viprinet®

Viprinet Software

User´s guide

Imprint

As of 5/2016
Subject to technical changes.

Produced by:
Viprinet Europe GmbH
Gaustr. 22-32
55411 Bingen am Rhein
Germany
Phone: +49 (0)6721 4 90 30-0
Fax: +49 (0)6721 4 90 30-109
E-mail: info@viprinet.com
Web: www.viprinet.com

Preface. How to use this manual

This document is structured to be useful for experienced network administrators setting up or operating their first or hundredth Viprinet deployment, yet also to serve as an introduction suitable for IT staff who are not specialized in networking.

If this is your first Viprinet deployment, it is important that you read section 2.0 to ensure that you will understand the way these terms are used in this manual.

IT staff less experienced in networking should start by reading Chapters 1 and 2 before setting up and operating their deployment. This part introduces concepts relevant to the setup and operation of your network. Chapter 2, the introduction to parts of a Viprinet deployment, is also useful as a reference for experienced network administrators who are looking for the location of a specific menu item, because it provides a guide to the GUI of each Viprinet administration and monitoring utility.

Network administrators who have already worked with Viprinet products can start with Chapter 4, which walks the reader through the process of setting up and tweaking their Viprinet deployment. Chapter 6 is a guide to the configuration of tools particularly relevant to more complex needs and larger systems. Both of these guides presume that you are using a star topology as described in Chapter 1; this is not important for every set of instructions provided, but is worth keeping in mind.

Chapter 7 provides troubleshooting and support information. It is followed by a glossary, reference appendices, and a list of all tables and figures in this manual.

Material that is not labeled as specific to either classic firmware or RuggedVPN firmware is relevant to both.

Index

Chapter 1. An overview of networking concepts

The purpose of this section is to provide an overview of networking to IT staff and stakeholders not specialized in that area. This is especially relevant to personnel who may have to support a Viprinet deployment administered and deployed by networking professionals. It may also be useful to other stakeholders with limited knowledge of the subject.

1.0 How networks work

Here's an analogy for how a packet travels from its source (the sender) to its destination (the receiver).

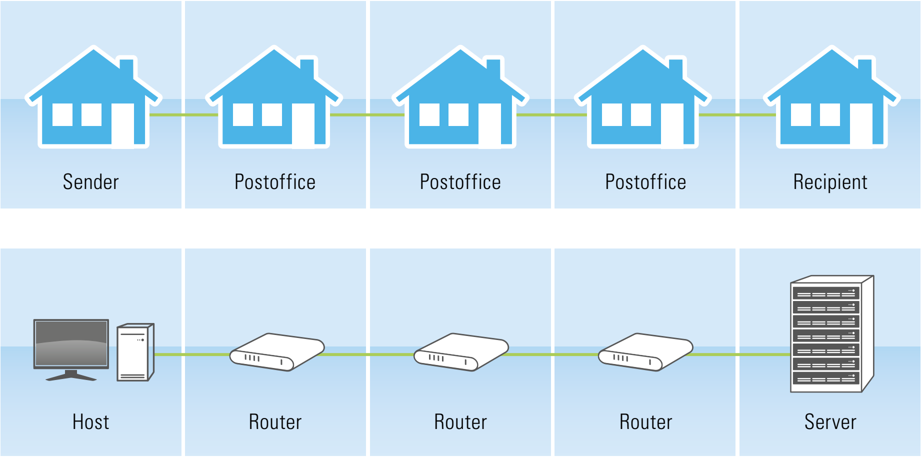


Figure 1.0 The postal analogy. Image 1 shows how mail moves from post office to post office. Image 2 shows how packets move from router to router. The sender is contacting a server. A local router sends the packet on to other routers, which pass it on to its destination.

Let's say you're sending a birthday card from San Francisco in the US to Bingen am Rhein in Germany. You write a message in the birthday card, then put it into an envelope. After checking your records for your friend's address, you copy it onto the envelope, along with your return address. Your neighborhood postal carrier takes the letter to your local post office. However, this is not a local letter, because it is going to Germany. So your post office can't just have one of their mail carriers deliver it. Instead, they send it on to a big central post office in Germany where the your friend's zip code is recognized. The central post office passes the letter on to the regional post office. The regional post office sends it on to Bingen am Rhein, and a mail carrier from the Bingen post office carries the card to your friend's street address.

Now imagine that you are trying to connect to an internet server with your computer. The packet that carries your data is equivalent to the envelope you put the card in, and the server's IP address is equivalent to the address. Your host's IP address is equivalent to your return address. You send the packet to the router that serves your LAN, which is like the local post office. This router has a record of the default path to send the packet. The router on the same network segment as the destination host sends the packet on to that host. This is just one very simplified routing path, but it will give you a basic idea of how networking works.

If your host has a private IP address, your local router or a gateway of your ISP does NAT (network address translation) to mask your private IP address with a public one that can be used on the internet without causing an addressing conflict. (An addressing conflict happens when two hosts use the same IP address and routers don't know where to send packets associated with that address).

This section gives you context for the rest of the explanations in this chapter. After you finish reading the rest of the chapter, you may wish to read this section again. You may also wish to review the glossary at this point. If you are interested in a more in-depth introduction to networking concepts after completing this chapter —an explanation of network layers, for example—the Viprinet Support department recommends that you consult this text:

Tanenbaum, Andrew S.,Wetherall, David J.
Computer Networks. 5th ed.
New Jersey: Prentice Hall, 2010.
ISBN-13: 9780132126953
http://computernetworks5e.org/blogs

1.1 Hosts and interfaces

IP addresses are associated with network interfaces. Multiple IP addresses and physical interfaces can be associated with the same router or other device.

In this manual, the term host can refer to either:

- a physical network card
- a device that contains a network card

The term interface can refer to:

- a physical network card fitted with a controller chip, connector, and drivers that allow it to be accessed with the user's OS
- a "port" or ethernet jack connected to the card
- the tool used to interact with a program or system, as in the term command line interface

The term "port" is not used to refer to hardware in this manual. Instead, it indicates a software construct. Ports are often associated with a protocol type. They are used to communicate with the host at a specific IP address in specific ways. 1024 well-known port numbers are associated with specific service types by convention. For example, port 443 is associated with secure HTTP (HTTPS) connections.

1.2 Public and private IP addresses

There are a limited number of public IP addresses in the world. At this point, there are no public IPv4 addresses left in most regions, so more and more IPv6 addresses are being used instead.
The use of private IP addresses is intended to conserve them by making it possible to re-use addresses on networks not

directly connected to the public internet. The Internet engineering task force designated three private ranges for this purpose: 192.168.0.0-192.168.255.255, 172.16.0.0-172.31.255.255, and 10.0.0.0-10.255.255.255. These IP addresses are no different technologically than public IP addresses, so their use is regulated only by general agreement.

1.3 Netmask

A netmask, also referred to as a network mask or a subnet mask, makes it possible to divide a network into segments. It indicates the number of addresses and the usable address range associated with a particular segment making it possible for networking hardware to identify that segment.

1.4 Segmentation

A LAN usually constitutes one network segment. A network segment can be an address range, a physical construct indicating which machines are physically or wirelessly connected to the same routers, or both. For more on segmentation, see 1.5.3 Basic principles of IP address allocation, applied to a star topology.

1.5 Network topologies, LANs, and WANs

Many consumer installations involve one host associated with a computer that has one network card which is associated with a private IP address and connected to a provider line via a home router or gateway, as in figure 1.1.

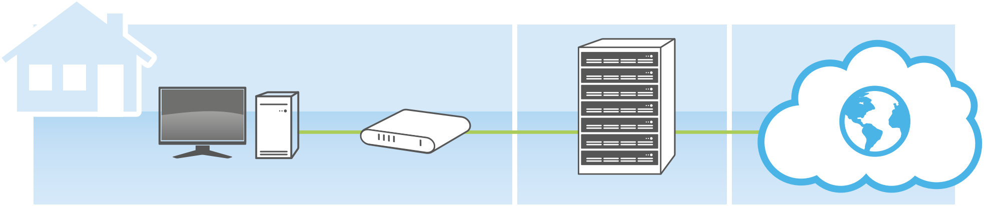


Figure 1.1 A typical consumer installation, displaying a PC, router, ISP datacenter, and connection to the internet.

