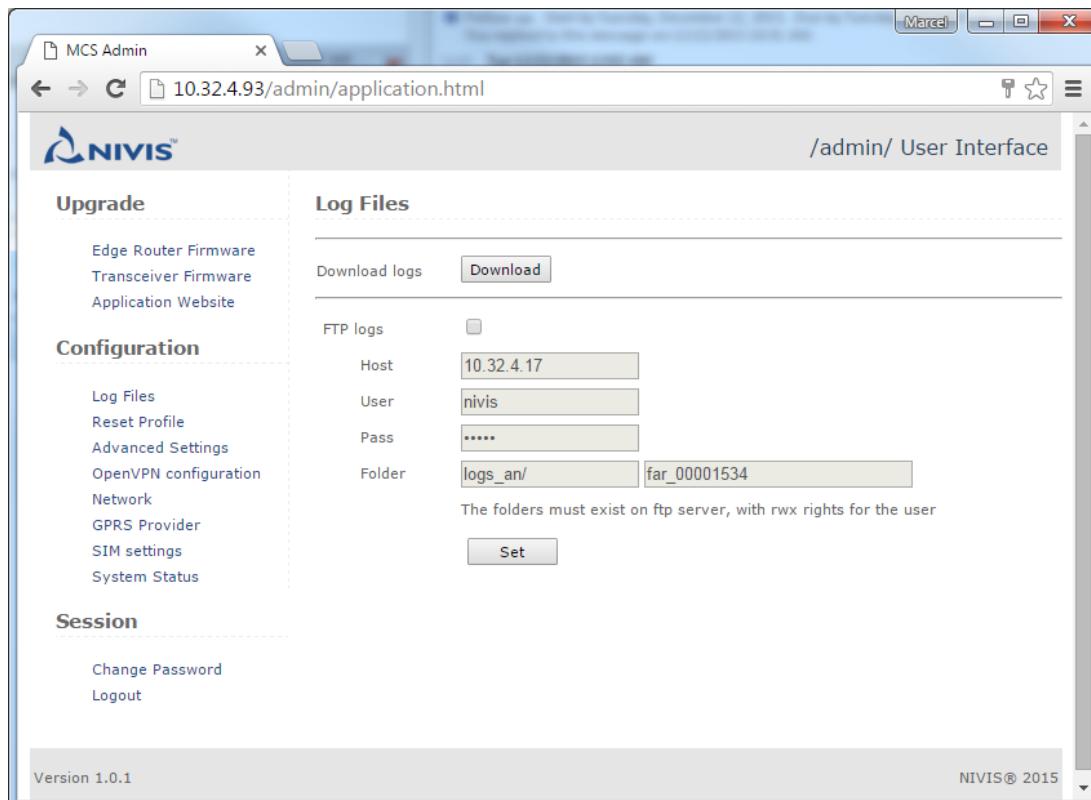
Wait about 5 minutes before attempting to connect the NAMT to the Edge Router.

3.9.1.3.4 Download Edge Router Logs or set-up Edge Router for FTP Logs Upload

User actions available on this page:

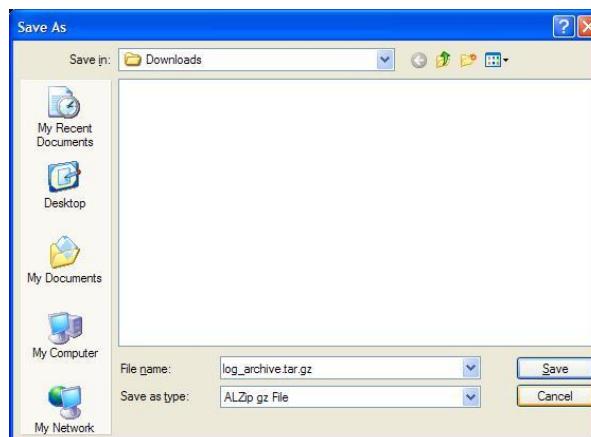
- Download the Edge Router **logs snapshot** when requested for troubleshooting purposes.
- Set-up Edge Router FTP logs upload

1. Log-in into /admin/ website, or click on **Log Files** if already logged in.



2. Click **Download Logs**. A window opens prompting you to open or save the archive.

3. Click **Save**. The **Save As** dialog will open.



4. In this dialog, choose the location for the archive and click **Save**.

This page allows also configuring the Edge Router to upload the logs to a FTP server when long-term logs are needed and the log snapshot does not provide enough information.

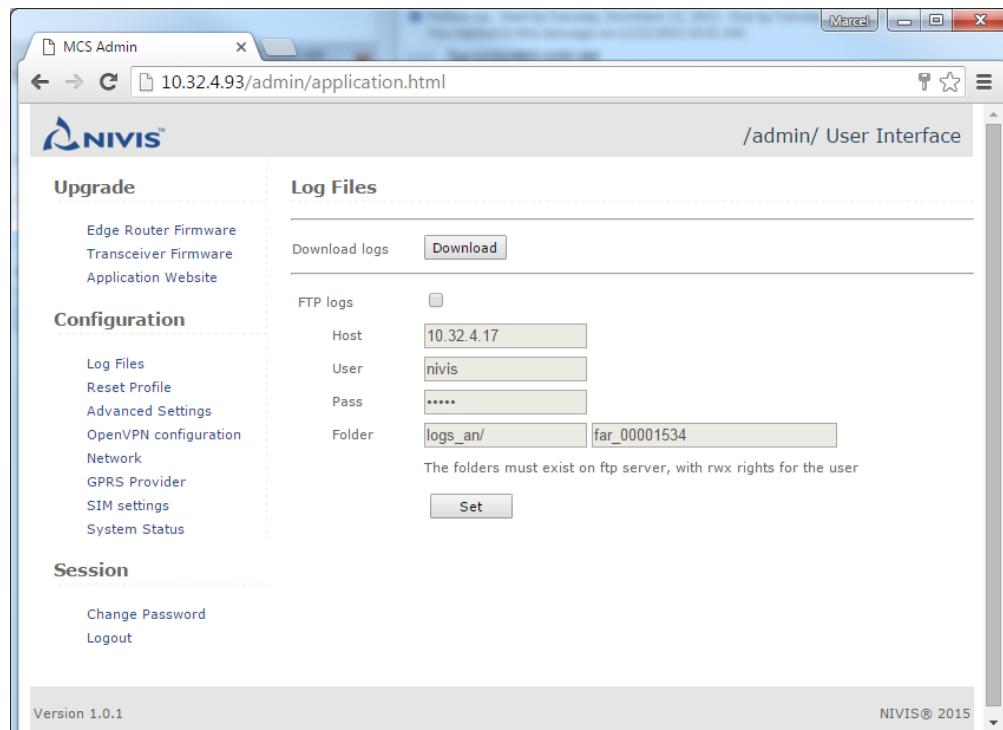
WARNING: This functionality is for advanced users only – do not use unless you have been instructed by a Nivis representative.

Because of space restrictions, the logs on the Edge Router are frequently removed. In order to retain logs over a longer period of time, a FTP server can be used. The Edge Router must be configured to move the logs onto the FTP server instead of removing them.

The external FTP server must meet the following conditions:

1. Be in the same network with the Edge Router. It **must be available in the network all the time**; otherwise, the Edge Router may not function correctly.
2. Be UNIX-compatible.
3. Have a username and password created. Anonymous users should **not** be used.

NOTE Please be aware that the most recent logs will still be on the Edge Router (available through log snapshot: **Download Logs** button) and not on the FTP server.



To configure the Edge Router to upload the logs to a FTP server, on the Application Configuration screen:

1. Select the **FTP logs** checkbox.
2. In the **Host** field, enter a valid FTP server IP address.
3. In the **User** and **Pass** input fields; enter a valid username and password for the FTP server. Do not use anonymous users.
4. Select the folder on the FTP server in which the logs are to be saved.
5. Click **Set**.

3.9.1.3.5 Reset profile

WARNING The **Reset Profile** section is for troubleshooting purposes only. **Do not use** unless instructed specifically by a Nivis representative.

3.9.1.3.6 Edit Edge Router General Configuration

This page allows you to view/set less common configuration variables.

WARNING This page is for advanced users only – do not use unless you have been instructed specifically by a Nivis representative on what values to change. Incorrect values may render the router non-functional or may cause difficult-to-trace malfunctions.

1. Click on **Advanced Settings**. The following form will open to the right of the operation list:

Edit configuration

Sections/variables	
Variable type	<input checked="" type="radio"/> Standard <input type="radio"/> Custom
Section	EntryPoint
Variable	LOG_LEVEL
Value	DEBUG
<input type="button" value="Set"/> <input type="button" value="Cancel"/>	

2. In the form, select a **Section** in the drop-down list. The **Variable** list will change accordingly.
3. Select a **Variable** in the drop-down list.
4. Set /edit the **Value** field, then click **Set**.

WARNING Do not change [GLOBAL].AN_ID under any circumstance.

To add a new variable, select **Custom** under **Variable type**. The **Section/Variable** items will be empty.

Sections/variables	
Variable type	<input type="radio"/> Standard <input checked="" type="radio"/> Custom
Section	
Variable	
Value	
<input type="button" value="Set"/> <input type="button" value="Cancel"/>	

Type the desired information in the **Section**, **Variable**, and **Value** fields and click **Set**.

3.9.1.3.7 Edit Edge Router openvpn configuration

WARNING The **Edit openvpn configuration** section is for troubleshooting purposes only. **Do not use** unless instructed specifically by a Nivis representative.

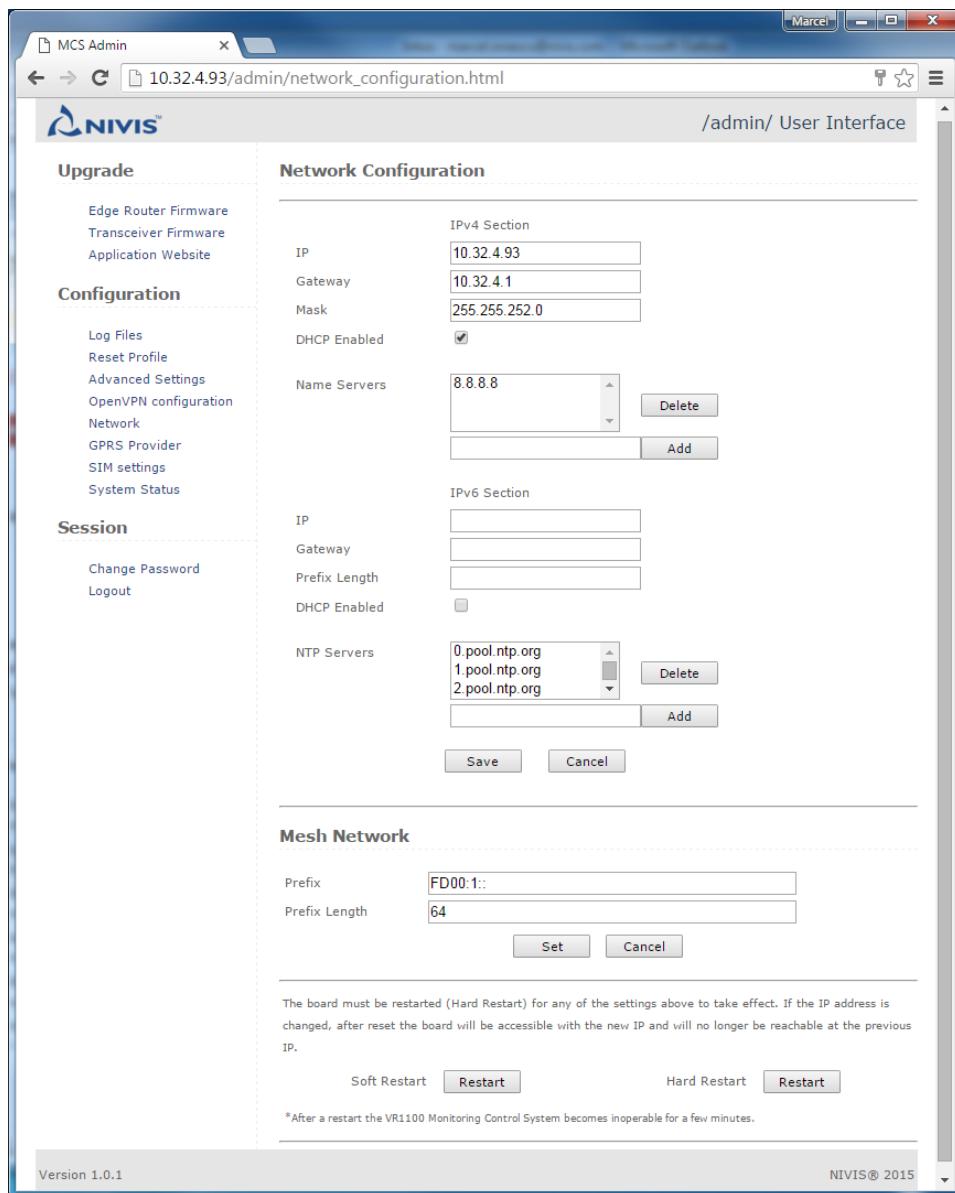
3.9.1.3.8 Edit Edge Router IP and other Network Settings

User actions available on this page:

- View/set network-related settings: IPv4/IPv6 address/mask/gateway, name servers used, time servers used
- View/set mesh network Prefix
- Restart the Router to activate the changes

WARNING This page is for advanced users only – do not use it unless you know precisely how to configure the network. Any invalid values may render the router dysfunctional, or may cause difficult to trace malfunctions.

1. Click on **Network**. The following form will open to the right of the operation list.



The screenshot shows the 'Network Configuration' section of the NIVIS MCS Admin interface. On the left, there's a sidebar with 'Upgrade' (Edge Router Firmware, Transceiver Firmware, Application Website), 'Configuration' (Log Files, Reset Profile, Advanced Settings, OpenVPN configuration, Network, GPRS Provider, SIM settings, System Status), and 'Session' (Change Password, Logout). The main area has two sections: 'IPv4 Section' with fields for IP (10.32.4.93), Gateway (10.32.4.1), Mask (255.255.252.0), and DHCP Enabled (checked); and 'Name Servers' (a list containing 8.8.8.8 with 'Delete' and 'Add' buttons). Below that is the 'IPv6 Section' with empty fields for IP, Gateway, Prefix Length, and DHCP Enabled. The 'NTP Servers' section lists 0.pool.ntp.org, 1.pool.ntp.org, and 2.pool.ntp.org with 'Delete' and 'Add' buttons. At the bottom are 'Save' and 'Cancel' buttons. The 'Mesh Network' section contains a 'Prefix' field (FD00:1::) and a 'Prefix Length' field (64) with 'Set' and 'Cancel' buttons. A note at the bottom states: 'The board must be restarted (Hard Restart) for any of the settings above to take effect. If the IP address is changed, after reset the board will be accessible with the new IP and will no longer be reachable at the previous IP.' Buttons for 'Soft Restart' and 'Hard Restart' are shown, along with a note: '*After a restart the VR1100 Monitoring Control System becomes inoperable for a few minutes.' The footer shows 'Version 1.0.1' and 'NIVIS® 2015'.

2. In the form, you can edit the input fields for IP, Gateway, and Mask, for IPv4 and/or IPv6

3. To add a name server or an NTP server, provide the correct value in the **Add** input field and click **Add**.
4. To delete a name server or an NTP server, select it in the list of existing items and click **Delete**.
5. When you are done, click **Save** to save the settings.
6. In the form, you can edit the input fields for Mesh network Prefix or Prefix Length
7. When you are done, click **Set** to save the settings.
8. Preform a **Hard Restart** too activate the settings modified above

Clicking the **Soft Restart** button will restart all the application on the Edge Router.

Clicking the **Hard Restart** button will reboot the Edge Router and activate the settings.

NOTES

Make sure you are not causing IP conflicts when you make changes.

Make sure the name servers used are functional and accessible from the Edge Router.

Make sure the NTP servers are functional and accessible from the Edge Router.