Hosts in other settings are only directly connected to their local area network (LAN), and communicate through a router to other LANs and the internet.

1.5.0 LANs

A LAN is a local area network; for example, a particular department in a company may have its own LAN. Hosts on a LAN may be part of the same network segment and have the same netmask.

1.5.1 WANs

To connect one LAN to another or the internet, you use a wide area network (WAN). This is a term that can be applied to any network that spans geographic distances. A company network connecting branch locations that are physically distant from one another can be referred to as a WAN, but the internet is a WAN too.

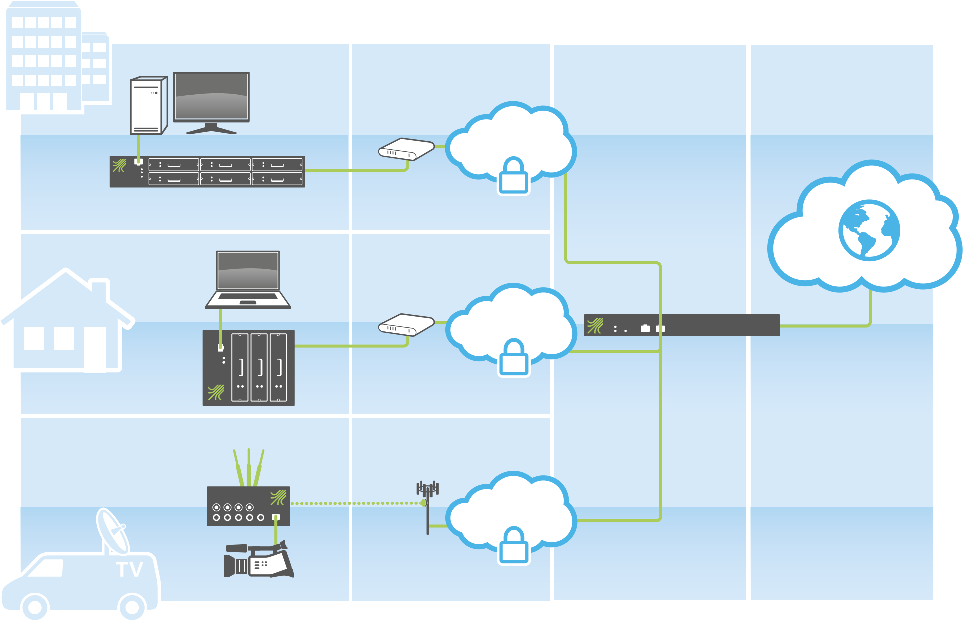


Figure 1.2 An example of a star topology.
This illustration depicts a Viprinet installation including multiple branch offices and an offsite mobile router, organized in a star topology. Nodes connect to ISPs with their modules. They use these connections to establish the Node end of the VPN tunnel, indicated by a cloud with a lock in the illustration. The Node establishes the VPN tunnel to the Hub, which connects it to the open internet.

1.5.2 Star topologies

A variety of network topologies exist. However, due to the nature of Viprinet's technology, our installations usually use a star topology, as pictured in figure 1.2. Viprinet networks are a good example of star topologies.

In Viprinet deployments, the routers directly associated with LANs are called Nodes, and the central routers that connect these Nodes to each other and the internet are called Hubs. See section 2.0 for more information about Hubs and Nodes and why both are used in Viprinet deployments.

Viprinet Nodes connect to Hubs through VPN tunnels. VPN means Virtual Private Network, and a VPN tunnel is an encrypted pathway between routers that does not expose them or the LANs associated with them directly to the open internet.

This section will cover two examples of star topologies commonly used in Viprinet deployments:

- Single branch office
- Multiple branch offices

Alternative topologies are possible, but should only be configured by experienced network administrators in consultation with Viprinet's Support department.
Example A: Single branch office
Hosts on an office LAN connect to a Node onsite. The Node connects to a Hub at a datacenter.
For this kind of simple small deployment, clients may wish to rent space on a Viprinet Hub from bonding service providers instead of purchasing and administering a Hub themselves.

Example B: Multiple branch offices
This setup is pictured in figure 1.2. All branch offices' VPN tunnels connect to the same Hub. The traffic between offices is routed through VPN tunnels to or from the Hub and never exposed to the open internet.

1.5.3 Basic principles of IP address allocation, applied to a star topology

Here is an example of how you can allocate IP addresses among multiple LANs. Table 1.0 and figure 1.3 illustrate the IP subnet you'd assign to each Node in the same sample network, assuming a IP network address of 10.0.0.0/8. Tables 1.0 and 1.1 give an example of how you might create IP address branches to assign unique private IP addresses to each of the devices on each of your LANs.

Branch 1	10.0.1.0/24 (254 addresses can be assigned within the range 10.0.1.0-10.0.1.255)
Branch 2	10.0.2.0/24
Branch 3	10.0.3.0/24
Branch 4	10.0.4.0/24

Table 1.0 Example: Assigning IP addresses; these are private IP addresses

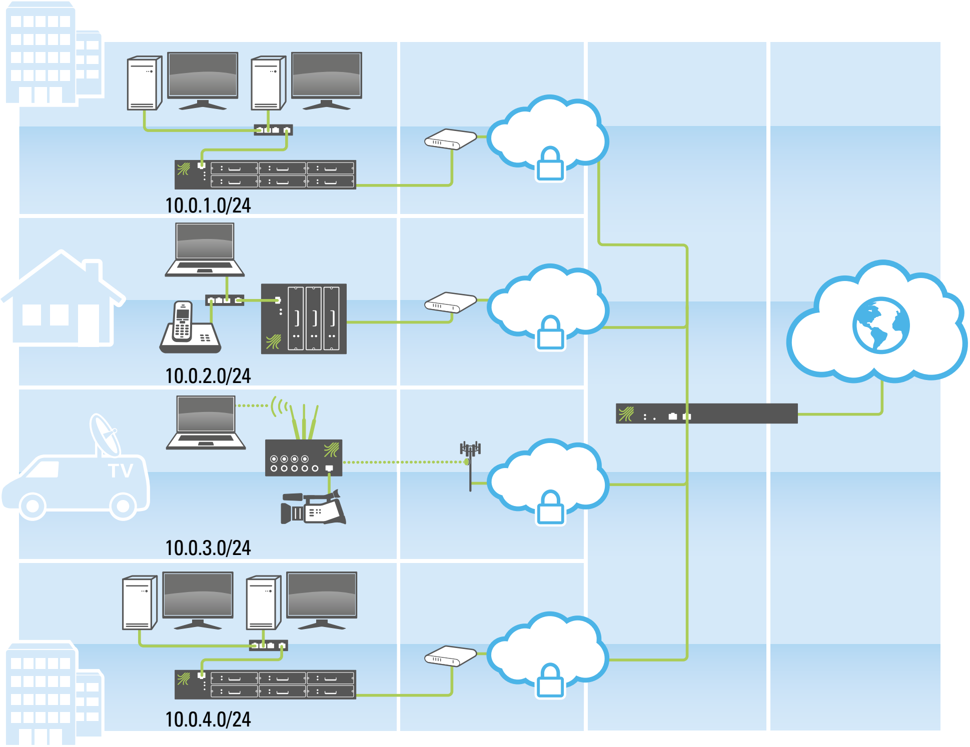


Figure 1.3 An illustration of LAN address assignments

	into two branches	into four branches	into eight branches
Branch 1	192.168.2.0/25	192.168.2.0/26	192.168.2.0/27
Branch 2	192.168.2.128/25	192.168.2.64/26	192.168.2.32/27
Branch 3		192.168.2.128/26	192.168.2.64/27
Branch 4		192.168.2.192/26	192.168.2.96/27
Branch 5			192.168.2.128/27
Branch 6			192.168.2.160/27
Branch 7			192.168.2.192/27
Branch 8			192.168.2.224/27

Table 1.1 Example: Assigning private IP addresses

1.5.4 Viprinet VPN Clients

Users offsite can connect into your network using a VPN Client. Viprinet VPN Client accounts are created on Hubs. Viprinet VPN Clients establish tunnels to the Hubs they are associated with. Viprinet VPN Client user IP addresses are dynamically assigned from a pool designed for Viprinet VPN Client use. This pool is in a separate address range from the rest of your network. You can remotely administer these users' routing and QoS settings. Consult section 5.1 and Appendix 7 for more information on installing, configuring, and using Viprinet VPN Client software and setups.