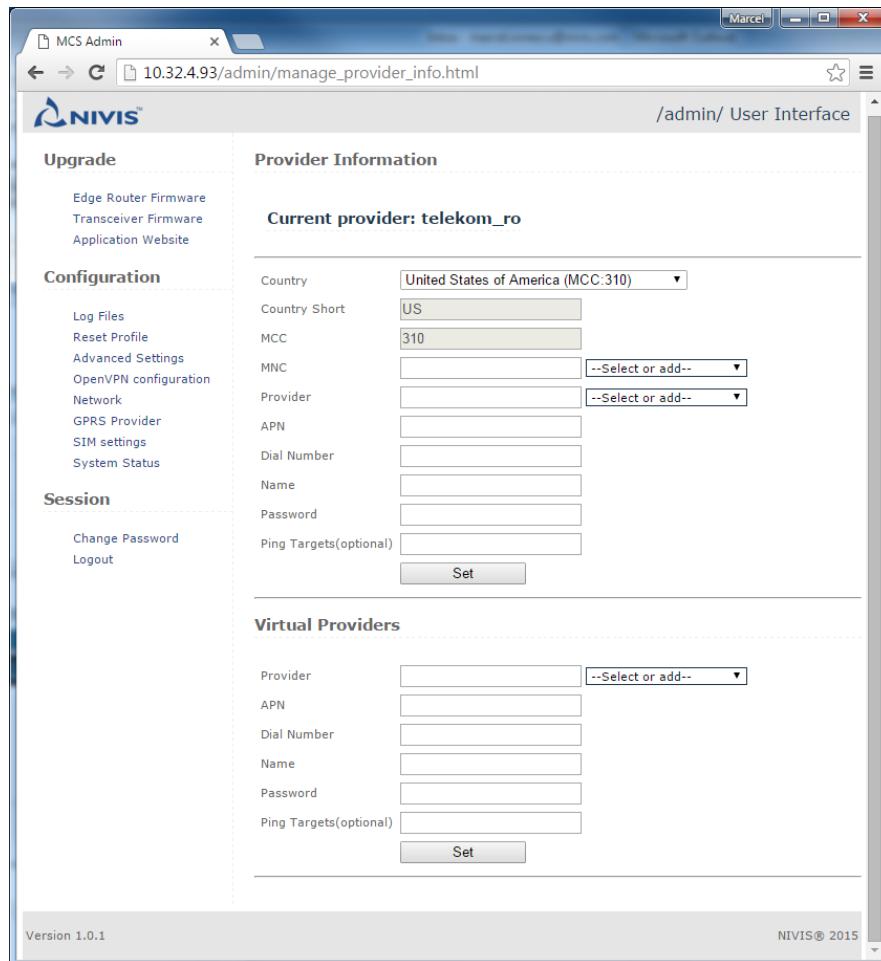
3.9.1.3.9 Edit Versa Router™ 1100 Titan GPRS provider [Titan ONLY]

To use a cellular data connection, the cellular modem must be configured properly for access to the cellular network. The network operator provides the settings specific for it and for the data plan associated with the SIM card (APN, user, password, etc. for carrier-specific MCC/MNC).

User actions available on this page:

- View/set cellular-provider-related settings: APN, Dial number, username, password for a cell provider identified by pair MCC/MNC
 - Separate page sections are provided for regular cell providers and virtual providers (MVNO)
 - Assign a symbolic name to the set of configuration (recommended using the same name as provider name)
 - Optionally assign an IP visible from within the provider network associated with the specific APN
-
1. Have the settings mentioned above readily available.
 2. Have the SIM card inserted in Titan SIM slot. The SIM card must be active, with PIN disabled, associated with an active data plan; see details at section [Configure the SIM card](#) above
 3. Have the Ethernet connected and the PC properly configured to be able to access Titan web interface. See section [Configure the PC static IP address to access the Edge Router](#) above
 4. Power on Titan
 5. Log in into /admin/ website

6. Click on **GPRS Provider**. The following screen appears:



7. If using a regular (i.e. not virtual) cellular operator, use the section at the top of the page
8. Choose the country from the Country drop-down; the MCC will populate automatically
9. Ensure that both MNC and Provider drop-downs are in position “Select or Add”
10. Enter the MNC and the provider name
11. Enter the rest of the settings: APN, Dial number, username, password (settings must be obtained from the cell provider)
12. Optionally, enter a ping target which is accessible via ping from within the cellular data network. Titan will verify the cell connection health by periodically sending pings to the ping target. This is only necessary for private networks with no Internet access. If data plan ensures full unrestricted Internet access, Titan has built-in means to monitor cell connection health.
13. If using a Virtual Provider (MVNO), use the respective section at the bottom of the page

NOTE This section is specific to Titan only. Quarks do not have cell connectivity.

It is **strongly** recommended to use a data plan with **full unrestricted internet access** (all ports including ports below 1024, TCP/UDP/ICMP)

3.9.1.3.10 Edit Versa Router™ 1100 Titan SIM Settings [Titan ONLY]

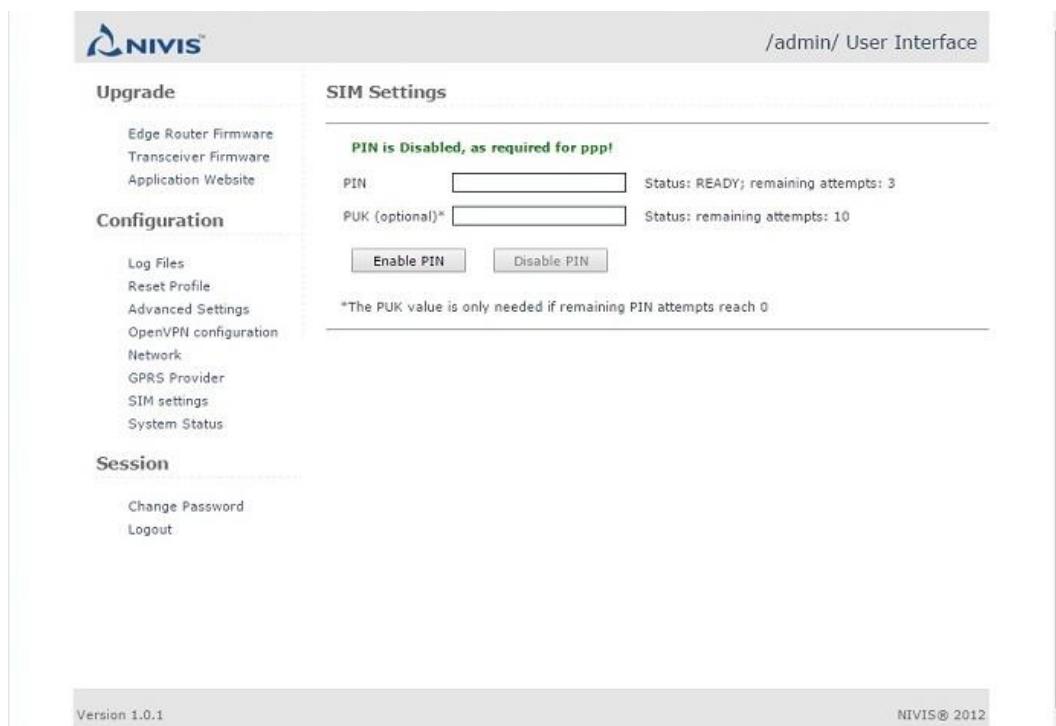
The Titan cell backhaul operation requires a SIM card with the PIN disabled.

If the PIN is enabled on the SIM card, you must disable it either by using a phone, or by using this section of Titan /admin/ website UI.

User actions available on this page:

- Disable the SIM PIN
- Enable the SIM PIN – this action is not necessary for Titan functionality. It may be used to restore the settings on a SIM card.

1. Have the SIM card inserted in Titan SIM slot. The SIM card must be active, with PIN disabled, associated with an active data plan; see details at section [Configure the SIM card](#) above
2. Have the Ethernet connected and the PC properly configured to be able to access Titan web interface. See section [Configure the PC static IP address to access the Edge Router](#) above
3. Power on Titan
4. Log in into /admin/ website
5. Click on **SIM settings**. The following screen appears (message on top of page might be different):



5. If the page shows “PIN is disabled”, there is nothing to do, the PIN is disabled already
6. If the page shows “PIN is enabled”: Enter current PIN and click “Disable”
7. If the “Remaining attempts” shows 0 (PIN was entered incorrectly for too many times), enter the PUK code and the *correct* PIN code in order to disable PIN

8. If the page show an error message
 - a. Check the SIM is properly inserted, make sure the board was rebooted after the SIM was inserted
 - b. A data connection may be in progress, if Titan was not restarted after inserting the ETH. Make sure to reboot the board after inserting the ETH.

NOTES This section is specific to Titans only. Quarks do not have SIM cards.

It is **mandatory** to perform SIM card insert/remove operations ETH connect/disconnect while Titan is powered off (disconnected from both mains and battery)

Use this section only if the SIM card has PIN enabled

Entering an incorrect PIN too many times may lead to an unusable SIM

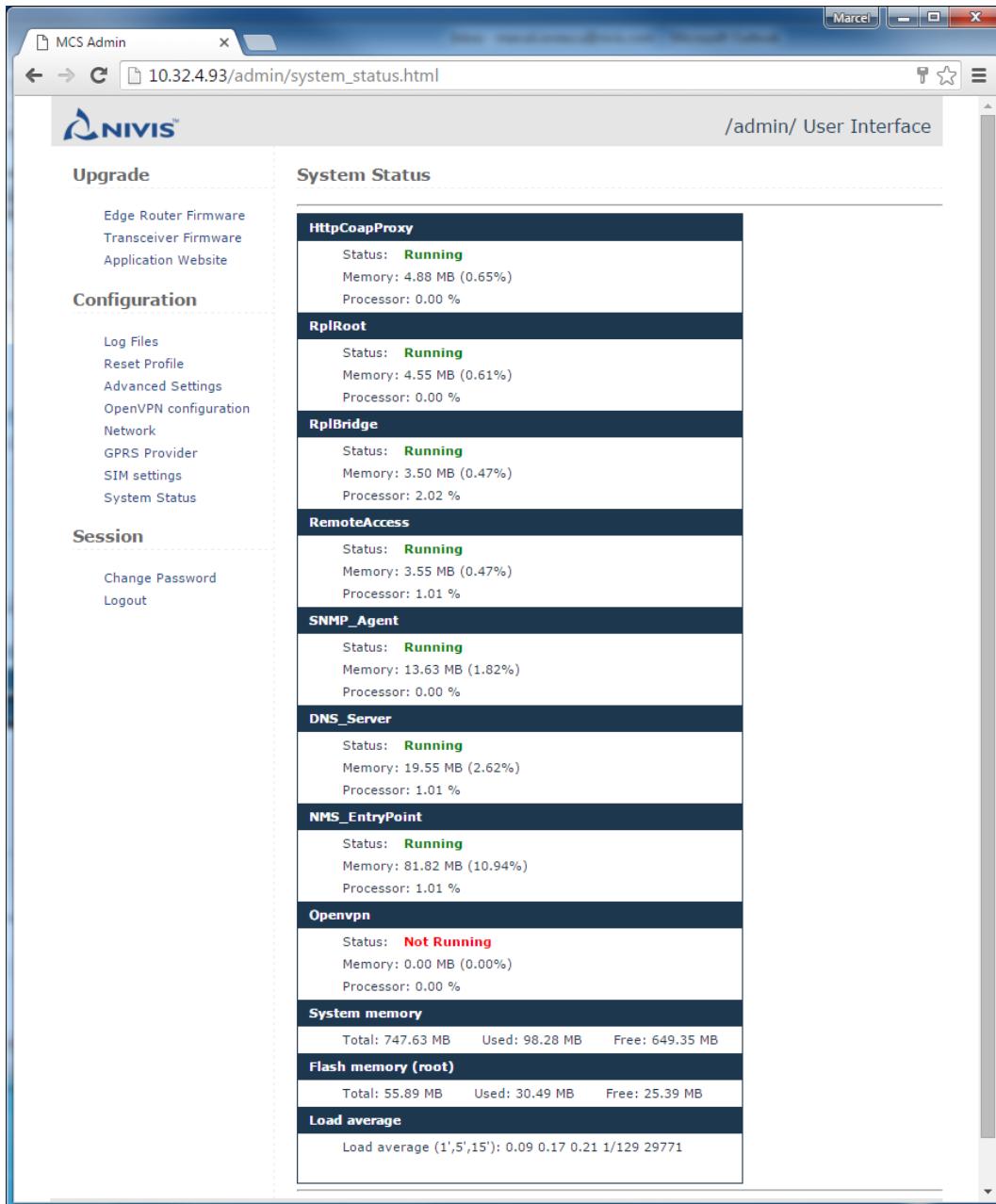
3.9.1.3.11 Checking the Edge Router System status

WARNING This page is for advanced users only – do not use it unless instructed by a Nivis representative.

User actions available on this page:

- View system status

1. Click on System Status



The screenshot shows a Microsoft Internet Explorer browser window titled 'MCS Admin' with the URL '10.32.4.93/admin/system_status.html'. The page displays the 'System Status' section of the NIVIS User Interface. On the left, there is a navigation menu with sections for Upgrade, Configuration, and Session, along with links for Log Files, Reset Profile, Advanced Settings, OpenVPN configuration, Network, GPRS Provider, SIM settings, and System Status. The main content area is titled 'System Status' and contains a table of system components and their status. The table includes the following rows:

Component	Status	Memory	Processor
HttpCoapProxy	Running	4.88 MB (0.65%)	0.00 %
RplRoot	Running	4.55 MB (0.61%)	0.00 %
RplBridge	Running	3.50 MB (0.47%)	2.02 %
RemoteAccess	Running	3.55 MB (0.47%)	1.01 %
SNMP_Agent	Running	13.63 MB (1.82%)	0.00 %
DNS_Server	Running	19.55 MB (2.62%)	1.01 %
NMS_EntryPoint	Running	81.82 MB (10.94%)	1.01 %
Openvpn	Not Running	0.00 MB (0.00%)	0.00 %
System memory	Total: 747.63 MB Used: 98.28 MB Free: 649.35 MB		
Flash memory (root)	Total: 55.89 MB Used: 30.49 MB Free: 25.39 MB		
Load average	Load average (1',5',15'): 0.09 0.17 0.21 1/129 29771		

3.9.1.4 Ports & interfaces

The following interfaces are usable on the Edge Router:

- The **serial port** is used as a kernel console and emergency backup.
- The Edge Router accepts **ssh 22/TCP** connections.
- The Edge Router has an **http** server listening on port **80/TCP** for a Nivis-specific user Interface.
- The Edge Router has an SNMP Agent listening on port **161/UDP**.
- The HTTP – COAP proxy listens on port **9999/TCP** for HTTP queries.
- The Edge Router utilizes the NTP protocol on port **123/UDP** to synchronize time with Internet time servers. In order to synchronize the time with Internet time servers, port **123/UDP** must be open in both directions to allow time synchronization.
- **In case of Versa Router™ 1100 Titan, the cellular data plan MUST allow access to the internet through port 123 UDP, IN/OUT.**

Not all interfaces are guaranteed to be enabled in all cases. Some may be disabled for specific applications.

4 Upgrading the Edge Router (Versa Router™ 1000 Quark and Versa Router™ 1100 Titan) components

4.1 Overview

The **Edge Router software** can be upgraded by using the Edge Router website, the Edge Router /admin/ interface, and using the Cloud-based NOC website.

The firmware running on the Edge Router **Transceiver** can be upgraded by using the Edge Router website, the Edge Router /admin/ interface, and using the Cloud-based NOC website.

The upgrade via Cloud-based NOC website can only be performed if the Edge Router is running on transparent mode, connected to the Cloud-based NOC.

4.2 Upgrading the Edge Router Transceiver firmware using Edge Router web interface

Follow the steps in section “[Upgrading the Edge Router Transceiver](#)”.

4.3 Upgrading the Edge Router Transceiver firmware using Edge Router /admin/ interface

Follow the steps in section “[Upgrade Edge Router Transceiver firmware](#)”.

4.4 Upgrading the Edge Router software using Edge Router web interface

Follow the steps in section “[Upgrading the Edge Router Software](#)”.

4.5 Upgrading the Edge Router using Edge Router /admin/ interface

Follow the steps in section “[Upgrade Edge Router Software](#)”.

4.6 Upgrading the Edge Router software using Cloud-based NOC website

See the Cloud-based NOC User Manual for upgrading the Edge Router software from Cloud-based NOC website.

4.7 Upgrading the Edge Router website using Edge Router /admin/ interface

Follow the steps in section “[Upgrade the Edge Router Website](#)”.

5 Configuring the Edge Router (Versa Router™ 1000 Quark and Versa Router™ 1100 Titan)

5.1 Overview

This section describes the steps necessary for configuring or re-configuring the Edge Router. It provides a set of default configuration parameters and details the steps that need to be followed in order to configure the Titan parameters such as the **Network ID**, Smart Objects **Join Key**, enable/disable **PANA/DTLS**, and other parameters. The section also describes the steps to be taken to connect to the Cloud-Based NOC/NMS.