1.6 Advanced concepts: autotuning and bonding

1.6.0 Bonding

Bonding routers aggregate multiple lines, delivering a single connection that offers more bandwidth than any one of those lines could provide on its own. Bonding is not load balancing. Load balancing routers send packet streams over one of the multiple lines available to them, determining which line to use based on connection quality at the moment of transmission. They do not aggregate bandwidth. Two bonded 1 Mbit/s lines are the equivalent of a 2 Mbit/s line. Two load balanced Mbit/s lines are two 1 Mbit/s lines; traffic flows are sent over one or the other.

With Viprinet, it is possible to bond different networking media (e.g. DSL, 4G/LTE, cable) from multiple providers. One of the challenges of bonding different media and network services from a variety of providers is that each connection will have its own particular bandwidth and latency characteristics. In addition, the kinds of connections best suited to hosts' needs will vary depending on whether users are in a video conference, downloading files, or browsing websites. Autotuning and QoS settings make it possible to provide connections that offer consistent service tailored to specific requirements. For more on QoS settings, see sections 6.0, 5.1.4, 5.0.0.0, 5.0.0.3, and 5.1 (in order of relevance).

1.6.1 Bandwidth, latency, and congestion

Bandwidth is a measure of the capacity of a line in kbps (kilobits per second). Latency is a measure of the speed of a line between two hosts in ms (milliseconds). Factors that affect bandwidth include the physical properties of the medium being used and whether it is shared. Cable and all wireless connections are shared media. Factors that affect latency include packet loss, your distance from DSLAMs, antennas, or routers; the protocols you are using; the medium you are using (satellite tends to have higher latency values than DSL, for example); throttling and bandwidth-shaping by your ISP; and packet size (MTU).

If a host uses too much of the bandwidth available to it, latency rises as a result of network congestion. A traffic analogy can help you understand network congestion. Only a limited number of cars can fit on any given road. The more cars on the road, the more slowly all them will travel. When a lot of cars arrive at a traffic light (equivalent to a router or server for the purposes of this analogy) they queue up. When the light turns green, each of them will take more time to get through the intersection than they would have on an empty road, because they are waiting for the cars in front of them to move. Congestion happens when a host sends or receives enough packets simultaneously to saturate the available bandwidth. Only a limited number of packets can fit on any given line, and when they arrive at routers or servers they must wait in a queue to be processed. The more packets there are on the line, the longer the queue becomes, and the more slowly all of those packets will be transmitted.

Congestion-related latency may be exaggerated when an ISP responds to heavy use of its line by reducing the amount of bandwidth available to the host. Providers control access to their bandwidth with throttling and traffic shaping in order to ensure that each host on their networks only uses the explicit or implicit quota allocated to it.

Using only 90-99% of the available bandwidth will help to keep latency values low for all types of connections. Congestion algorithms (see Appendix 10) and autotuning can help you get more bandwidth out of a line than you otherwise could without increasing latency.

A line's bandwidth delay product is a measure in bits (or bytes) of the maximum amount of data that can be carried on that network circuit at any given time, having been sent but not yet acknowledged. To calculate this value, multiply bandwidth (in kbps) by round-trip delay time (in seconds). Long high-speed lines tend to have a high bandwidth-delay product.

1.6.2 Autotuning

Autotuning programs run network diagnostics to determine what settings are best for your situation so you do not have to figure out what bandwidth and latency values to enter. They either run speed tests on the line to find the bandwidth utilization level at which latency rises, or use normal traffic to determine its capacity and latency ranges.

See more on this in section 6.1.

Chapter 2. The components of a Viprinet deployment

In this chapter, as in the rest of this manual, material that is not labeled as specific to either classic firmware or RuggedVPN firmware is relevant to both.

2.0 Hubs and Nodes

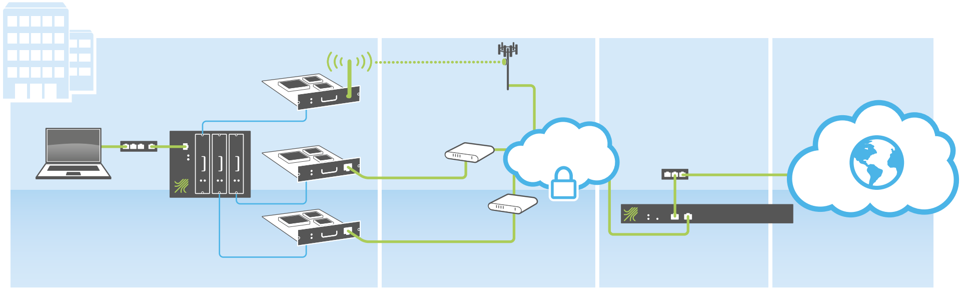


Figure 2.0 A typical Viprinet network

At least two routers, a Node and a Hub, are needed in every Viprinet deployment. Each is specialized for its function.

Viprinet Nodes and Hubs are all connected to each other through VPN tunnels. A VPN tunnel is an encrypted pathway between routers that does not expose them or the LANs associated with them directly to the open internet.

How packets travel from hosts to the internet

The Node establishes a VPN tunnel with the Hub. Hosts send packets upstream to the Node that routes traffic through their LAN. The Node fragments and encrypts these packets (and if relevant features are activated, compresses them), then transmits this traffic to the Hub over an appropriately aggregated set of channels in the tunnel. The Hub decrypts and reintegrates this traffic coming from the Node and transmits it to the open internet or other Nodes in the deployment. Incoming packets generally follow the same path in the opposite direction.

The primary differences between Hubs and Nodes are:

- applicable software licenses
- bonding capacity (Hubs frequently have more)

- which configuration items are available
- whether their chassis are designed to accept modules
- Hubs route traffic between tunnels rather than just connecting to a single one

2.0.0 Hubs

Hubs are Viprinet routers, which receive the incoming VPN connections from Viprinet Nodes.

Hubs do not contain hot-plug module slots. They only use wired connections, and should be plugged into two of them, preferably at a datacenter. Hubs installed onsite at your organization's premises may only be able to access lower-speed connections and might not have access to power and connection redundancies available at properly-run datacenters.

In most Viprinet deployments, Hubs sit at the center of the network topology. Two public IP addresses should be set aside for every Hub.

Things to remember about Hubs

- Hub channels are enabled by default because they just listen for incoming connections, which does not consume bandwidth unless they are receiving data
- Viprinet VPN Client users establish their connections through Hubs

Different models of Hub are distinguished from one another by their capacity. They cannot be stacked the way Nodes can, but they can be put into redundancy groups. See section 6.4 for more on Hub redundancy.

The LAN interface on Hubs is labeled Uplink and the WAN interface is labeled WAN/VPN.

The LEDs on Hubs' LAN and WAN interfaces have three states:

- Off: No link established
- Green LED lit: 100 Mbit/s link established
- Green and orange LEDs lit: 1000 Mbit/s link established

The Hub status LED also has three states:

- Off: No incoming or established VPN connections
- Flashing: a Node is establishing an incoming tunnel connection
- Lit: a VPN tunnel has been established with a Node

2.0.0.0 Additional support documents

- http://www.viprinet.com/hubs
- http://www.viprinet.com/factsheets
- Product folders: http://www.viprinet.com/productfolder

2.0.1 Nodes

Nodes cannot be used on their own, because they are unable to establish a VPN tunnel without having a Hub to connect to. Hubs are also needed to decode the encrypted packet streams that Nodes send, and reassemble and reorder packets that have been sent over multiple channels in a tunnel. Each Node that connects to a Hub establishes its own

VPN tunnel, unless you are using stacking. In that case, you can create on virtual Node based on multiple Viprinet router hardware appliances.