NOTES

The end user is NOT allowed to convert system configured for US to a system configured for JP or EU or the other way around.

The end user is NOT allowed to modify the channels bitmap (the list of channels to use for frequency hopping).

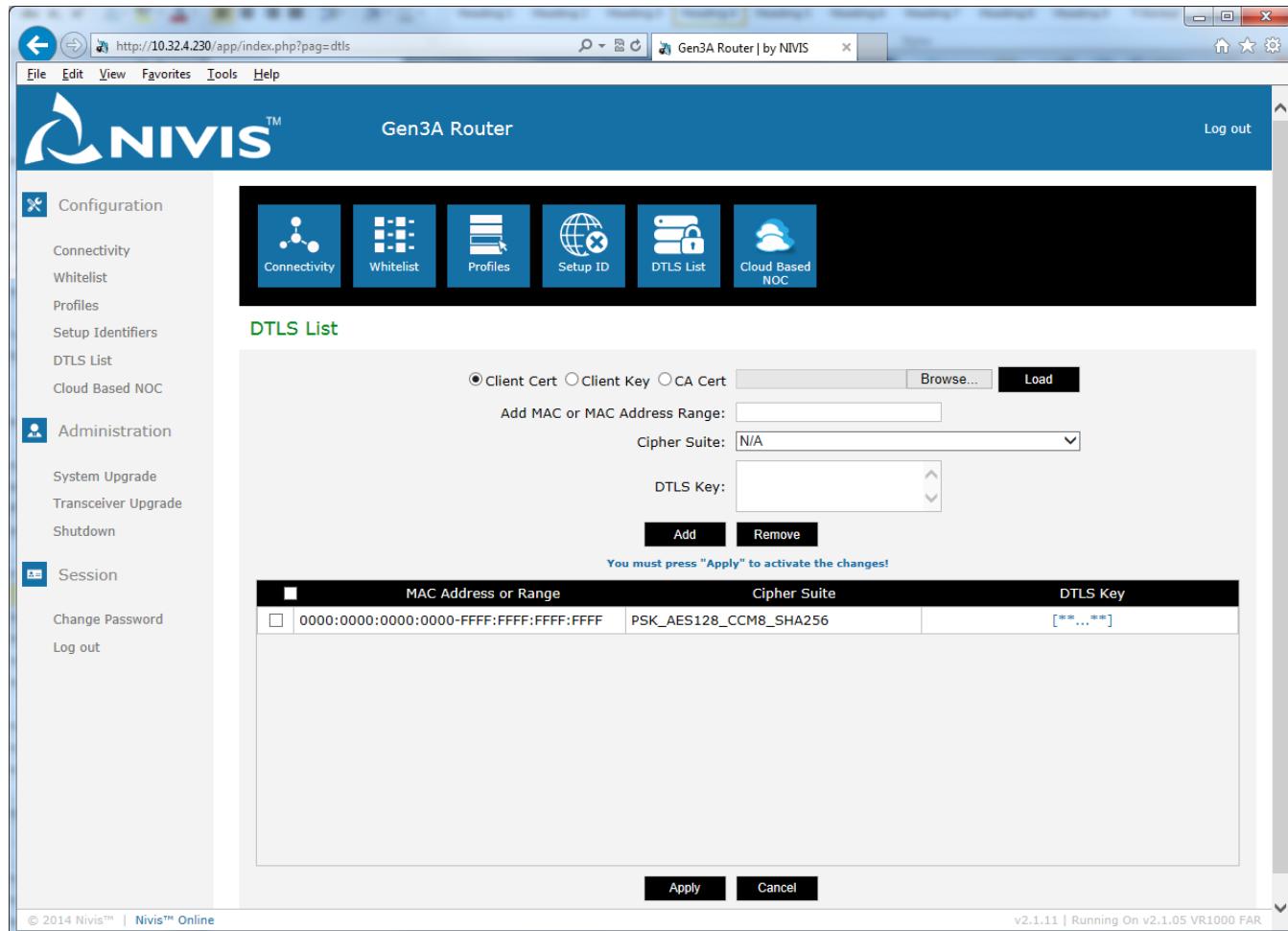
5.2 Accessing the configuration interface on Edge Router

The Edge Router website on the Edge Router can be accessed by pointing a web browser to the Edge Router IP.

See [Configuration and administration of the Edge Router](#) for details on how to operate the Edge Router configuration interface.

5.3 Enable/disable DTLS on the Edge Router

Click on **DTLS List** in the **Configuration** section on the Edge Router website to access the DTLS configuration page.



The screenshot shows the Gen3A Router by NIVIS web interface. The left sidebar has sections for Configuration (Connectivity, Whitelist, Profiles, Setup Identifiers, DTLS List, Cloud Based NOC), Administration (System Upgrade, Transceiver Upgrade, Shutdown), and Session (Change Password, Log out). The main content area is titled "DTLS List". It includes fields for "Client Cert", "Client Key", and "CA Cert" with "Client Cert" selected, and "Browse..." and "Load" buttons. There are also fields for "Add MAC or MAC Address Range" (with a dropdown menu), "Cipher Suite" (set to "N/A"), and "DTLS Key" (with a dropdown menu). Below these are "Add" and "Remove" buttons. A note at the bottom says "You must press "Apply" to activate the changes!". A table lists a single entry: MAC Address or Range (0000:0000:0000:0000:FFFF:FFFF:FFFF:FFFF), Cipher Suite (PSK_AES128_CCM8_SHA256), and DTLS Key (***...**). At the bottom are "Apply" and "Cancel" buttons. The status bar at the bottom shows "© 2014 Nivis™ | Nivis™ Online" and "v2.1.11 | Running On v2.1.05 VR1000 FAR".

Select the Smart Object MAC, or select a range including the Smart Object MAC, or, if this is a device missing from the list, add the MAC. Then choose the cipher suite, enter the DTLS key if necessary, click **Add**, then click **Apply**.

NOTES

If you are configuring more than a single device, please update the settings for all of the devices, and then click **Apply**.

If you choose to enable DTLS and choose a cipher suite that requires a key or certificate, you will need to choose a matching key/certificate on the Smart Object and Edge Router

See [Configuring the Edge Router DTLS list](#) for details on setting the DTLS on Edge Router.

5.4 Change the DTLS Certificate / pre-shared Key

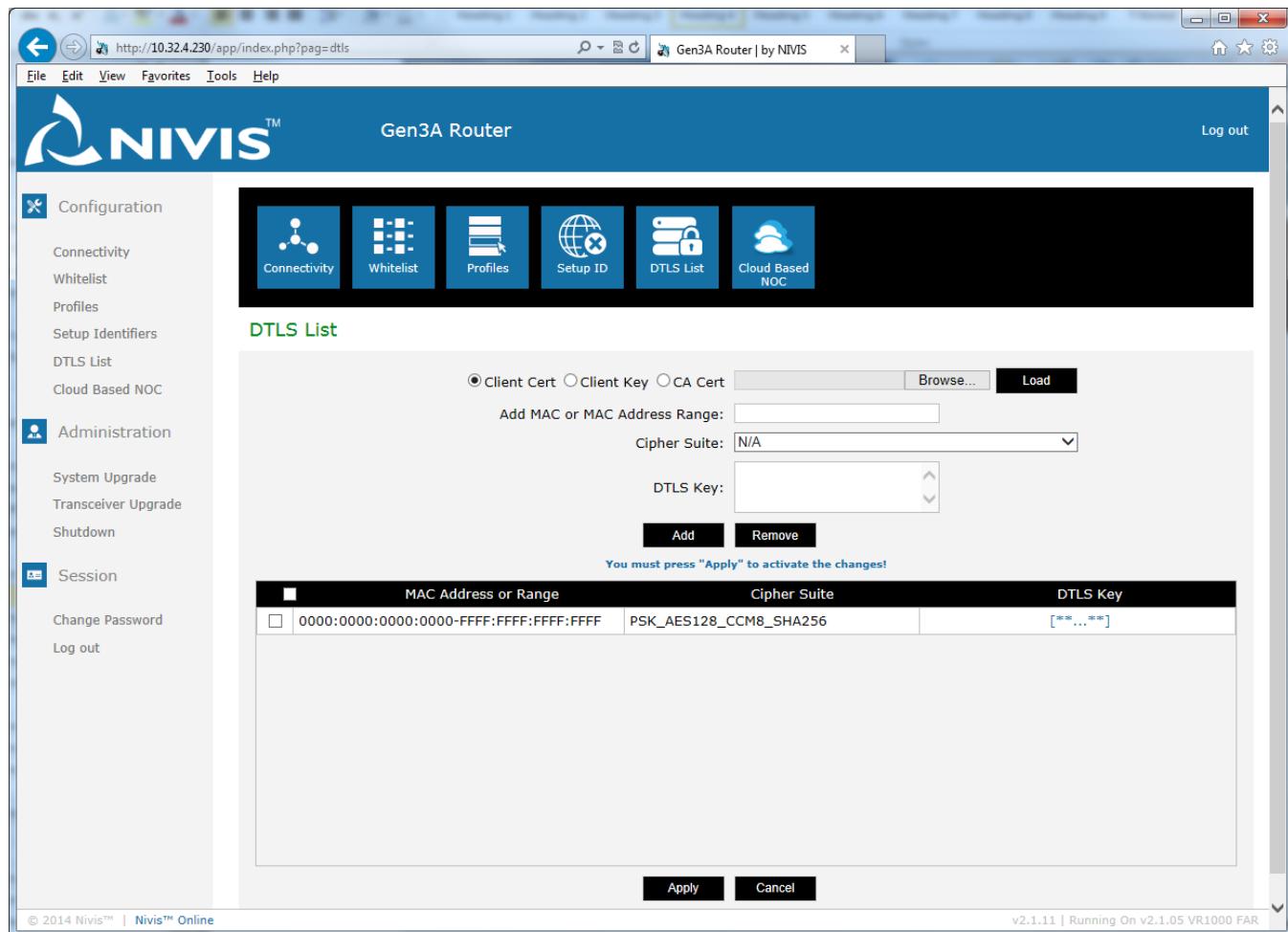
5.4.1 Overview

When DTLS is enabled and the cipher suite chosen require a pre-shared Key or a Certificate, the Key or Certificate on the Smart Object and Edge Router must match.

See [Configuring the Edge Router DTLS list](#) for details on which cipher suites require a pre-shared Key and which cipher suites require a Certificate.

5.4.2 Change the DTLS Key/Certificate

Click on **DTLS List** in the **Configuration** section on the Quark website to access the DTLS configuration page.



The screenshot shows the Gen3A Router NIVIS configuration interface. The left sidebar has sections for Configuration (Connectivity, Whitelist, Profiles, Setup Identifiers, DTLS List, Cloud Based NOC), Administration (System Upgrade, Transceiver Upgrade, Shutdown), and Session (Change Password, Log out). The main area title is "DTLS List". It contains fields for selecting "Client Cert", "Client Key", or "CA Cert" (with a "Browse..." button and "Load" button), "Add MAC or MAC Address Range" (input field), "Cipher Suite" (dropdown menu set to "N/A"), and "DTLS Key" (dropdown menu set to "[** ... **]"). Below these is a note: "You must press \"Apply\" to activate the changes!". A table lists a single entry: "MAC Address or Range" (0000:0000:0000:0000:FFFF:FFFF:FFFF:FFFF), "Cipher Suite" (PSK_AES128_CCM8_SHA256), and "DTLS Key" ([** ... **]). At the bottom are "Apply" and "Cancel" buttons. The footer says "© 2014 Nivis™ | Nivis™ Online" and "v2.1.11 | Running On v2.1.05 VR1000 FAR".

5.4.2.1 Change the DTLS Certificate on the Edge Router

Select the file type to load (Client Certificate/Client key/CA Certificate), browse for the file, and click **Load**.

NOTES

All three file types must be loaded on the Edge Router for a Certificate-based cipher suite to work.

Currently the Edge Router supports a single certificate per network.

5.4.2.2 *Change the DTLS Key on the Edge Router*

Select the Smart Object MAC, or select a range including the Smart Object MAC, or, if this is a device missing from the list, add the MAC. Then choose the cipher suite (a suite using a pre-shared Key), enter the DTLS key, click **Add**, then click **Apply**.

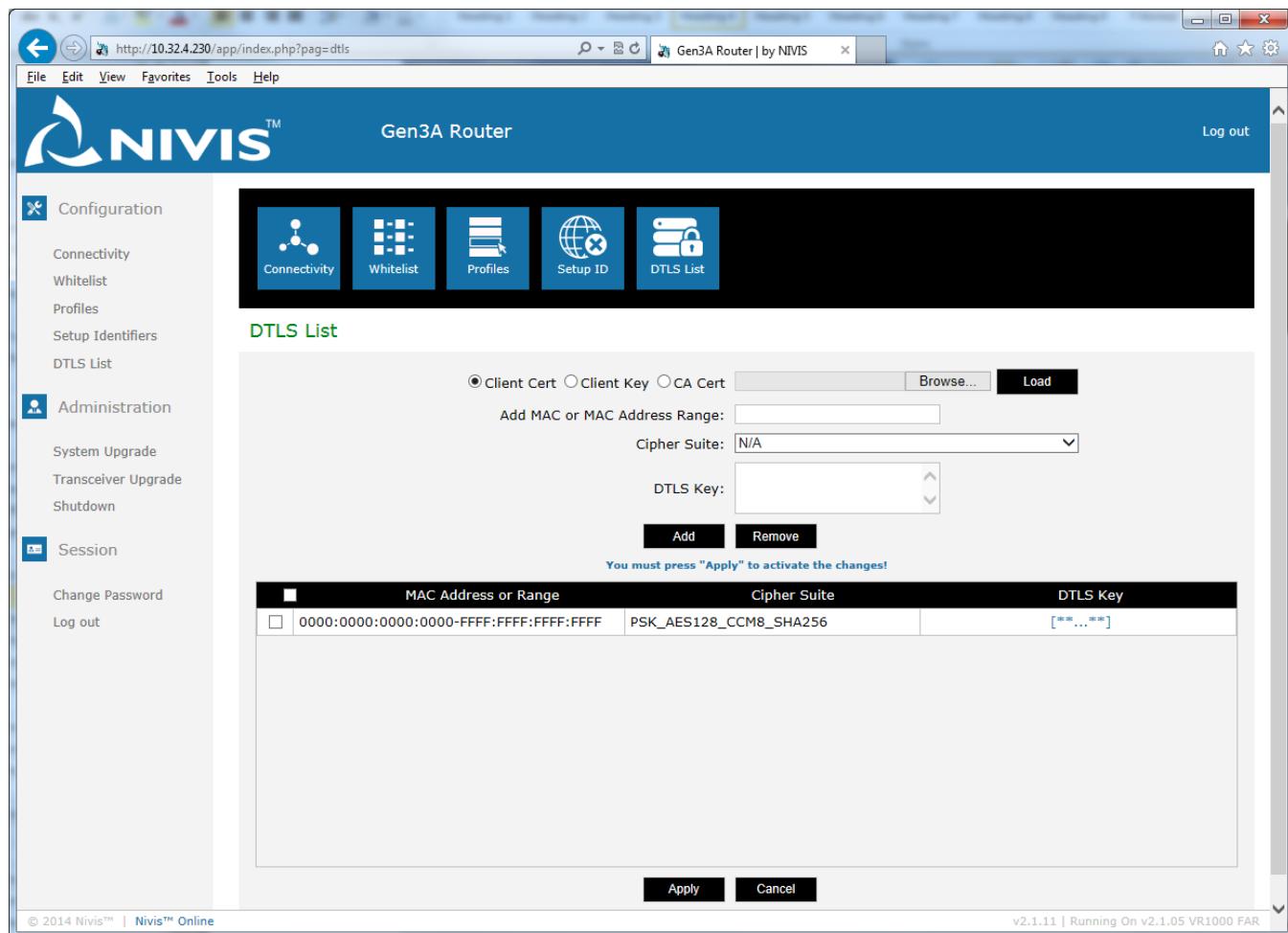
See [Configuring the Edge Router DTLS list](#) for details on setting the DTLS on the Edge Router.

5.5 Change the PANA Certificate / pre-shared Join Key

Network admission can be done based on pre-shared keys or based on PANA Certificates. The two methods are mutually exclusive.

5.5.1 Change the PANA Certificate

Click on **DTLS List** in the **Configuration** section on the Edge Router website to access the DTLS configuration page. The PANA certificates are loaded using the same page as for DTLS.