Most Nodes contain hot-plug module slots. These modules are associated with the channels that make up the VPN tunnel (see section 2.2 and figure 2.1 for a more in-depth description of channels). Channels are disabled by default on Nodes, because sending data can incur data fees. When you want to set up spare Nodes to take over for each other in case of failure, or increase the capacity of a particular part of your network, you enable Node stacking (see section 6.9). Mobile Nodes contain non-hot-plug 3G or 4G modules that are fixed in place.

Different models of Node are distinguished from one another by bonding capacity how many hot-plug modules they can support and which price points and deployment scenarios they're most appropriate for. There are models optimized for both wired and wireless use, although all modular Nodes can take modules for either wired or wireless connections.

The 500 and 51X series are engineered for mobile use. Their modules are fixed in place and primarily connect to mobile data services, using up to four SIM cards inserted in slots that can be accessed by removing a panel on the top of the router. Each module or SIM card, like modules in other Nodes, corresponds to a channel in the VPN tunnel. These models also have a built-in gigabit ethernet interface that can connect to any type of external modem. In addition to other hardware common to all Nodes, the 51X also have sockets for antennas and LEDs to indicate the state of each mobile connection.

All Nodes have power and connection indicator LEDs and an Ethernet LAN interface. An additional Gigabit Ethernet WAN interface is available in 200 and 5xx series routers.

The antenna socket LEDs for mobile Nodes have three states:

- Off: modem deactivated or no SIM card inserted
- Blinking: connecting to network
- Lit: connected to network

The LAN interface LEDs for all Nodes have three states:

- Off: no cable attached; cable defective
- Flashing: data is passing through the line
- Lit: cable is correctly connected

The *Online* LEDs for all Nodes have three states:

- Off: No outgoing or established VPN connections
- Blinking: Tunnel is enabled, at least one channel is enabled and one module is up; trying to establish the tunnel
- Lit: A tunnel is established

2.0.1.0 Additional support documents

- http://www.viprinet.com/router-modular
- http://www.viprinet.com/router-mobile
- http://www.viprinet.com/reception-solutions
- Datasheets for each Node type, available at: http://www.viprinet.com/factsheets
- Product folders: http://www.viprinet.com/productfolder

2.1 Modules

Hot-plug modules can be removed or installed while the Node is running, hence their name. They enable your Node to connect to wired or wireless provider networks. Each module used corresponds to one of the channels that make up the VPN tunnel between the Node and the Hub. See figure 2.0 for more information. Module slots are numbered from the upper left-hand to the bottom right-hand corner of the Node. Labels on the top right of the modules' faceplates indicate their model numbers and the medium they support.
Each module must be configured individually. After the setup tool has been run on a Node containing a given type of module, modules of that same type can be substituted without any reconfiguration, provided that they are installed in the same slot. If you put a module of one type in a slot previously used for another type, the new module must be configured in the AdminDesk, even if it has already been used in another router. Module configuration settings are stored in the Node, not on the module.

Each module has two indicator LEDs on its face, labeled Link and Online.

The *Link* LED displays three states:

- Lit: cable is properly seated or modem has connected to the wireless network
- Flickering: data is passing through the line
- Flashing: ADSL only; module is trying to synchronize with the DSLAM

The *Online* LED displays two states:

- Blinking: Trying to obtain configuration information, for example obtaining an IP address or getting a DHCP answer. If the module has not been configured properly, a channel cannot be established, but the router will still try to connect
- Lit: An IP address has been obtained

As of this writing, Viprinet offers eight types of hot-plug module:

Module type	Used for
ADSL2+ Annex A	All types of analog phone line DSL except SDSL, Annex 2, and SHDSL (no external modem needed)
ADSL2+ Annex B	All types of DSL except SDSL, Annex 2, and SHDSL (no external modem needed)
VDSL 2 / ADSL2+, and VDSL 2 / ADSL2+ for dual line setups	Carrier Sets (Ghz): I43, V43, A43, B43, J43 Annex A/B/J/L/M, ADSL1/2/2+ VDSL1 VDSL2 8A, 8B, 8C, 8D, 12A, 12B,17A, 30A
802.11 b/g/n WiFi Client	2.4 ghz, IEEE 802.11 b/g/n
4G Europe II	All current mobile phone technologies, Europe frequencies only
Gigabit Ethernet	External modems
LTE/DC-HSPA+/EDGE/GPS *will be replaced by 4G Europe/Australia and 4G Americas by 2016*	Europe: All current mobile connection types. US and Australia: Specialized versions of this model are available to accommodate LTE bands in these countries. Both: Location of the Node (GPS tracking). 4G is downward compatible with 3G connections.
LTE/UMTS/HSPA+/GPRS/EDGE *will be replaced by 4G Europe/Australia and 4G Americas by 2016*	Europe: All current mobile connection types. US and Australia: Specialized versions of this model are available to accommodate LTE bands in these countries. 4G is downward compatible with 3G connections.

Module type	Used for
UMTS/HSPA+/GPRS/EDGE *will be replaced by 4G modules, which are backwards compatible*	Connection types listed.
CDMA 450	Northern and Eastern Europe
CDMA/EV-DO	United States
LTE 450	Northern and Eastern Europe; only supports RuggedVPN firmware

Table 2.2 Types of module

As technology changes, new modules are being developed. Consult the Viprinet website for the most current list of modules available.

2.1.0 Additional support documents

- http://www.viprinet.com/hot-plug-modules
- http://www.viprinet.com/reception-solutions
- Datasheets for each module type, available at: http://www.viprinet.com/factsheets
- Product folders: http://www.viprinet.com/productfolder

2.2 Channels and tunnels

The VPN tunnels that connect Nodes to Hubs in your Viprinet deployment are composed of channels. A channel is the name for a SSL-encrypted TCP connection between a module slot in a Node and the WAN interface of a Hub.

- Each active hot-plug module in your Node corresponds to a channel
- The Hub bonds the channels together to establish the VPN tunnel
- Every channel in every VPN tunnel connected to a given router can be viewed in the device's AdminDesk interface

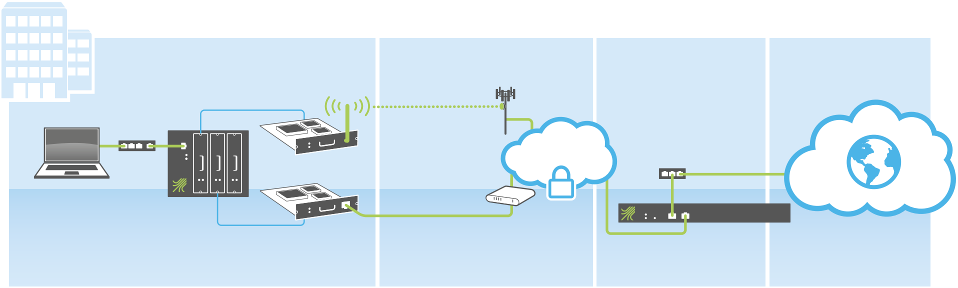


Figure 2.1 An exploded diagram of two modules in a Node, the top connecting to a wireless medium and the bottom to a wired medium. These two different channels are bonded by the Hub into a single VPN tunnel (the cloud with the lock) and connect to the Hub via its WAN interface. Each Node associated with a Hub has its own VPN tunnel.

2.2.0 Channels vs module slots

Although channels and module slots are associated with each other, channels are logical constructs and modules are physical ones. Different settings can be modified in the menus associated with each—see sections 2.5.1.5.0 and 2.5.1.5.2. One set of QoS rules governs all of the traffic that passes through the tunnel. Another handles VPN Client user traffic

For more on customizing QoS and autotuning settings, see sections 6.0 and 6.1.

2.3 Assigning IP addresses in a Viprinet deployment

You will need one static IP subnet for every Node on your network, and ideally two static public IP addresses for every Hub. In this context, static means set manually rather than assigned by DHCP. Nodes need to be in the same network segment as each of the LANs; this can be accomplished with LAN IP address aliases (see section 5.3).   Usually module IP addresses are dynamic and assigned by the relevant service providers.