The screenshot shows the NIVIS Gen3A Router configuration interface. The left sidebar has sections for Configuration (Connectivity, Whitelist, Profiles, Setup Identifiers, DTLS List), Administration (System Upgrade, Transceiver Upgrade, Shutdown), and Session (Change Password, Log out). The main area is titled "DTLS List". It contains fields for selecting file type (radio buttons for Client Cert, Client Key, CA Cert), a "Browse..." button, and a "Load" button. Below these are fields for "Add MAC or MAC Address Range" (text input), "Cipher Suite" (dropdown menu showing "N/A"), and "DTLS Key" (text input with dropdown arrows). At the bottom are "Add" and "Remove" buttons, and a note: "You must press "Apply" to activate the changes!". A table below shows a single entry: MAC Address or Range (0000:0000:0000:0000:FFFF:FFFF:FFFF:FFFF), Cipher Suite (PSK_AES128_CCM8_SHA256), and DTLS Key (***...***). At the very bottom are "Apply" and "Cancel" buttons. The browser address bar shows "http://10.32.4.230/app/index.php?pag=dtls".

Select the file type to load (Client Certificate/Client key/CA Certificate), browse for the file, and click **Load**.

NOTES

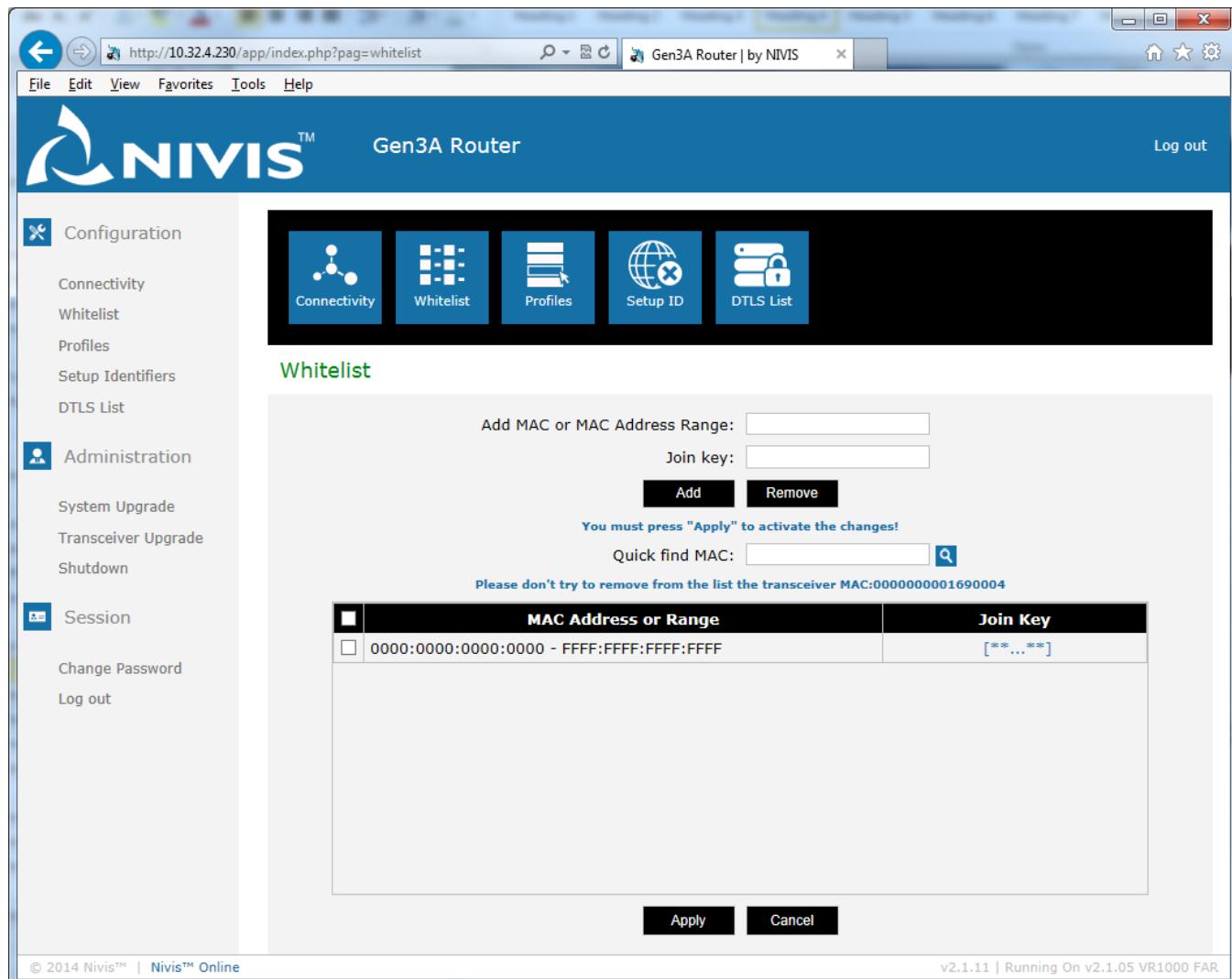
All three file types must be loaded on the Edge Router for a Certificate-based cipher suite to work.

Currently the Edge Router supports a single certificate per network.

5.5.2 Change the pre-shared Join Key

The instructions below are valid for both PANA Enabled and Disabled.

Click on **Whitelist** in the **Configuration** section on the Edge Router website.



The screenshot shows the NIVIS Gen3A Router configuration interface. The left sidebar menu includes Configuration, Administration, and Session sections. The Configuration section is currently selected, showing sub-options like Connectivity, Whitelist, Profiles, Setup Identifiers, and DTLS List. The main content area is titled "Whitelist". It features input fields for "Add MAC or MAC Address Range" and "Join key", with "Add" and "Remove" buttons. A note says "You must press "Apply" to activate the changes!". Below is a table with one entry:

	MAC Address or Range	Join Key
<input type="checkbox"/>	0000:0000:0000:0000 - FFFF:FFFF:FFFF:FFFF	[**...**]

At the bottom are "Apply" and "Cancel" buttons. The footer indicates the page is running on v2.1.11 | Running On v2.1.05 VR1000 FAR.

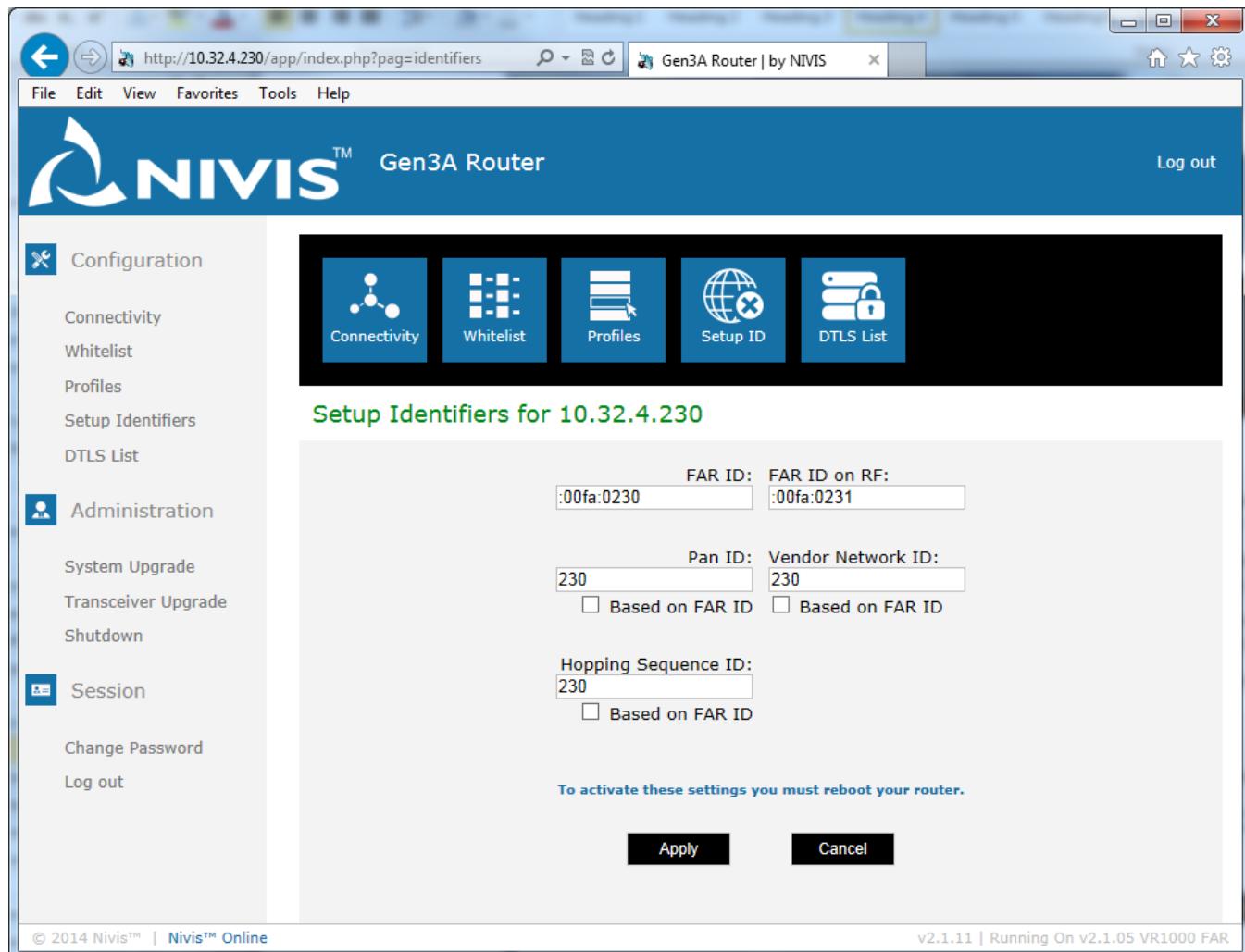
Select the Smart Object MAC, or select a range including the Smart Object MAC, or, if this is a device missing from the list, add the MAC. Then enter the Join Key, click **Add**, then click **Apply**.

See [Configuring the Edge Router Whitelist](#) for details on setting the Join Key on the Edge Router.

5.6 Change the Network ID

The Net ID on the Smart Object must match the Vendor Network ID on the Edge Router to which it needs to join.

Click on **Setup Identifiers** in the **Configuration** section on the Edge Router website.



The screenshot shows the NIVIS Gen3A Router configuration interface. The left sidebar has sections for Configuration (Connectivity, Whitelist, Profiles, Setup Identifiers, DTLS List), Administration (System Upgrade, Transceiver Upgrade, Shutdown), and Session (Change Password, Log out). The main content area is titled "Setup Identifiers for 10.32.4.230". It contains fields for FAR ID (:00fa:0230) and Vendor Network ID (:00fa:0231). Below these are fields for Pan ID (230) and Hopping Sequence ID (230), each with a checkbox for "Based on FAR ID". A note at the bottom says "To activate these settings you must reboot your router." with "Apply" and "Cancel" buttons.

Modify the **Vendor Network ID**, then click **Apply**.

NOTE

Please be aware, the Edge Router will reboot and the network will unjoin. The Smart Objects will rejoin only after their Net ID settings match the Vendor Network ID on the Router.

See [Configuring the Edge Router Identifiers](#) for details on setting the Vendor Network ID on the Edge Router.

5.7 Set-up Edge Router - Cloud-Based NOC communication

Normal deployment scenario requires that the NMS - a subsystem of the Cloud-Based NOC – expose a public IPv4 address. The Edge Router may or may not have a public IPv4 address.

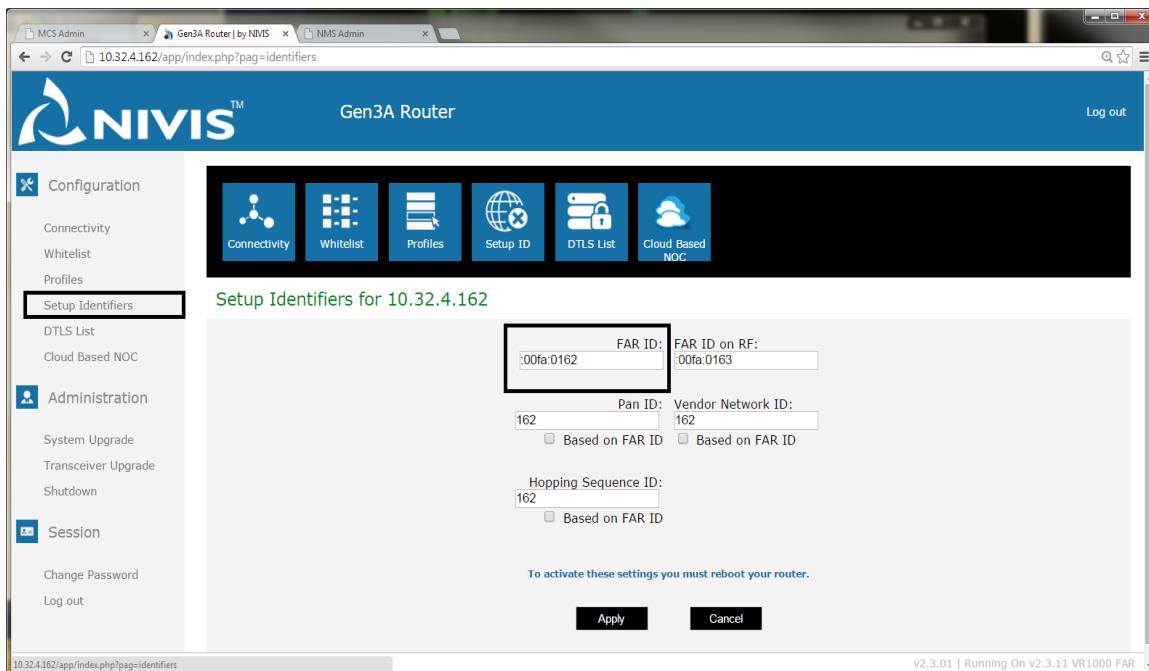
Recommended configuration is to use VPN for Edge Router - NMS connectivity.

Non-VPN communication is only acceptable for laboratory tests.

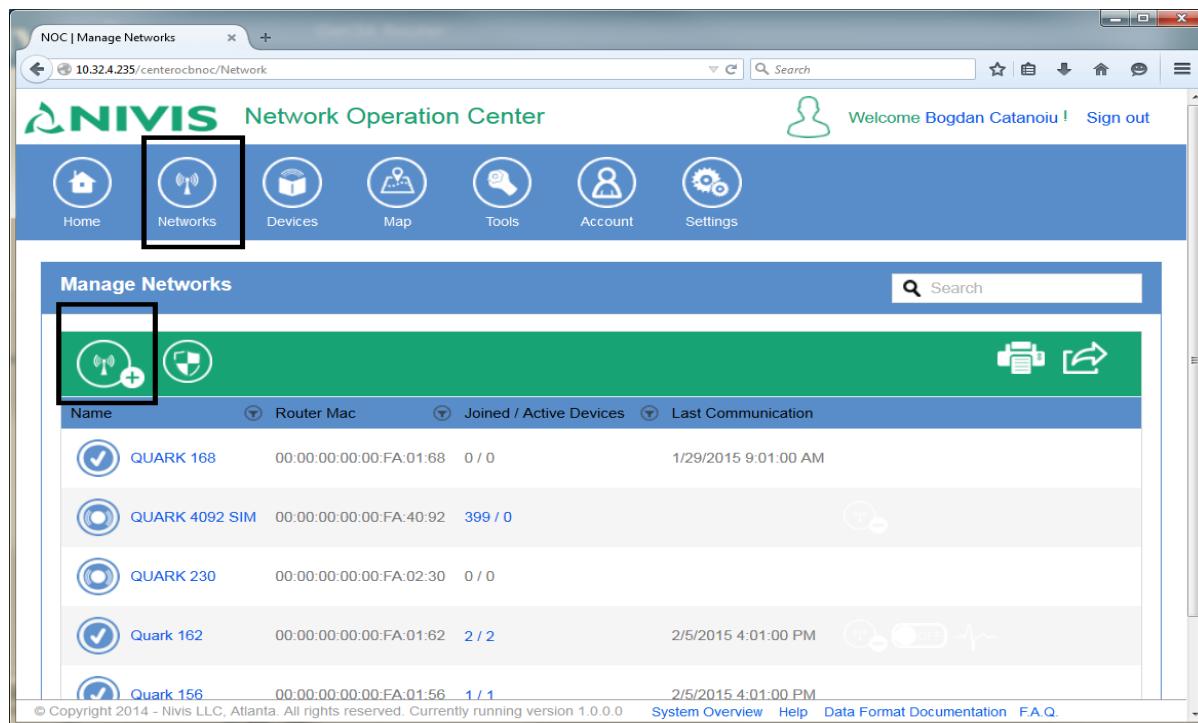
5.7.1 Add Edge Router in the Cloud-Based NOC Whitelist

Before trying to connect an Edge Router to the Cloud-Based NOC, the Edge Router FAR ID must be added to the Cloud-based NOC. The Cloud-Based NOC identifies networks using their controlling Edge Router.