All hosts in your LAN can generally use private IP addresses. If you wish to include servers with public IP addresses in your LAN, you will need to request a block of public IP addresses from your bonding service provider. When your BSP assigns these, they will be routed to the Hub that LAN is associated with. All IP address ranges that should be used in the LAN behind the Node must be routed from the Hub and through the tunnel to the Node. From there they can be assigned by a DHCP Server, or static IP addresses can be set. Either you can set up NAT on your Hub or receive NAT service from your BSP. See section 5.3, on routing rules, for details.

The Hub does NAT for the LANs it is connected to. Frequently its LAN IP address is used *as the IP address to mask with.*

Connections outside the LAN, including to other LANs within your organization, must be made through the Hub, except in special circumstances; consult Support for more information. See figure 2.2 for an illustration of routing between Nodes and from Nodes to the internet.

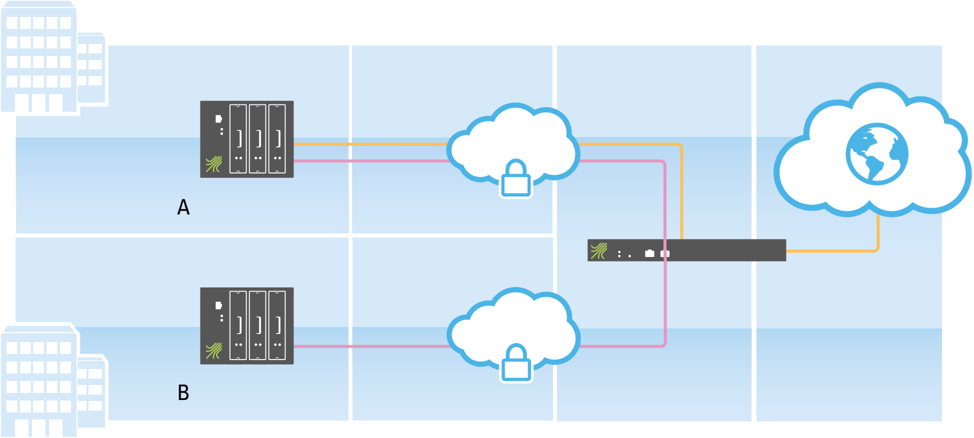


Figure 2.2 Routing paths. The orange route connects the LAN in branch office A to the internet. The pink route connects branch offices B and A.

2.4 SSL certificates and Node->Hub connections in the AdminDesk

One SSL certificate is associated with each Viprinet router's AdminDesk and LAN interface. By default, this certificate is automatically created during the initial configuration of the router.

Nodes use the tunnel certificate to identify the Hub they are connecting to. Hubs identify Nodes with the tunnel name and password associated with them. If you enter a new SSL fingerprint on a Hub or reset the Hub, you will also need to update the *Remote router's SSL certificate fingerprint* on every Node that is already connected to this Hub.

If you access the router using the http protocol rather than https while using a browser that supports the recent version of the AdminDesk, a security warning will pop up that suggests you permit the system to automatically redirect you to the https version.

If your browser accepts automatically generated certificates and you are not connecting on port 80, click *Ok* to proceed to the SSL-encrypted version.

A good solution if you prefer to access the AdminDesk via an SSL-protected connection and your browser does not like automatically-generated certificates is to un-tick the *Automatically generate self-signed SSL certificate box in the Integrated Services > AdminDesk Service* settings, and apply a fingerprint associated with a certificate that you have externally generated instead.

Attention
If you change the SSL certificate fingerprint for the AdminDesk, you will lose access to the SSL version of the AdminDesk for at least ten minutes. Make sure that your ACLs allow access to the AdminDesk via HTTP, at least while you are making this adjustment.

2.5 The AdminDesk

After you have used the setup tool (see sections 4.0.7 through 4.0.9 and 4.1) to configure your Node or Hub, you will be able to administer it through the browser-based AdminDesk interface.

To access the AdminDesk for your Node or Hub:

- Make sure the Node or Hub is connected to the LAN your computer is using
  - If your router has a public IP address, you should be able to reach it from anywhere
- Enter the router's IP address into your browser's address bar

Attention
If you bookmark your router's AdminDesk in your browser after logging in, you must make sure that only the IP address and port forward for the router are included in the bookmark URL. If /exec is included you will not be able to access the router with this bookmark.

2.5.0 CLI and text browser access

The current version of the AdminDesk requires that Javascript be activated in your browser. If you prefer not to use or cannot use this feature, use the legacy interface on the router landing page. You will not be able to access all menus and options in legacy mode; see table 2.3 for details.

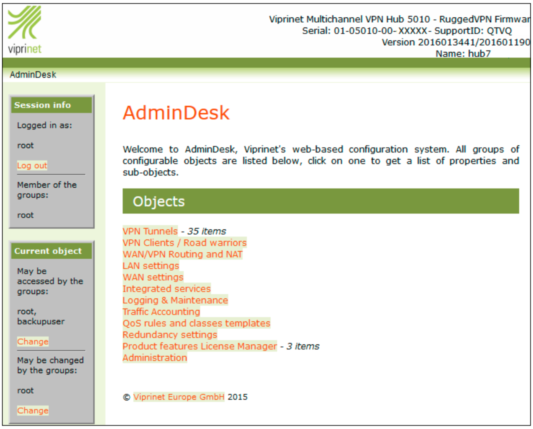
Utilities	Legacy	CLI
Ping tool	✓	✓
Traceroute tool	✓	✓
Download tool	✓	
Configuration backup/restore	✓	
Connectivity diagnostics	✓	
Module Info	✓	✓
ARP tool	✓	✓
DSL modulation tool (ADSL only)	✓	✓
AT command tool	✓	✓
AccessPoint info	✓	✓
Logwatcher	✓	
QoS backup	✓	
Heartbeat-map	✓	✓
Offline update	✓	
DHCP leases tool	✓	✓
Traffic accounting tool	✓	
Google Maps Geolocation		

Table 2.3 CLI and legacy AdminDesk

Although the AdminDesk can be viewed with text browsers, such as lynx, only the legacy version is accessible, and users will not be able to configure certain options from this interface; see table 2.3. It is preferable to use the command line interface (CLI), which is missing fewer options; it is primarily intended for scripting.

To activate CLI access, tick the Enabled box in the *SSH CLI Service settings* menu associated with the Integrated services item in the AdminDesk menu tree. You can do this on either the up-to-date or legacy GUI (see section 2.5.1 for more information on the AdminDesk GUI). Also make sure that ACLs for the CLI are correctly set to allow access. Every user in the *Administration* group can now log in on port 22 using any SSH client. Public keys can be stored on this router as a more secure login option.

The command prompt you see when you log in will match the serial number of the router you are accessing. You can get a list with explanations of all commands by entering *help*. Standard Linux shell navigation commands such as cd and ls are present. Tab auto-complete is enabled. You will be automatically logged out after 120s of inactivity.



Viprinet Multichannel VPN Hub 5010 - RuggedVPN Firmwar
Serial: 01-05010-00- XXXXX- SupportID: QTVQ
Version 2016013441/201601190
Name: hub7

AdminDesk

Session info

Logged in as:

root

Log out

Member of the groups:

root

Current object

May be accessed by the groups:

root, backupuser

Change

May be changed by the groups:

root

Change

AdminDesk

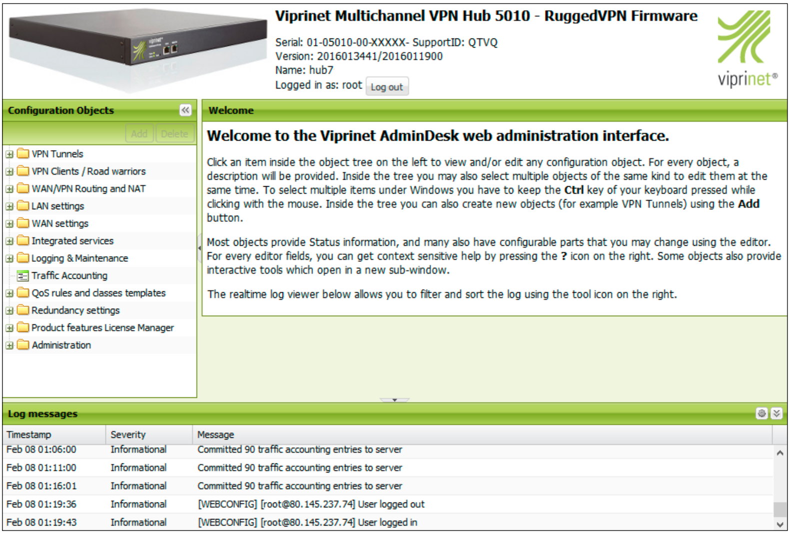
Welcome to AdminDesk, Viprinet's web-based configuration system. All groups of configurable objects are listed below, click on one to get a list of properties and sub-objects.

Objects

- VPN Tunnels - *35 items*
- VPN Clients / Road warriors
- WAN/VPN Routing and NAT
- LAN settings
- WAN settings
- Integrated services
- Logging & Maintenance
- Traffic Accounting
- QoS rules and classes templates
- Redundancy settings
- Product features License Manager - *3 items*
- Administration

© Viprinet Europe GmbH 2015

Figure 2.3 The legacy version of the AdminDesk



Viprinet Multichannel VPN Hub 5010 - RuggedVPN Firmware

Serial: 01-05010-00-XXXXX- SupportID: QTVQ
Version: 2016013441/2016011900
Name: hub7
Logged in as: root Log out

Welcome to the Viprinet AdminDesk web administration interface.

Click an item inside the object tree on the left to view and/or edit any configuration object. For every object, a description will be provided. Inside the tree you may also select multiple objects of the same kind to edit them at the same time. To select multiple items under Windows you have to keep the **Ctrl** key of your keyboard pressed while clicking with the mouse. Inside the tree you can also create new objects (for example VPN Tunnels) using the **Add** button.

Most objects provide Status information, and many also have configurable parts that you may change using the editor. For every editor fields, you can get context sensitive help by pressing the **?** icon on the right. Some objects also provide interactive tools which open in a new sub-window.

The realtime log viewer below allows you to filter and sort the log using the tool icon on the right.

Log messages

Timestamp	Severity	Message
Feb 08 01:06:00	Informational	Committed 90 traffic accounting entries to server
Feb 08 01:11:00	Informational	Committed 90 traffic accounting entries to server
Feb 08 01:16:01	Informational	Committed 90 traffic accounting entries to server
Feb 08 01:19:36	Informational	[WEBCONFIG] [root@80.145.237.74] User logged out
Feb 08 01:19:43	Informational	[WEBCONFIG] [root@80.145.237.74] User logged in

Figure 2.4 The modern AdminDesk

The most up-to-date version of the AdminDesk interface is divided into four resizable frames:

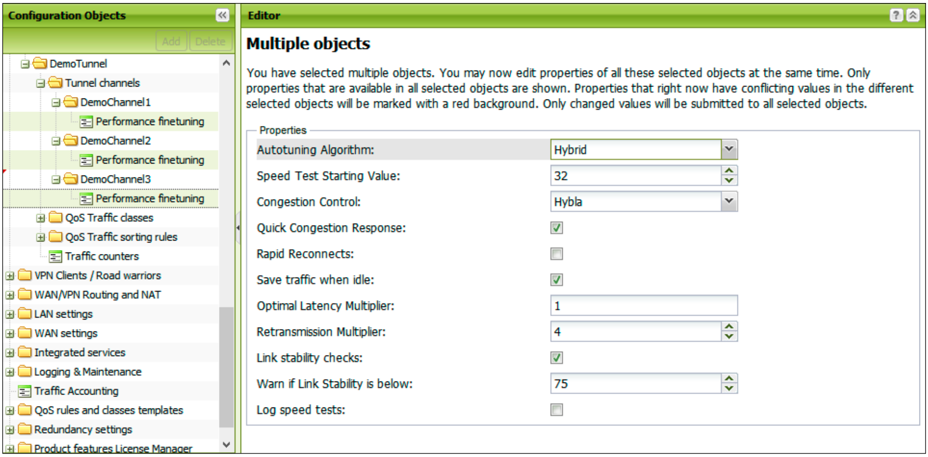
- Top: Vital statistics (basic model and firmware information)
- Left: Configuration menu tree (“Configuration Objects”)
- Right: Main Control window; this is where you enter your settings
- Bottom: Status log (“log messages”)

2.5.1 GUI Anatomy and components

This section provides an overview of the AdminDesk GUI.

2.5.1.0 General principles

- In order to access all of the AdminDesk's features, you need a browser released within the past five years that has Javascript enabled.
- Click directories in the menu tree to view and edit associated parameters. Expand directories with the plus signs to their left. Modified configuration fields will be highlighted until you click Apply. The buttons that allow you to add and delete items, such as VPN tunnels or QoS rules, appear above the configuration menu tree. The Control windows of several top-level menus, such as VPN Tunnels, include matrices listing information about their sub-items.
- When you click each top-level menu, a brief explanation of its functions appears in this pane. Click within configuration entry fields to view balloon help about the values you can enter there. To make balloons disappear, click outside of the field.
- Where a Change button appears, click on it to change settings, not the field associated with it. To edit multiple menu tree items of the same type at the same time (e.g. two LAN IP address aliases), hold down your shift or control key, then click each of them.
- Resize the menu tree and status log with the double arrows at their top right-hand corners. Expand or narrow them with the small black arrows at their edges. Resize matrix columns by clicking and moving the gray border dividing them. To filter and sort log messages click the gear on the right.
- A red mark will appear in the upper right corner of the menu item for a module that is disabled.
- Menus do not appear to user groups without the appropriate permissions. It is evident when a user does not have permissions to view a particular menu when the error message "This menu was not accessed, but the router also did not specify an error" appears.
- Every aspect of router operations that is only determined during the VPN Tunnel connection handshake needs a reconnect for changes to take effect—enabling/disabling encryption, changing tunnel password, changing any name. Other things like Max Bandwidth and latency settings take effect immediately. Channel fine tuning settings take effect immediately.



Multiple objects

You have selected multiple objects. You may now edit properties of all these selected objects at the same time. Only properties that are available in all selected objects are shown. Properties that right now have conflicting values in the different selected objects will be marked with a red background. Only changed values will be submitted to all selected objects.

Properties

Autotuning Algorithm: Hybrid

Speed Test Starting Value: 32

Congestion Control: Hybla

Quick Congestion Response: ☑

Rapid Reconnects: ☐

Save traffic when idle: ☑

Optimal Latency Multiplier: 1

Retransmission Multiplier: 4

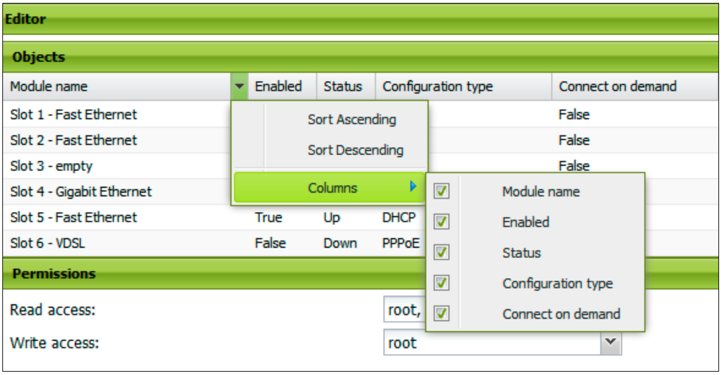
Link stability checks: ☑

Warn if Link Stability is below: 75

Log speed tests: ☐

Figure 2.5 Making multiple selections

2.5.1.1 Sorting and searching matrices



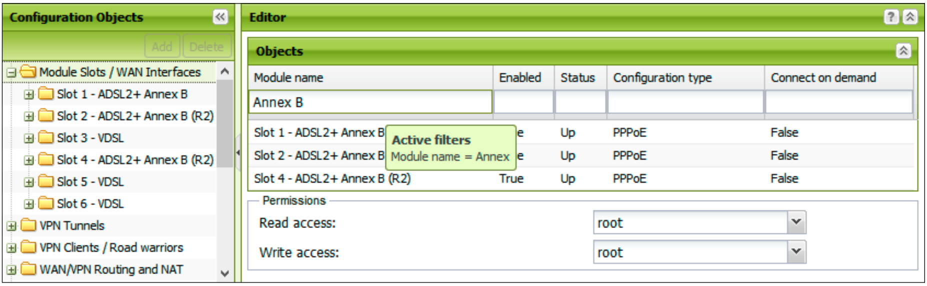
Module name	Enabled	Status	Configuration type	Connect on demand
Slot 1 - Fast Ethernet				False
Slot 2 - Fast Ethernet				False
Slot 3 - empty				False
Slot 4 - Gigabit Ethernet				
Slot 5 - Fast Ethernet	True	Up	DHCP	
Slot 6 - VDSL	False	Down	PPPoE	

Read access: root,

Write access: root

Figure 2.6 Sorting matrices in the classic firmware

In the classic firmware, you can sort and modify display settings for columns.