1. Point a web browser to the Edge Router website (http://<router_ip>/), enter credentials
2. Go to “Setup Identifiers” page
3. Read or copy the FAR ID



4. Point a web browser to the Cloud-Based NOC website, enter credentials
5. Go to on “Networks” page
6. Press “Register Network” button



NOC | Manage Networks

Welcome Bogdan Catanoiu | Sign out

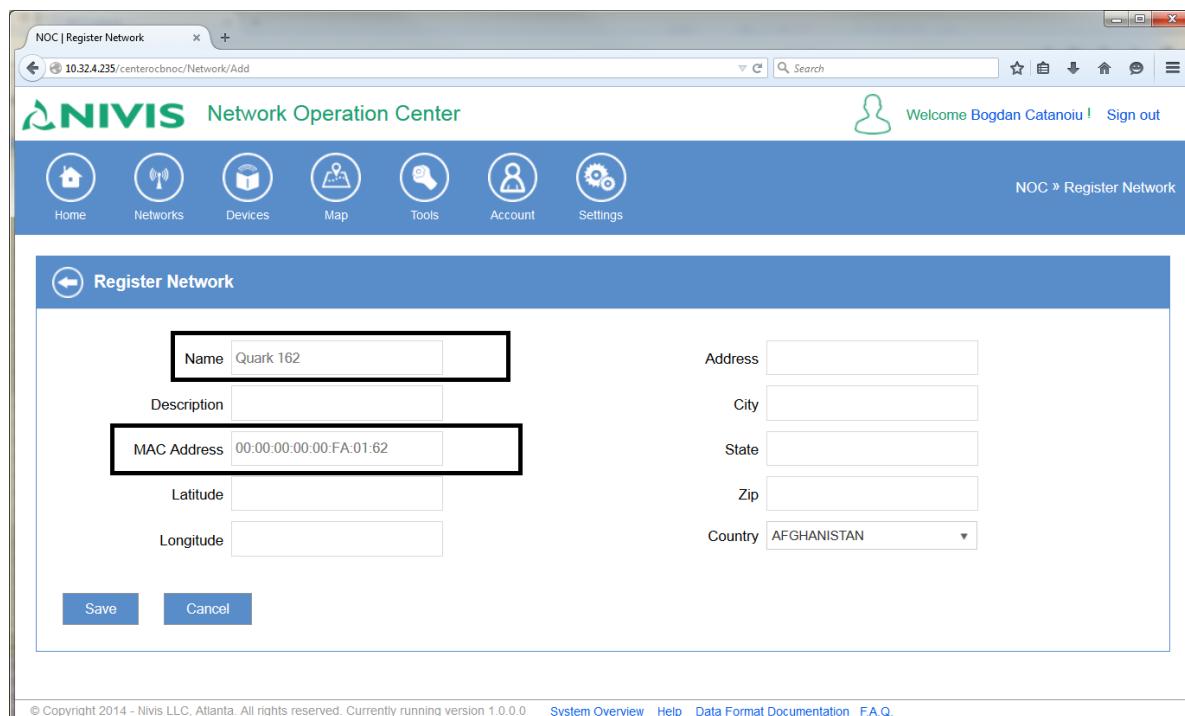
Home Networks Devices Map Tools Account Settings

Manage Networks

Name	Router Mac	Joined / Active Devices	Last Communication
QUARK 168	00:00:00:00:FA:01:68	0 / 0	1/29/2015 9:01:00 AM
QUARK 4092 SIM	00:00:00:00:FA:40:92	399 / 0	
QUARK 230	00:00:00:00:FA:02:30	0 / 0	
Quark 162	00:00:00:00:FA:01:62	2 / 2	2/5/2015 4:01:00 PM
Quark 156	00:00:00:00:FA:01:56	1 / 1	2/5/2015 4:01:00 PM

Copyright 2014 - Nivis LLC, Atlanta. All rights reserved. Currently running version 1.0.0.0. [System Overview](#) [Help](#) [Data Format Documentation](#) [F.A.Q.](#)

7. Provide a network Name.
8. Use the Edge Router FAR ID identified at step 3 above to provide the “MAC Address”.
9. Press “Save”.



NOC | Register Network

Welcome Bogdan Catanoiu | Sign out

Home Networks Devices Map Tools Account Settings

Register Network

Name	Quark 162	Address	
Description		City	
MAC Address	00:00:00:00:FA:01:62	State	
Latitude		Zip	
Longitude		Country	AFGHANISTAN

Save Cancel

Copyright 2014 - Nivis LLC, Atlanta. All rights reserved. Currently running version 1.0.0.0. [System Overview](#) [Help](#) [Data Format Documentation](#) [F.A.Q.](#)

5.7.2 Set-up Edge Router and NMS communication using VPN [RECOMMENDED]

These steps below load Open VPN certificates into NMS and Edge Router. The steps are performed **only once** for NMS, and **only once** for each Edge Router, and then the Edge Router can be switched between “transparent” and “standalone” modes indefinitely without the need to re-load certificates.

Only if the root CA was changed on the Cloud-Based NOC (or when the Edge Router needs to connect to a different cloud-Based NOC, with a different root CA) the Edge Router will need to load a new certificate – generated using the new root CA.

NOTE

The certificate sets for Edge Router and NMS must be delivered in **.tar.gz** format.

The Edge Router certificate set is specific per Edge Router.

Do NOT attempt to use a certificate set built for an Edge Router on a different Edge Router.

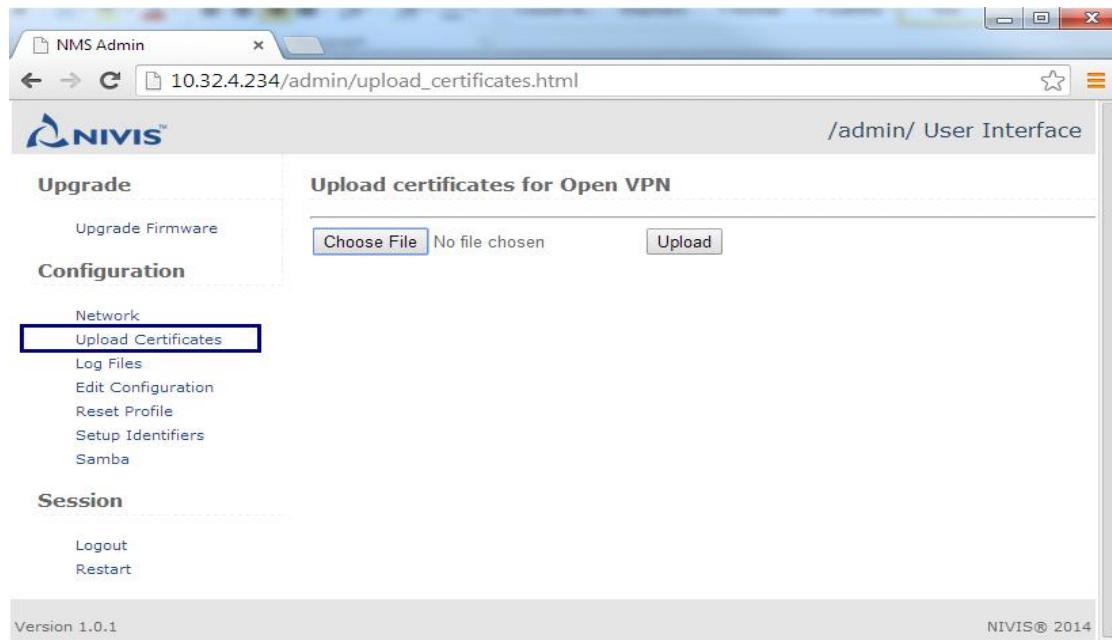
The Edge Routers are delivered with a set of certificates pre-installed. The certificate set is compatible only with Cloud-based NOC hosted by Nivis.

There's no need to upload new certificate set on Edge Routers connecting to Nivis-hosted Cloud-based NOC.

In any other case, the certificate set needs to be uploaded to the Edge Router

5.7.2.1 Set-up NMS VPN certificates

10. Point a web browser to the NMS /admin/ website (http://<nms_ip>/admin/), enter credentials
11. Go to “Upload Certificates” page
12. Press “Choose File” button
13. Select the archive holding the NMS certificate set
14. Press “Upload” button

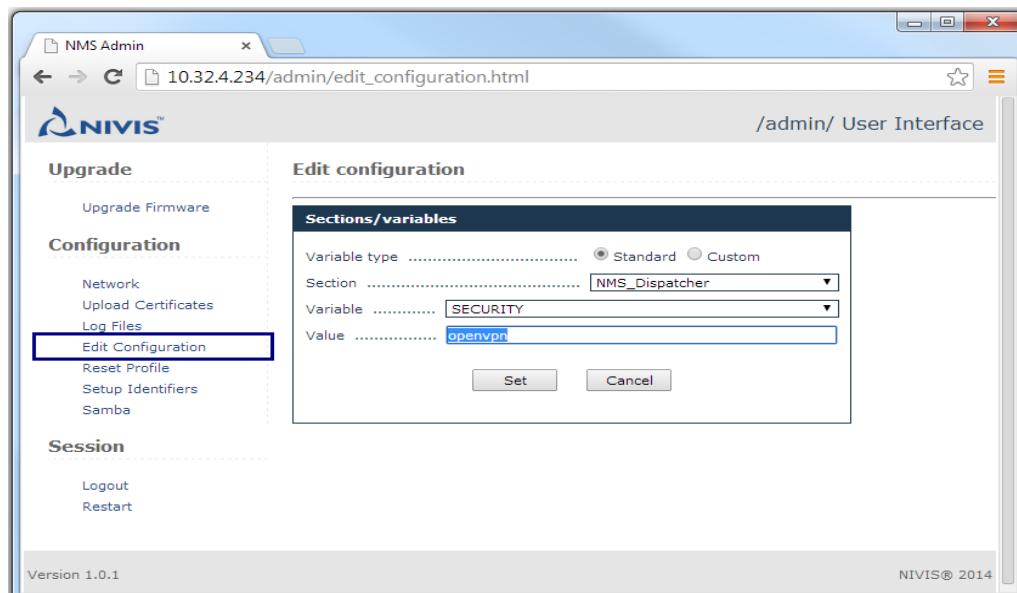


NOTE

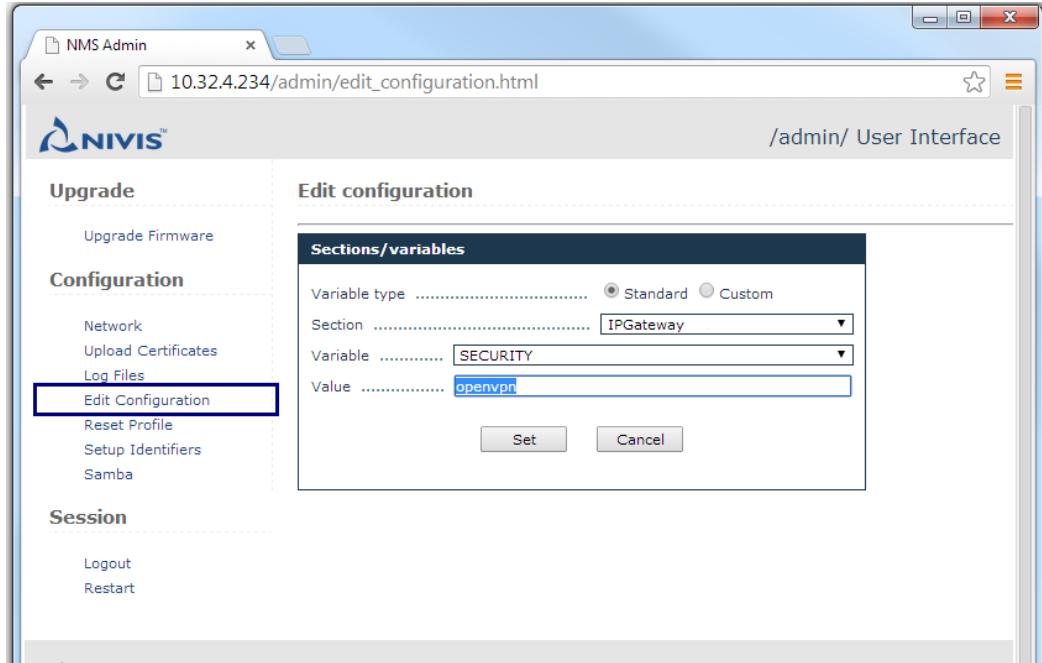
This steps has to be done only once, regardless of the number of subsequent switches of communication between “openvpn” and “none”

5.7.2.2 Configure NMS modules to use OpenVPN

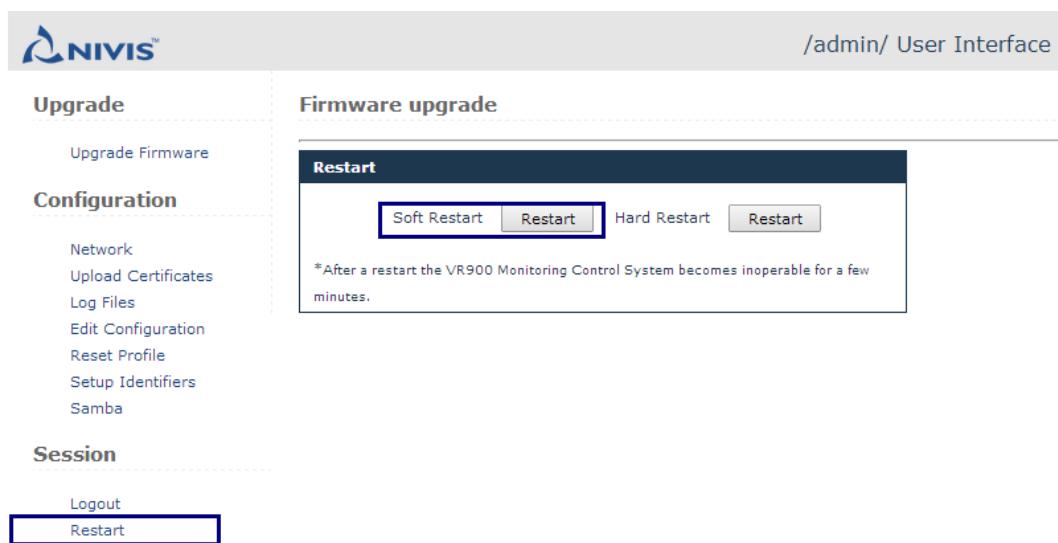
1. Point a web browser to the NMS /admin/ website (http://<nms_ip>/admin/), enter credentials
2. Go to “Edit configuration” page
3. Choose “NMS_Dispatcher” from “Section” drop-down
4. Choose “SECURITY” in “Variable” drop-down
5. Make sure the “Value” edit reads “openvpn” (no quotes, not other char)



6. Choose “IPGateway” from “Section” drop-down
7. Choose “SECURITY” in “Variable” drop-down
8. Make sure the “Value” edit reads “openvpn” (no quotes, not other char)