Module name	Enabled	Status	Configuration type	Connect on demand
Annex B				
Slot 1 - ADSL2+ Annex B	e	Up	PPPoE	False
Slot 2 - ADSL2+ Annex B	e	Up	PPPoE	False
Slot 4 - ADSL2+ Annex B (R2)	True	Up	PPPoE	False

Read access: root

Write access: root

Figure 2.7 Sorting and searching matrices in RuggedVPN

In the new firmware, you can also search within matrices easily.

2.5.1.2 Vital statistics bar

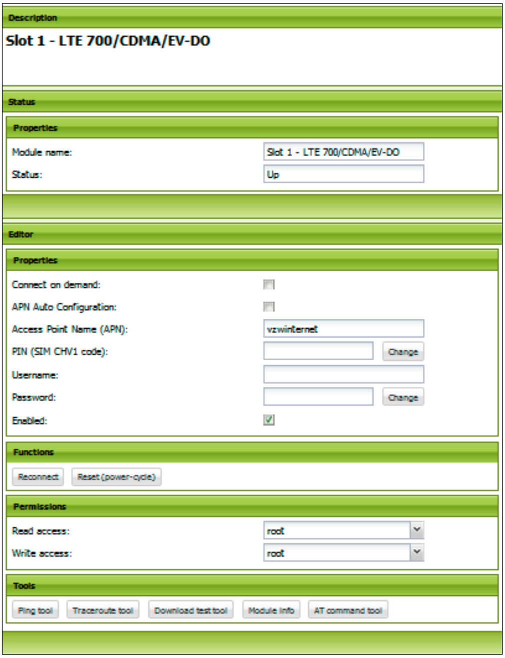
This part of the tool lists all the basic information about your Node or Hub, including:

- Model #
- Serial #
- Firmware version
- Name
- Username of the logged-in user
- SupportID

It is also where the logout button is.

2.5.1.3 Control window

When you select items from the configuration menu tree, the fields you can modify appear in this frame.



Description

Slot 1 - LTE 700/CDMA/EV-DO

Status

Properties

Module name: Slot 1 - LTE 700/CDMA/EV-DO

Status: Up

Editor

Properties

Connect on demand: □

APN Auto Configuration: □

Access Point Name (APN): vzwinternet

PIN (SIM CHV1 code): [Change]

Username:

Password: [Change]

Enabled: ☑

Functions

[Reconnect] [Reset (power-cycle)]

Permissions

Read access: root

Write access: root

Tools

[Ping tool] [Traceroute tool] [Download test tool] [Module info] [AT command tool]

Figure 2.8 A sample Control Window menu

The control window contains a variety of panes that vary based on the item:

- Description
  - This pane is always present. It explains what the configuration menu item you have selected is for
- Status
  - For read-only values that are automatically updated by the router
  - Indicates data that is subject to change; with GEO Tracking it refers to location
- Editor
  - Items you modify to change the Node or Hub settings appear here
  - Revert and Apply buttons appear in this section. Revert allows you to change settings back to their defaults. Apply allows you to apply setting changes.
- Properties
  - Often multiple panes
  - Usually appears within the Editor pane
  - You enter most of your settings here
- Functions
  - This pane does not appear in all menus
  - It includes buttons that allow you to do things to the router, such as reboot it
- Tools
  - This pane does not appear in all menus
  - Buttons that allow you to use tools specifically relevant to the menu you are viewing appear here

- Permissions
    - Appears at the bottom of all menus
    - Allows you to set which groups are allowed to view and edit the settings in the menu you are viewing

2.5.1.4 Status log

This frame displays activity notices for your Node or Hub.
To search within the status log, click the gear symbol to the left of the expansion arrows at the top of the log frame.
You can search by time stamp, by severity, or by the text of the log entry message
Once you've entered what you are searching for, click *Show as text* to see the results
You can also filter the log window by clicking *Apply Filters*; to remove them click *Clear Filters.*

2.5.1.5 Configuration menu tree

Select the directories in this frame or their sub-items to access their properties in the control window.

Certain features are only accessible if you purchase licenses for the relevant add-ons (see the list in Appendix 6; related menus can be viewed in sections 2.5.1.5.0 through 2.5.1.5.2). Licenses are bound to the serial number of the device they have been installed on.

The order of items in the menu tree is as follows, including all top-level menus and first-level submenus:

- (Nodes only) Module slots/WAN interfaces
    - Modules
        - Module submenus
- VPN Tunnels
    - Tunnels
        - Tunnel channels
        - QoS traffic classes
        - QoS traffic sorting rules
        - (if Streaming Optimization add-on enabled) Receive dejitter buffer fine-tuning
- VPN Clients/Road warriors
    - VPN Client users
    - QoS Traffic classes
    - QoS Traffic sorting rules
    - Client's Routing and DNS settings
    - (if Hub Segmentation add-on enabled) Segmented VPN Clients
- WAN/VPN Routing and NAT
    - WAN/VPN routing rules
    - Masquerading (outbound NAT) Entries
    - Port forwarding entries
- LAN settings
    - LAN IP address aliases
    - Additional LAN Routes
    - Ethernet speed and auto-negotiation settings
- (Hubs only) WAN settings
    - WAN/VPN routing rules
    - Masquerading (outbound NAT) entries
    - Port forwarding entries

- Integrated services
    - AdminDesk service settings
    - SNMP settings
    - DNS service settings
    - NTP service settings
    - SSH CLI service settings
- Logging and maintenance
    - Router Health
    - Router Firmware Update
    - (if traffic accounting server add-on enabled) Traffic accounting
- QoS rules and classes templates
    - QoS traffic classes
        - Individual classes
    - QoS traffic sorting rules
        - Individual rules
- (Nodes with add-on only) Stacking
    - Stacked routers
    - LAN IP address aliases
    - Additional LAN Routes
- (Hubs with add-on only) Redundancy
    - Hosts to ping by ICMP (via WAN)
    - Hosts to ping by ICMP (via LAN)
- (certain Nodes only) GEO Tracking
- Product features license manager
- Administration
    - Users
    - Groups

The lists of menu tree commands in the sections below are most useful as a reference that you can scan for specific menu items you're looking for, although a brief description of most items is provided. For configuration instructions, consult chapters 3-6. The *Permissions* section included in all menus is omitted from this listing. In every case, it includes the items Read Access and *Write Access*, which an administrator can use to grant access to user groups.

In the sections below, the arrow symbol indicates a submenu that can be viewed by clicking the plus sign on a directory in the menu tree. Multiple arrows indicate that a menu is multiple levels down.

2.5.1.5.0 Options for Nodes only

Module slots / WAN interfaces

- A matrix listing of modules
  - Module name
  - Enabled (checkbox)
  - Status
    - Disconnected
    - Connected
    - Connecting
    - Disconnecting
    - Connected Too Slow
    - Connected Stalled
    - Error
  - Configuration type
    - This refers to an internet protocol relevant to this module, for example DHCP, QMI, or PPPoE
  - Using QMI protocol (checkbox) [LTE modules only]
    - QMI is an interface for interacting with Qualcomm Mobile Station modems and replaces the AT protocol
  - Connect on demand (checkbox)
    - Enable this feature to ensure that backup channels connected to time-billed services are only connected as needed

These menus appear with multiple types of module as applicable, depending on the access level of the user:

Automated reconnect Settings

These settings specify when reconnects should take place. Can be reconfigured to accommodate time-based reconnects and power-cycling during extended downtime.