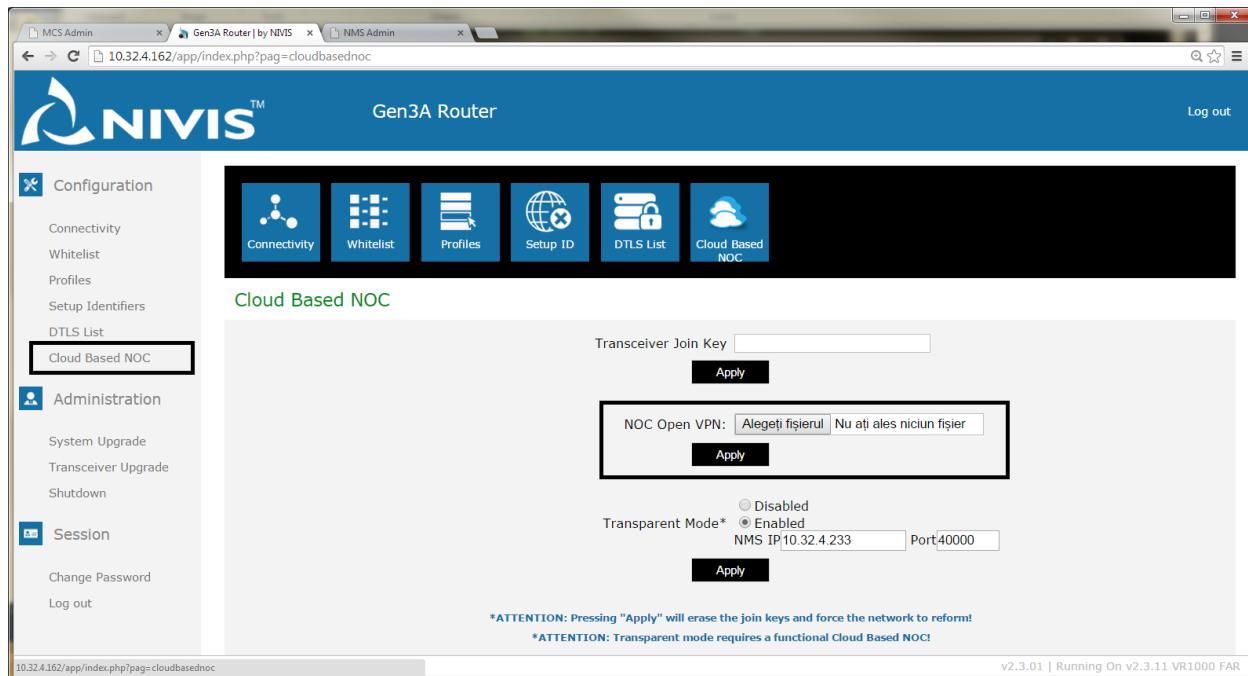


9. Go to “Restart” page
10. Perform a “Soft Restart”



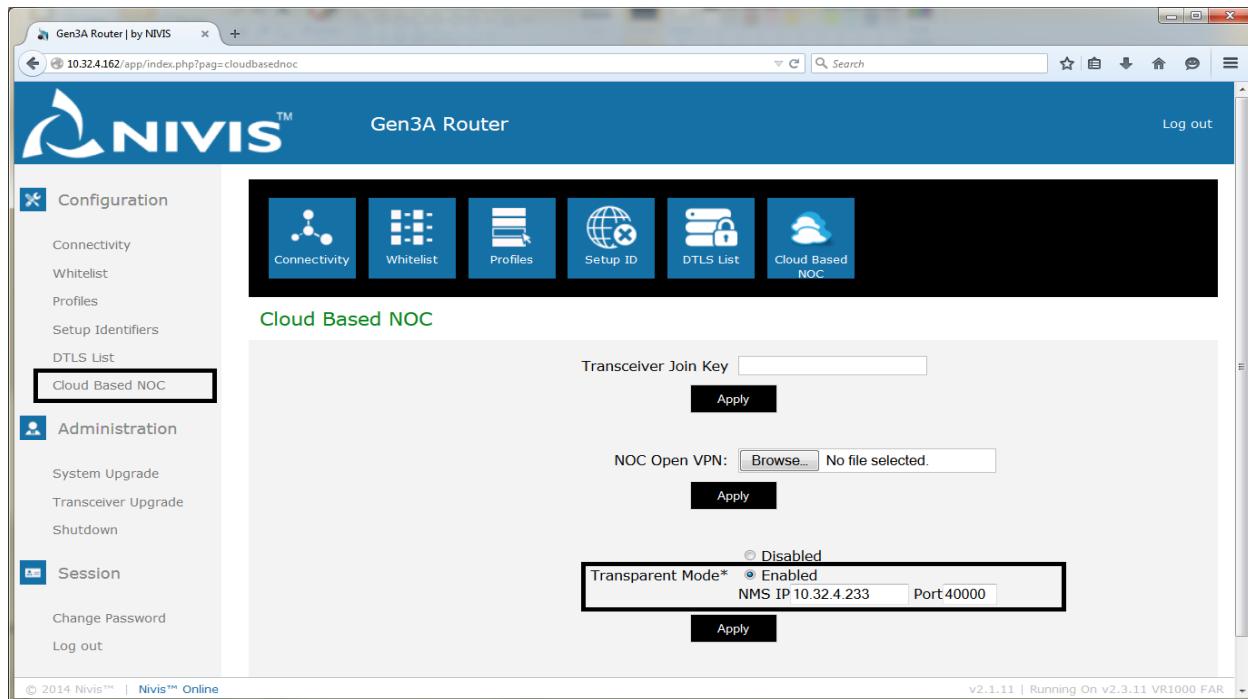
5.7.2.3 Set-up Edge Router VPN certificates

1. Point a web browser to the Edge Router website (http://<router_ip>/), enter credentials
2. Go to “Cloud Based NOC” page
3. Press the “Choose File” button corresponding to ‘NOC Open VPN’ label
4. Browse for the archive with the Edge Router certificate set
5. Press the corresponding “Apply” button



5.7.2.4 Set-up Edge Router in “transparent” mode (connect to NMS, use openvpn)

1. Point a web browser to the Edge Router website (http://<router_ip>/), enter credentials
2. Go to “Cloud Based NOC” page
3. Click to Enable the transparent mode
4. Fill in the NMS **Public IPv4**
5. Fill in the NMS port (default: 40000)
6. Press “Apply” button



NOTE

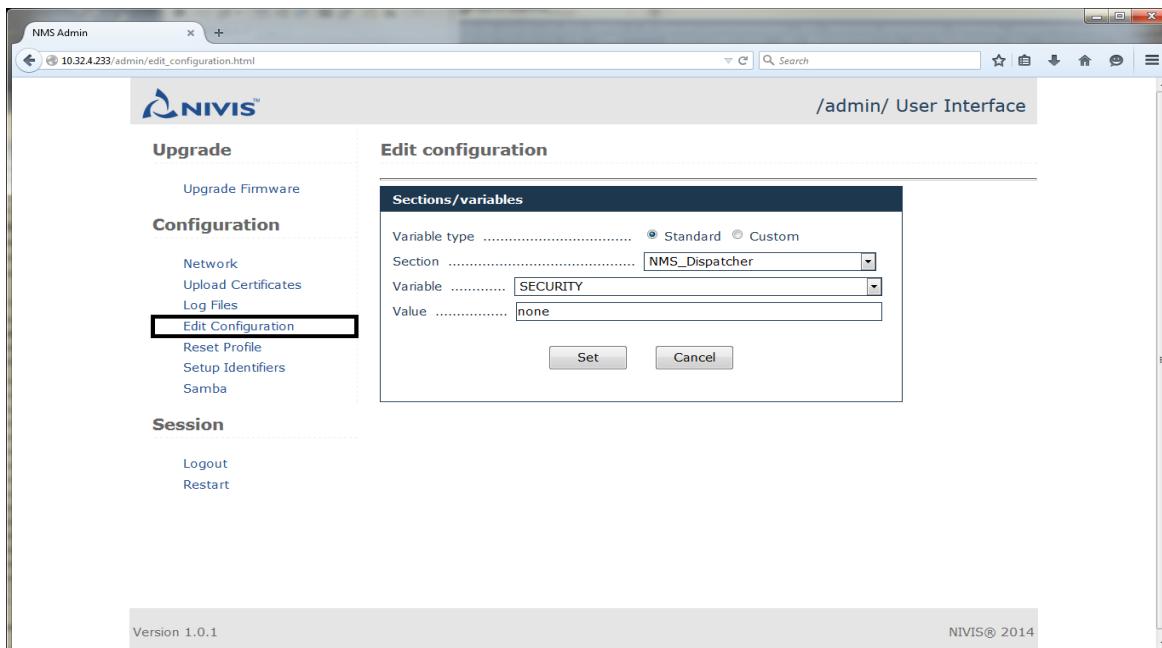
Enabling “transparent” mode on Edge Router automatically enables the “openvpn” communication for Edge Router relevant module (BHManager)

5.7.3 [Alternate] Set-up Edge Router / NMS plain-text communication (Use for lab tests only)

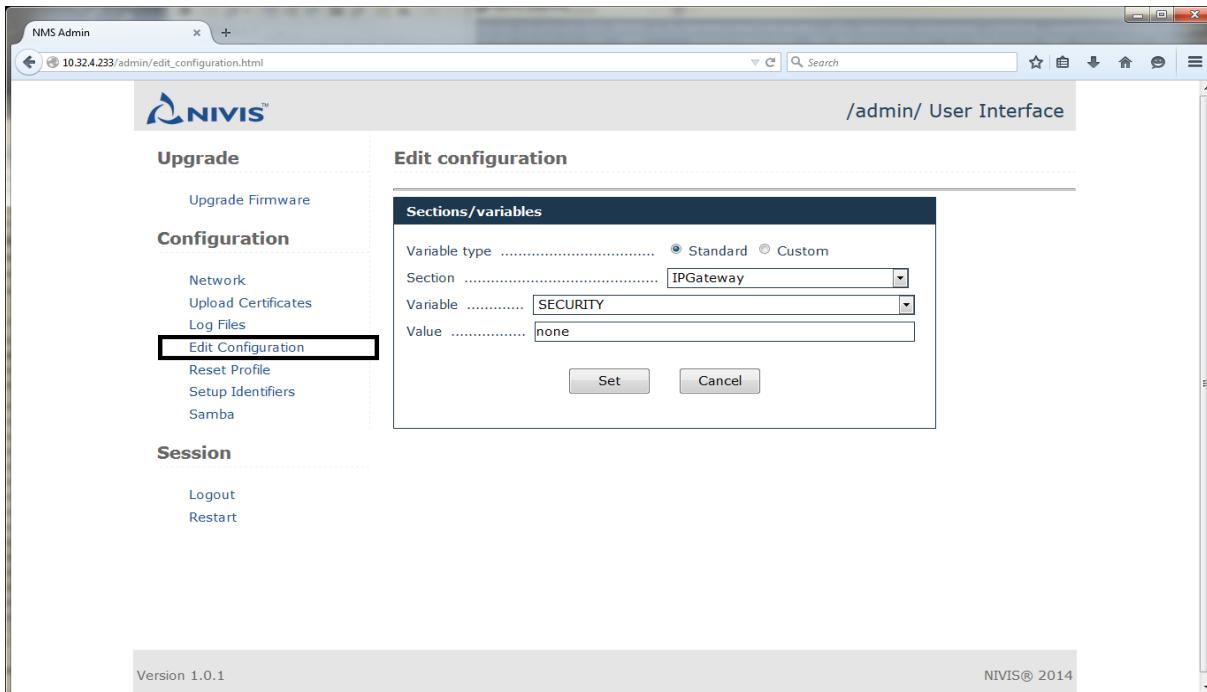
These steps below configure NMS and Edge Router for non-VPN (open/plaintext) communication. The steps are performed **only once** for NMS, but **each time** the Quark is switched between “standalone” and “transparent” mode, because setting the “transparent” mode automatically enable VPN communication and this step disables it.

5.7.3.1 Configure NMS modules to use open communication

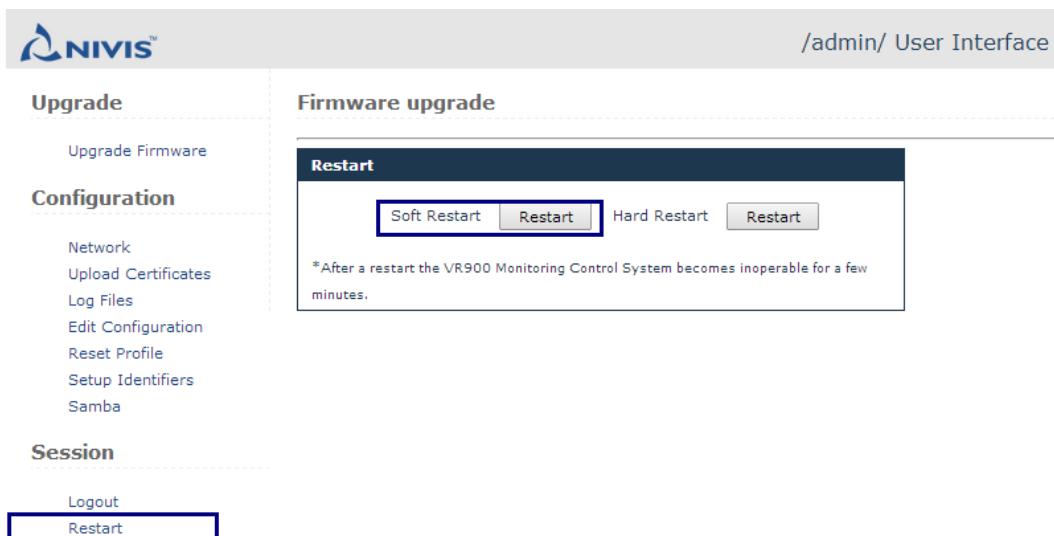
1. Point a web browser to the NMS /admin/ website (http://<nms_ip>/admin/), enter credentials
2. Go to “Edit configuration” page
3. Choose “NMS_Dispatcher” from “Section” drop-down
4. Choose “SECURITY” in “Variable” drop-down
5. Set the field “Value” to “none” (no quotes, not other char)



6. Choose “IPGateway” from “Section” drop-down
7. Choose “SECURITY” in “Variable” drop-down
8. Set the field “Value” to “none” (no quotes, not other char)

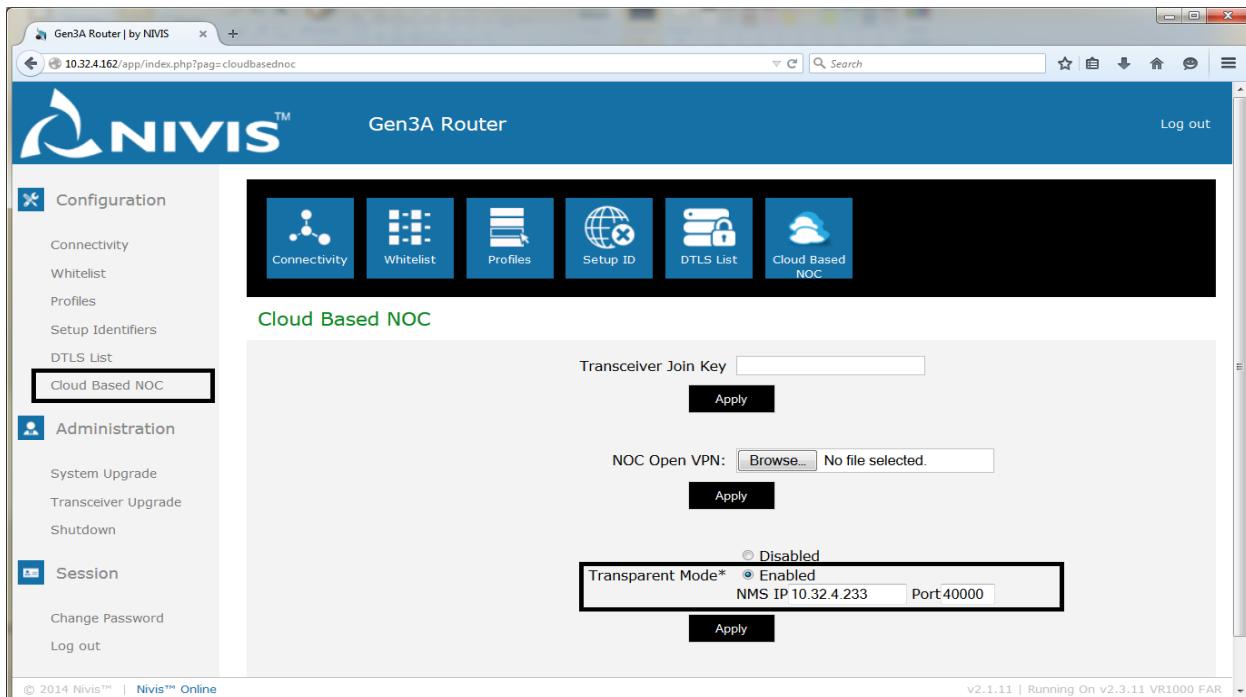


9. Go to “Restart” page
10. Perform a “Soft Restart”



5.7.3.2 Set-up the Edge Router in “transparent” mode – connect to the Cloud-based NOC

1. Point a web browser to the Edge Router website (http://<quark_ip>/), enter credentials
2. Go to “Cloud Based NOC” page
3. Click to Enable the transparent mode
4. Fill in the NMS **Public IPv4**
5. Fill in the NMS port (default: 40000)
6. Press “Apply” button



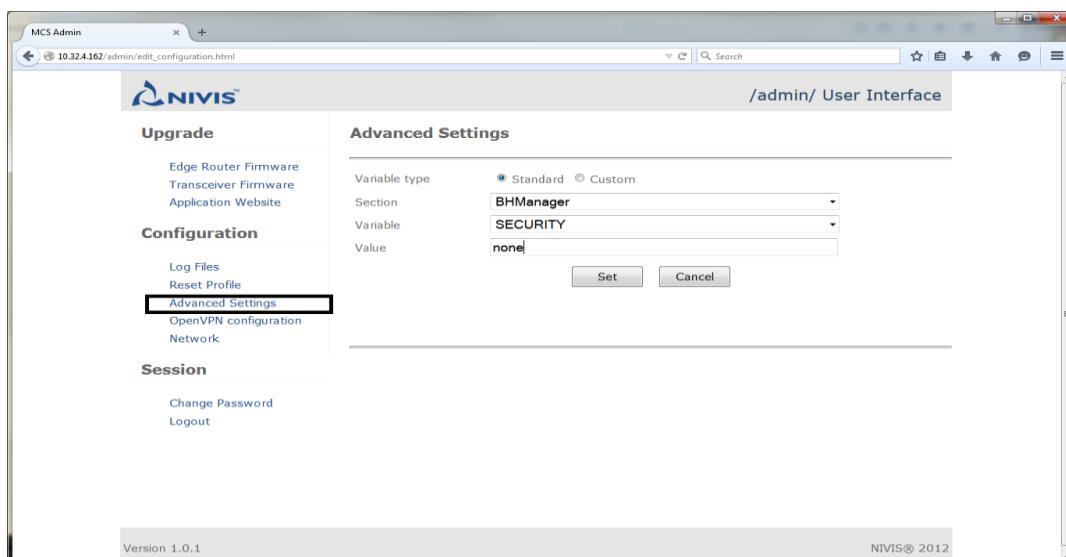
NOTE

Enabling “transparent” mode on Edge Router automatically enables the “openvpn” communication for Edge Router relevant module (BHManager). Since this step uses open communication, the next step is necessary to set the communication back to “open” for BHManager.

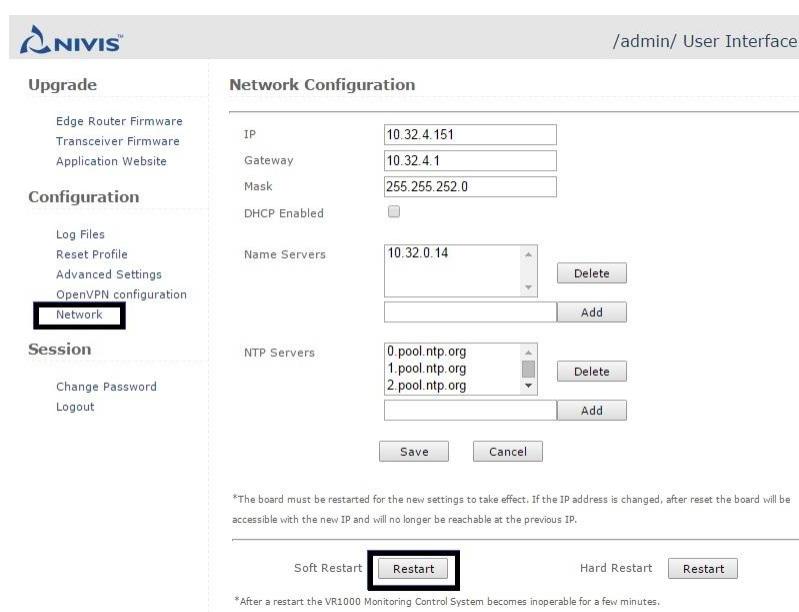
5.7.3.3 Configure Edge Router modules to use open communication

This step must be performed **after** setting the “transparent” mode, as setting the transparent mode automatically configures the Edge Router modules to use OpenVPN. After setting the “transparent” mode, the Edge Router software restarts rendering the web interface inaccessible for few tens of seconds. Wait until the web interface is accessible.

1. Point a web browser to the Edge Router /admin/ website (http://<quark_ip>/admin/), enter credentials
2. Go to “Advanced settings” page
3. Choose “BHManager” from “Section” drop-down
4. Choose “SECURITY” in “Variable” drop-down
5. Set the field “Value” to “none” (no quotes, not other char)



6. Go to “Network” page
7. Perform a “Soft Restart” to activate the changes



6 Use Cases

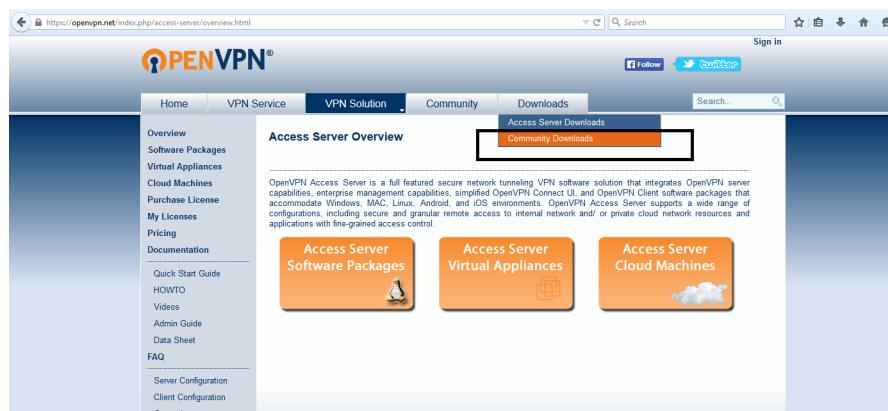
6.1 Setting the PC-to-device communication using Edge Router in transparent mode

The PC-to-Device communication is taking place via the following path: PC – NMS – Edge Router – Device. There are distinct settings to be made in case the PC runs Windows or Linux OS. The PC / NMS communication can be VPN-based or non-VPN based. The NMS / Edge Router are always VPN-based on real deployments, but for lab tests, it can be non-VPN (Setting up the NMS/VR1000 communication was covered above). The sections below describe possible combinations to set-up the remaining segment: PC/NMS.

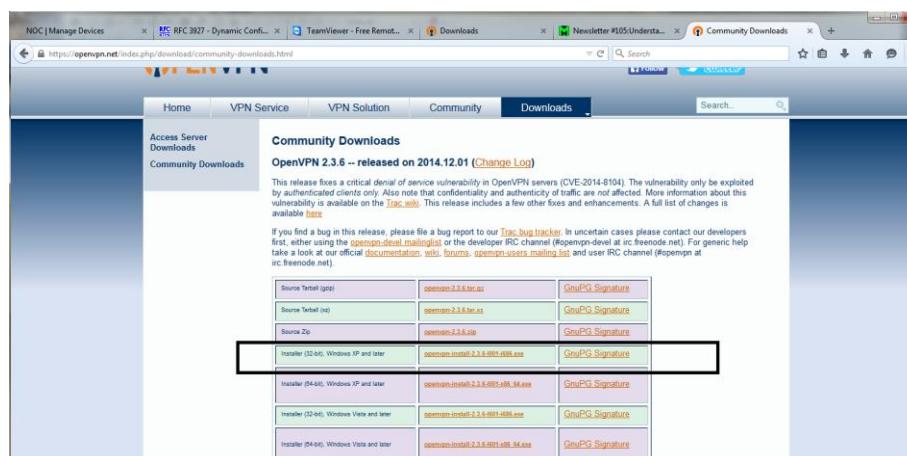
6.1.1 PC-to-device IPv6 communication for Windows user, VPN based

6.1.1.1 *Install Open VPN on Windows*

1. Go to <https://openvpn.net/>, select ‘VPN Solution’ option and choose ‘Community Downloads’ tab option:



2. Download the release ‘*.exe’ that suits user computer. For example, there was chosen the following openvpn for 32-bit windows computer:



3. Install it as **administrator** in the (preferably) default directory “C:\Program Files\OpenVPN”.

6.1.1.2 Setup Windows/NMS IPv4 communication VPN-based

1. Get the following certificates: **nms_ca.crt**, **nms_remote_user.crt**, **nms_remote_user.key** from the NMS administrator.
2. Create a configuration file ‘*.ovpn’ in the “c:\Program Files\OpenVPN\config” with the following information (replace placeholders “<server_public_IPv4>” and “<server_port>” with the appropriate values):

```
client
dev tun1500
proto tcp
remote <server_public_IPv4> <server_port>
resolv-retry infinite
nobind
ca nms_ca.crt
cert nms_remote_user.crt
key nms_remote_user.key
comp-lzo
ns-cert-type server
verb 3
```

3. Start as **administrator** the OpenVPN by executing the exe file: "C:\Program Files\OpenVPN\bin\openvpn-gui.exe"
4. After it was started, right click on the icon of the VPN application and choose to connect to VPN Server.
5. Test the VPN connection:
 - a. Check if the interface with the assigned VPN ipv4 address <client_VPN_IPv4> was created:
 - i. ipconfig
 - ii. Check in the command output shows and IPv4 in the range **10.185.0.0/24**
 - b. Check the VPN connection with server:
 - i. ping **10.185.0.1**

NOTE

Use 1194 for <server_port> variable

The NMS server is configured by default to provide to the clients the <client_VPN_IPv4> in the range **10.185.0.0/24**

The NMS server is configured with <server_VPN_IPv4>: **10.185.0.1**

6.1.1.3 Setup Windows/NMS IPv6 communication VPN-based

1. Prepare to connect to NMS from Windows PC:
 - a. Use **ipconfig** command to get the local VPN IPv4 address: <client_VPN_IPv4>, for example 10.185.0.14
 - b. The server (NMS) VPN IPv4 address <server_VPN_IPv4> is known, configured by default as: **10.185.0.1**
 - c. Compute the IPv6 address <client_VPN_IPv6> based on client VPN IPv4 address, using FD00 as prefix, and <client_VPN_IPv4> converted to hex as postfix. For example:
 - i. Computed IPv6: FD00::0AB9:000E
 1. FD00 is a MUST
 2. **0AB9:000E** is **10.185.0.14** converted to hex
2. Connect to NMS:
 - a. On **Windows PC** (on administrator console): create 6in4 tunnel
 - i. netsh interface ipv6 add v6v4tunnel remote_user_tunn <client_VPN_IPv4> <server_VPN_IPv4>
 - ii. netsh interface ipv6 add address remote_user_tunn <client_VPN_IPv6>/128
 - iii. netsh interface ipv6 add route ::/0 remote_user_tunn
 - b. On **NMS**: create route to remote user machine
 - i. sudo ip route add <client_VPN_IPv6>/128 via ::<client_VPN_IPv4>

Example using the variables chosen above:

- a. On **Windows PC** (on administrator console): create 6in4 tunnel
 - i. netsh interface ipv6 add v6v4tunnel remote_user_tunn 10.185.0.14 10.185.0.1
 - ii. netsh interface ipv6 add address remote_user_tunn FD00::0AB9:000E/128
 - iii. netsh interface ipv6 add route ::/0 remote_user_tunn
- a. On **NMS**: create route to remote user machine
 - i. sudo ip route add FD00::0AB9:000E/128 via ::10.185.0.14

NOTE

All configurations are preserved if the OpenVPN Client is restarted

6.1.1.4 Test Windows PC/NMS IPv6 communication

1. Select an address of an already connected Edge Router or Smart Object as destination (ex. 2012:0:0:2::00fa:0162):
 - a. **ping -6 2012:0:0:2::00fa:0162**

6.1.1.5 Cleaning up the remote access to NMS from Windows PC

In order to clean up the settings after the connectivity test was done, the following steps are necessary:

1. Disconnect from NMS:
 - a. On **Windows PC** (on administrator console), close 6in4 tunnel:
 - i. netsh interface ipv6 delete address remote_user_tunn <client_VPN_IPv6>/128
 - ii. netsh interface ipv6 delete route ::/0 remote_user_tunn
 - iii. netsh interface ipv6 delete remote_user_tunn
 - b. On **NMS**, remove route to Windows PC:
 - i. sudo ip route del <client_VPN_IPv6>/128 via ::<client_VPN_IPv4>

Example using the variables chosen above:

- a. On **Windows PC** (on administrator console), close 6in4 tunnel:
 - ii. netsh interface ipv6 delete address remote_user_tunn FD00::0AB9:000E/128
 - iii. netsh interface ipv6 delete route ::/0 remote_user_tunn
 - iv. netsh interface ipv6 delete remote_user_tunn
 - b. On **NMS**, remove route to Windows PC:
 - v. sudo ip route del FD00::0AB9:000E/128 via ::10.185.0.14
2. Remove VPN certificates and key for remote user from path c:\Program Files\OpenVPN\config on Windows PC.

6.1.2 PC-to-device IPv6 communication for Windows user, non-VPN based

The non-VPN based connectivity will only work if the PC can communicate directly via IPv4 with the NMS (the NMS IPv4 is visible to the PC)

6.1.2.1 *Setup Windows/NMS IPv6 communication non-VPN-based*

1. Test IPv4 connection with NMS
 - a. On **NMS**, use **ifconfig** to get the remote(NMS) IPv4 address (<server_IPv4>), for example 10.32.4.233
 - b. On **Windows PC**, test the connectivity with NMS:
 - i. ping <server_IPv4>
2. Prepare to connect to NMS from remote user machine:
 - a. On PC client, use **ipconfig** command to get the local IPv4 address: <client_IPv4>, for example 10.32.4.131
 - b. Compute the IPv6 address <client_IPv6> based on client IPv4 address, using FD00 as prefix, and <client_IPv4> converted to hex as postfix. For example:
 - i. Computed IPv6: FD00::0A20:0483
 1. FD00 is a MUST
 2. **0A20:0483** is **10.32.4.131** converted to hex
3. Connect to NMS:
 - a. On **Windows PC** (on administrator console), create 6in4 tunnel:
 - i. netsh interface ipv6 add v6v4tunnel remote_user_tunn <client_IPv4> <server_IPv4>
 - ii. netsh interface ipv6 add address remote_user_tunn <client_IPv6>/128
 - iii. netsh interface ipv6 add route ::/0 remote_user_tunn
 - b. On **NMS** add route to Windows PC
 - i. sudo ip route add <client_IPv6>/128 via ::<client_IPv4>

Example using the variables chosen above:

- a. On **Windows PC** (on administrator console), create 6in4 tunnel:
 - i. netsh interface ipv6 add v6v4tunnel remote_user_tunn 10.32.4.131 10.32.4.233
 - ii. netsh interface ipv6 add address remote_user_tunn FD00::0A20:0483/128
 - iii. netsh interface ipv6 add route ::/0 remote_user_tunn
- b. On **NMS** add route to Windows PC
 - i. sudo ip route add FD00::0A20:0483/128 via ::10.32.4.131

6.1.2.2 *Test Windows PC/NMS IPv6 communication*

1. Select an address of an already connected Edge Router or Smart Object as destination (ex. 2012:0:0:2::00fa:0162):
 - a. **ping -6 2012:0:0:2::00fa:0162**

6.1.2.3 Cleaning up the remote access to NMS from Windows PC

In order to clean up the settings after the connectivity test was done, the following steps are necessary:

1. Disconnect from NMS:
 - a. On **Windows PC** (on administrator console), close 6in4 tunnel:
 - i. netsh interface ipv6 delete address remote_user_tunn <client_IPv6>/128
 - ii. netsh interface ipv6 delete route ::/0 remote_user_tunn
 - iii. netsh interface ipv6 delete remote_user_tunn
 - b. On **NMS**, remove route to Windows PC:
 - i. sudo ip route del <client_IPv6>/128 via ::<client_IPv4>

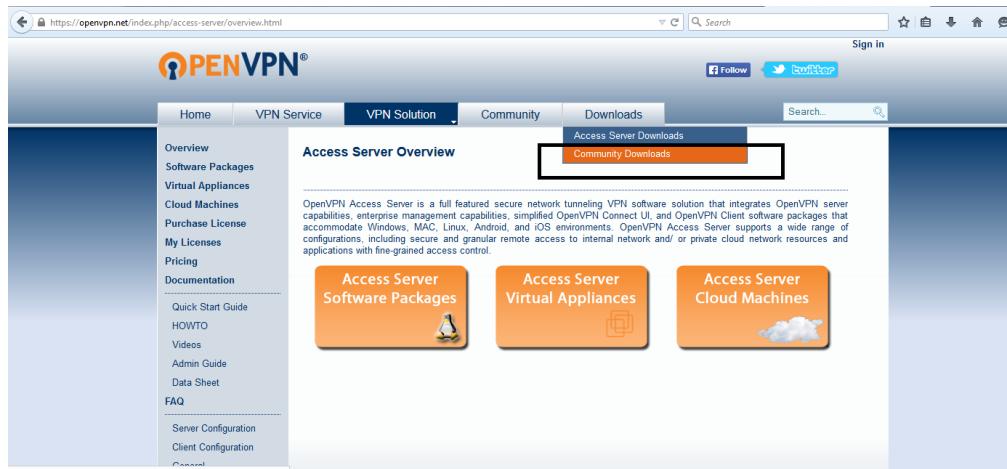
Example using the variables chosen above:

- c. On **Windows PC** (on administrator console), close 6in4 tunnel:
 - ii. netsh interface ipv6 delete address remote_user_tunn FD00::0A20:0483/128
 - iii. netsh interface ipv6 delete route ::/0 remote_user_tunn
 - iv. netsh interface ipv6 delete remote_user_tunn
- d. On **NMS**, remove route to Windows PC:
 - i. sudo ip route del FD00::0A20:0483/128 via :: 10.32.4.131

6.1.3 PC-to-device IPv6 communication for Linux user, VPN based

6.1.3.1 Install OpenVPN on Linux

1. Go to <https://openvpn.net/>, select ‘VPN Solution’ option and choose ‘Community Downloads’ tab option:



The screenshot shows the OpenVPN.net homepage. The top navigation bar has tabs for Home, VPN Service, VPN Solution (which is currently selected), Community, and Downloads. Below the navigation bar, there's a sub-navigation for 'Access Server Overview' with three orange buttons: 'Access Server Software Packages', 'Access Server Virtual Appliances', and 'Access Server Cloud Machines'. On the left, there's a sidebar with links like Overview, Software Packages, Virtual Appliances, Cloud Machines, Purchase License, My Licenses, Pricing, Documentation, and FAQ. The main content area contains text about OpenVPN Access Server and its features.

2. Download the release ‘*.tar.gz’ that suits user computer. For example, openvpn for 32-bit Linux computer:



The screenshot shows the 'Community Downloads' page for OpenVPN 2.3.6. It highlights a critical denial of service vulnerability (CVE-2014-8104) that can only be exploited by authenticated clients. It lists various download options for different platforms and architectures, each with a GnuPG Signature link. The page also includes instructions for verifying signatures and static URLs for automation.

Source Tarball (gpg)	File Name	GnuPG Signature
Source Tarball (xz)	openvpn-2.3.6.tar.xz	GnuPG Signature
Source Zip	openvpn-2.3.6.zip	GnuPG Signature
Installer (32-bit), Windows XP and later	openvpn-install-2.3.6-901-i686.exe	GnuPG Signature
Installer (64-bit), Windows XP and later	openvpn-install-2.3.6-901-x64.exe	GnuPG Signature
Installer (32-bit), Windows Vista and later	openvpn-install-2.3.6-901-i686.exe	GnuPG Signature
Installer (64-bit), Windows Vista and later	openvpn-install-2.3.6-901-x64.exe	GnuPG Signature

3. Compile and install it as follows:

- a. tar xfz openvpn-[version].tar.gz
- b. cd ‘top_level_directory’
- c. ./configure
- d. make
- e. make install

6.1.3.2 Setup Linux/NMS IPv4 communication VPN-based

1. Get the following certificates: **nms_ca.crt**, **nms_remote_user.crt**, **nms_remote_user.key** from the NMS administrator.
2. Create a configuration file “*.conf” with the following information (replace placeholders “<server_public_IPv4>” and “<server_port>” with the appropriate values):

```
client
dev tun1500
proto tcp
remote <server_public_IPv4> <server_port>
resolv-retry infinite
nobind
ca nms_ca.crt
cert nms_remote_user.crt
key nms_remote_user.key
comp-lzo
ns-cert-type server
verb 3
```

3. Start **as administrator** the OpenVPN
 - a. sudo openvpn [path_to_config_file]
4. Test the VPN connection:
 - a. Check if the interface with the assigned VPN ipv4 address <client_VPN_IPv4> was created:
 - i. ipconfig
 - ii. check in the command output shows and IPv4 in the range **10.185.0.0/24**
 - b. Check the VPN connection with server:
 - i. ping **10.185.0.1**

NOTE

Use 1194 for <server_port> variable

The NMS server is configured by default to provide to the clients the <client_VPN_IPv4> in the range **10.185.0.0/24**

The NMS server is configured with <server_VPN_IPv4>: **10.185.0.1**

6.1.3.3 Setup Linux/NMS IPv6 communication VPN-based

1. Prepare to connect to NMS from Windows PC:
 - a. Use **ipconfig** command to get the local VPN IPv4 address: <client_VPN_IPv4>, for example 10.185.0.38
 - b. The server (NMS) VPN IPv4 address <server_VPN_IPv4> is known, configured by default as: **10.185.0.1**
 - c. Compute the IPv6 address <client_VPN_IPv6> based on client VPN IPv4 address, using FD00 as prefix, and <client_VPN_IPv4> converted to hex as postfix. For example:
 - i. Computed IPv6: FD00::0AB9:0026
 1. FD00 is a MUST
 2. **0AB9:000E** is **10.185.0.38** converted to hex
2. Connect to NMS:
 - a. On **client Linux PC**: create 6in4 tunnel
 - i. sudo ip tunnel add remote_user_tunn mode sit local <client_VPN_IPv4> remote <server_VPN_IPv4>
 - ii. sudo ip addr add <client_VPN_IPv6>/128 dev remote_user_tunn
 - iii. sudo ip route add ::/0 dev remote_user_tunn
 - iv. sudo ip link set dev remote_user_tunn up
 - b. On **NMS**: create route to remote user machine
 - i. sudo ip route add <client_VPN_IPv6>/128 via ::<client_VPN_IPv4>

Example using the variables chosen above:

- b. On **client Linux PC** (on administrator console): create 6in4 tunnel
 - i. sudo ip tunnel add remote_user_tunn mode sit local 10.185.0.38 remote 10.185.0.1
 - ii. sudo ip addr add FD00::0AB9:0026/128 dev remote_user_tunn
 - iii. sudo ip route add ::/0 dev remote_user_tunn
 - iv. sudo ip link set dev remote_user_tunn up
- a. On **NMS**: create route to remote user machine
 - i. sudo ip route add FD00::0AB9:0026/128 via ::10.185.0.38

NOTE

All configurations are preserved if the OpenVPN Client is restarted

6.1.3.4 Test Linux PC/NMS IPv6 communication

1. Select an address of an already connected Edge Router or Smart Object as destination (ex. 2012:0:0:2::00fa:0162):
 - a. **ping6 2012:0:0:2::00fa:0162**

6.1.3.5 Cleaning up the remote access to NMS from Linux PC

In order to clean up the settings after the connectivity test was done, the following steps are necessary:

1. Disconnect from NMS:
 - a. On **client Linux PC**, close 6in4 tunnel:
 - i. sudo ip addr del <client_VPN_IPv6>/128 dev remote_user_tunn
 - ii. sudo ip route del ::/0 dev remote_user_tunn
 - iii. sudo ip tunnel del remote_user_tunn
 - b. On **NMS**, remove route to Windows PC:
 - i. sudo ip route del <client_VPN_IPv6>/128 via ::<client_VPN_IPv4>

Example using the variables chosen above:

- a. On **client Linux PC**, close 6in4 tunnel:
 - i. sudo ip addr del FD00::0AB9:0026/128 dev remote_user_tunn
 - ii. sudo ip route del ::/0 dev remote_user_tunn
 - iii. sudo ip tunnel del remote_user_tunn
 - b. On **NMS**, remove route to Windows PC:
 - i. sudo ip route del FD00::0AB9:0026/128 via ::10.185.0.38
-
2. Remove VPN certificates and key from the client Linux PC.

6.1.4 PC-to-device IPv6 communication for Linux user, non-VPN based

The non-VPN based connectivity will only work if the PC can communicate directly via IPv4 with the NMS (the NMS IPv4 is visible to the PC)

6.1.4.1 *Setup Linux/NMS IPv6 communication non-VPN-based*

1. Test IPv4 connection with NMS
 - a. On **NMS**, use **ifconfig** to get the remote(NMS) IPv4 address (<server_IPv4>), for example 10.32.4.233
 - b. On **Windows PC**, test the connectivity with NMS:
 - i. ping <server_IPv4>
2. Prepare to connect to NMS from remote user machine:
 - a. On PC client, use **ipconfig** command to get the local IPv4 address: <client_IPv4>, for example 10.32.4.17
 - b. Compute the IPv6 address <client_IPv6> based on client IPv4 address, using FD00 as prefix, and <client_IPv4> converted to hex as postfix. For example:
 - i. Computed IPv6: FD00::0A20:0411
 1. FD00 is a MUST
 2. **0A20:0483** is **10.32.4.17** converted to hex
3. Connect to NMS:
 - a. On **client Linux PC**: create 6in4 tunnel
 - i. sudo ip tunnel add remote_user_tunn mode sit local <client_IPv4> remote <server_IPv4>
 - ii. sudo ip addr add <client_IPv6>/128 dev remote_user_tunn
 - iii. sudo ip route add ::/0 dev remote_user_tunn
 - iv. sudo ip link set dev remote_user_tunn up
 - b. On **NMS**: create route to remote user machine
 - i. sudo ip route add <client_IPv6>/128 via ::<client_IPv4>

Example using the variables chosen above:

- a. On **client Linux PC** (on administrator console): create 6in4 tunnel
 - i. sudo ip tunnel add remote_user_tunn mode sit local 10.185.0.17 remote 10.185.0.1
 - ii. sudo ip addr add FD00::0A20:0411/128 dev remote_user_tunn
 - iii. sudo ip route add ::/0 dev remote_user_tunn
 - iv. sudo ip link set dev remote_user_tunn up
- b. On **NMS**: create route to remote user machine
 - i. sudo ip route add FD00::0A20:0411/128 via ::10.185.0.17

6.1.4.2 Test Windows PC/NMS IPv6 communication

1. Select an address of an already connected Edge Router or Smart Object as destination (ex. 2012:0:0:2::00fa:0162):
 - a. **ping6 2012:0:0:2::00fa:0162**

6.1.4.3 Cleaning up the remote access to NMS from Linux PC

1. Disconnect from NMS:
 - a. On **client Linux PC**, close 6in4 tunnel:
 - i. sudo ip addr del <client_VPN_IPv6>/128 dev remote_user_tunn
 - ii. sudo ip route del ::/0 dev remote_user_tunn
 - iii. sudo ip tunnel del remote_user_tunn
 - b. On **NMS**, remove route to Windows PC:
 - i. sudo ip route del <client_VPN_IPv6>/128 via ::<client_VPN_IPv4>

Example using the variables chosen above:

- c. On **client Linux PC**, close 6in4 tunnel:
 - iv. sudo ip addr del FD00::0A20:0411/128 dev remote_user_tunn
 - v. sudo ip route del ::/0 dev remote_user_tunn
 - vi. sudo ip tunnel del remote_user_tunn
- d. On **NMS**, remove route to Windows PC:
 - ii. sudo ip route del FD00::0A20:0411/128 via ::10.32.4.17

6.1.4.4 Cleaning up the remote access to Edge Router from Windows PC

In order to clean up the settings after the connectivity test was done, the following steps are necessary:

1. Disconnect from VR1000:
 - a. On **Windows PC** (on administrator console), close 6in4 tunnel:
 - i. netsh interface ipv6 delete address remote_user_tunn <client_VPN_IPv6>/128
 - ii. netsh interface ipv6 delete route ::/0 remote_user_tunn
 - iii. netsh interface ipv6 delete remote_user_tunn
 - b. On **VR1000**, remove route to Windows PC:
 - i. sudo ip route del <client_VPN_IPv6>/128 via ::<client_VPN_IPv4>

Example using the variables chosen above:

- e. On **Windows PC** (on administrator console), close 6in4 tunnel:
 - ii. netsh interface ipv6 delete address remote_user_tunn FD00::0AB9:000E/128
 - iii. netsh interface ipv6 delete route ::/0 remote_user_tunn
 - iv. netsh interface ipv6 delete remote_user_tunn
 - f. On **VR1000**, remove route to Windows PC:
 - v. sudo ip route del FD00::0AB9:000E/128 via ::10.185.0.14
-
2. Remove VPN certificates and key for remote user from path c:\Program Files\OpenVPN\config on Windows PC.

7 Troubleshooting

The following table represents some typical problems that may be encountered while working with the Smart Object Development Kit, the common cause of each problem, and some possible solutions.

Problem	Explanation	Solution
No device joins the network (not even Transceiver)	The Transceiver module present on the Edge Router is not connected properly to the antenna.	Ensure that the Transceiver is properly connected to the antenna.
No SO device joins the network, but Transceiver does join the network	The Net ID on the Smart Objects does not match the Vendor ID on the Edge Router.	Ensure consistency between SO Network ID and Quark Vendor ID (consistent with default settings).
Network slow to form, unstable after join	Smart Object or Transceiver on Edge Router has improperly connected antenna.	Make sure the antenna is properly connected.
With multiple coexisting networks, network slow to form, unstable after join	Overlapping networks with the same NetworkID/PanID	The NetworkID/PanID depends on the last byte of Edge Router IPv6.
Network unstable after connecting NAMT in Development Kit mode	Too aggressive interrogation rate	Reduce the number of devices or increase the interrogation interval (Settings→Development Kit Refresh interval).
NAMT in Development Kit mode slow to update after powering off a Smart Object	There is no unjoin notification; NAMT keeps requesting COAP resources from devices powered off.	Restart the Edge Router to rebuild the resource list.
Transceiver FW upgrade from NAMT fails at start, immediately after setting the time from NAMT	Did not wait a few minutes after setting the time from NAMT before connecting to the kit again.	Do not start the Transceiver firmware upgrade immediately after the Transceiver appears in the Network view; wait half a minute.
Inconsistent COAP resources shown after an Edge Router firmware upgrade	Smart Objects were not power cycled after Edge Router FW upgrade.	Restart all Smart Objects after Edge Router FW upgrade.
NAMT refuse to connect to Edge Router after setting time on Edge Router	The PC time changed significantly after setting the time on the Edge Router, resulting in time differences between PC and Quark, which lead to undefined network behavior.	Power cycle the whole system (Edge Router and Smart Objects).

Appendix A: List of Standards Supported in the Smart Object Platform

Standardization Body	Standard Designator	Revision	Title
IEEE	802.15.4g-2012	Final	Low-Rate Wireless Personal Area Networks (WPANs) Amendment 4: Physical Layer Specifications for Low Data Rate Wireless Smart Metering Utility Networks
IEEE	802.15.4e-2012	Final	Wireless Medium Access Control(MAC) and Physical Layer (PHY)Specifications for Low-Rate Wireless Personal Area Networks (WPANs)
IETF	RFC 2460	Final	Internet Protocol, Version 6 (IPv6)Specification
IETF	RFC 4443	Final	Internet Control Message Protocol for the IPv6 Specification
IETF	RFC 4944	Final	Transmission of IPv6 Packets over IEEE 802.15.4 Networks
IETF	RFC 6282	Final	Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks
IETF	RFC 6775	Final	Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)
IETF	RFC 6550	Final	RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks
IETF	RFC 6202	Final	The Trickle Algorithm
IETF	RFC 6552	Final	Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)
IETF	RFC 6551	Final	Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks
IETF	RFC768	Final	User Datagram Protocol (UDP)
IETF	ID.draft-ietf-core-coap	Rev 16	Constrained Application Protocol (CoAP)
IETF	RFC 6690	Final	Constrained RESTful Environments (CoRE) Link Format
IETF	ID.draft-ietf-core-observe	Rev 8	Observing Resources in CoAP
IETF	RFC 6347	Final	Datagram Transport Layer Security Version 1.2
IETF	RFC 5191	Final	Protocol for Carrying Authentication for Network Access (PANA)
IETF	RFC 3748	Final	Extensible Authentication Protocol (EAP)
IETF	RFC 5216	Final	EAP-TLS Authentication Protocol
IETF	RFC 5246	Final	Transport Layer Security (TLS) Protocol Version 1.2

Appendix B: FCC and Industry Canada Compliance Information

FCC Compliance

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.

NOTE: 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 or more 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.

NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT

This equipment complies with the FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of the human body.

This equipment must only be sold with an omni antenna that has 3.0 dbi or lesser gain.

Industry Canada Compliance

This device complies with Industry Canada licence-exempt RSS standard(s). Operation 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.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le

but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This equipment complies with the ICES RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of the human body.

Cet équipement est conforme aux limites d'exposition aux radiations ICES définies pour un environnement non contrôlé . Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et une partie de votre corps.