- Reconnect after minutes of uptime
- Reconnect at time of day
- Reset after minutes of downtime

➔➔➔ Traffic counters

- Incoming packets
  - The number of packets received by this Node since last counter reset or router reboot
- Outgoing packets
  - The number of packets sent by this Node since last counter reset or router reboot
- Outgoing dropped packets
  - Packets transmitted by this Node that have not been received at their destination
- Incoming bytes
  - Bytes of traffic received by this Node since last counter reset or router reboot
- Outgoing bytes
  - Bytes of traffic transmitted by this Node since last counter reset or router reboot

Functions

- Reset counters
  - Zeroes out traffic record values

➔➔➔➔ Expected internet link capacity

- Auto-configuration (checkbox)
  - This function auto-detects realistic traffic capacities to auto-fill the bandwidth capacity fields below. Do not activate it on a gigabit ethernet module connected to an external modem, as it will not detect external modem values. Instead, set capacity values for that connection manually.
- Bandwidth capacity to WAN
  - Outgoing traffic in Kbit/s (auto-filled if automated)
- Bandwidth capacity from WAN
  - Incoming traffic in Kbit/s (auto-filled if automated)

➔➔➔➔ VPN Bypass Settings (RuggedVPN only)

VPN Bypass does not treat the line connected to this module as a channel. Instead, when this function is activated, all outgoing traffic for the specified IP address is NAT masked with the WAN IP address of this module. This mode is for data that does not need to go to the datacenter. The destination of traffic on this line must be defined with special routing rules. Contact your vendor or Viprinet Support for additional information.

- Enabled (checkbox)
- IPv4 address
- IPv6 address

These submenus appear for cellular data modules only:

➔➔➔➔ Enabled mobile technologies

Activate relevant mobile data technologies in this menu. All of these controls are checkboxes except for the radio band settings dropdown.

- CDMA 1xRTT
- CDMA EV-DO
- GSM
- UMTS
- LTE
- Enabled LTE bands (LTE only)
- Radio band settings (dropdown)
- Allow roaming

➔➔➔➔ Managed SIM Settings

Status

- Card Status
- Card Account Status
- The status of the provider account associated with this SIM
- Estimated traffic left (in GB)
- Estimated Days Left
- The number of days until this SIM card expires and must be replaced

Properties

- SIM pin

Functions

➔➔➔➔ Managed SIM Settings

- Contact activation server
  - Used to update SIM status on the provider's server

Families of similar module types have the same menu items. Some module types are unique. Menus for the non-swappable SIM card modules in 51X and 500 routers are the same as their hot-plug relatives, with the exception that only the 51X series includes GEO Tracking.

➔➔➔➔ LTE/4G modules

- 4G Europe II
- 4G Americas
  - (LTE 700 with a variety of the following: AWS/CDMA/EV-DO/UMTS/HSPA+/GPRS/EDGE)
- 4G Europe/Australia
- LTE/UMTS/HSPA+/GPRS/EDGE (EU)
- Note: some carriers don't allow failover to UMTS/GSM from LTE.

Properties

- Description
- Module name
- Status
  - Up, down, connecting, etc. Full list on the first page of section 2.5.1.5.0.
- Connect on demand (checkbox)
  - Enable this feature to ensure that backup channels connected to time-billed services are only connected as needed
- APN Auto Configuration (checkbox)
  - Detects the appropriate access point name for this provider
- Access point name (APN)
  - Auto-configured with function above or obtained from cellular radio provider, e.g. fast.t-mobile.com
- PIN (SIM CHV1 code)
  - Your cardholder verification number
- Username
- Password
- Enabled (checkbox)

Functions

- Reconnect
  - Disconnects and reconnects the module to the ISP; necessary so that modified settings can take effect
- Reset (power-cycle)

Tools

➔➔➔➔ LTE/4G modules

Use these utilities to troubleshoot connectivity problems associated with this module connection, outside of the tunnel. See Appendix 1 for details about individual tools.

- Ping
  - A command-line tool discussed in Appendix 1
- Traceroute
  - A command-line tool discussed in Appendix 1
- Download test
- A test of downstream speeds without QoS settings applied. In this menu, this utility only tests this connection outside of the tunnel. In the LAN settings menu, it checks all links at the same time.
- Module info
  - A list of detailed specification and provider info; these may include IP addresses, DSL synchronization rates, mobile data signal strength and cell ID, among others.
- AT command
  - Used to deliver an attention command to the modem. Only available if module is disabled.

➔➔➔➔ UMTS and CDMA modules

- UMTS/HSPA/GPRS/EDGE
- UMTS/HSPA+/GPRS/EDGE
- CDMA 450

The rest of this menu is the same as LTE, with the addition of a Dial String item. UMTS dial strings are frequently formatted ATDT*99***1#. CDMA dial strings are frequently formatted ATDT#777.

➔➔➔➔ GPS-capable modules

LTE/DC-HSPA+/EDGE/GPS
All modular routers can be fitted with a GPS-capable LTE module. Of our non-modular routers, the 51X series, contains them by default; the 500 series does not. The menu set for this module is the same as other LTE types, with the addition of a GEO Tracking submenu.

[Module slots] ➔ [Module] ➔➔ Position determination

➔➔ GEO Tracking

Properties

➔➔ GEO Tracking

- Longitude
- GPS coordinates
- Latitude
- Altitude
  - How far the Node is above sea level
- Speed
  - If the Node is on a vehicle, how fast the vehicle is going in km/h
- Heading
  - Which way the vehicle the Node is in is going, in degrees
- Last updated
  - The date/time when the position information was last updated
- Log position changes
  - If this box is ticked, the location data will be included in the Node log
- Log satellite info
  - As with position changes
- Log NMEA sentences
  - As with position changes and satellite info; NMEA sentences are three letter codes relevant to geographical positioning

Tools

- Google Maps button
  - This tool shows the location of the Node on a map

AccessPoint

Wifi-capable Nodes: 200, 500, and 51X

AccessPoint

- Enabled (checkbox)
- SSID
  - The unique string associated with this WLAN (wireless LAN) and included in the header of all packets originating at it; allows connecting users to identify it
- SSID Broadcast
  - A WLAN with broadcast turned off is not discoverable; only hosts that have already recorded its SSID or sniff other hosts' connections to the WLAN can connect
- Frequency
  - The radio frequency associated with the technology you are using
- Radio channel
  - A relevant sub-frequency within one of the permissible WLAN channels for your region
- Encryption
  - None
  - WEP
  - WPA PSK
  - WPA2 PSK
- Allow 802.11n (checkbox)
  - Enables support for the standard referenced
- Password
  - The password for the WLAN
  - Only available if encryption is on
- Authentication mode
  - Deny Only – clients with their MAC address in the list of Denied Clients will be rejected
  - Authorized Only – only clients with their MAC addresses in the list of
- Authorized Clients will be accepted
- Authorized clients
  - A list of the IP addresses of hosts allowed to automatically connect to the WLAN
- Denied clients
  - A list of the IP addresses of hosts not allowed to connect to the WLAN
- AccessPoint Info / Connected Clients
  - A list of currently connected clients

➔➔➔➔ Ethernet modules and DSL

- Gigabit Ethernet
- Fast Ethernet
- VDSL2/ADSL2+
- ADSL+ Annex A
- ADSL+ Annex B

Properties

- MTU
- Maximum transmission unit. MTU size = packet size. The default is 0, indicating that a value is selected automatically (1500 for ethernet modules, different sizes depending on the configuration type for ADSL). This setting only needs to be modified for modules connected to external modems with no MSS clamping. MSS means maximum segment size. Clamping in this case refers to the MSS value's restriction on TCP traffic. Troubleshooting note: if a timed channel using this module always disconnects on connect, it may be a sign that the MTU value has been set too high.
  - Line type [DSL only] (equivalent to Annex Mode)
  - Changing this setting will reset VDSL Expert settings to defaults
  - Annex A, L, M – Annex A
  - Annex B, J – Annex B
- Multiplex mode
  - As required by provider, e.g. LLC
- ATM VPI (virtual path identifier)
  - ADSL carrier give country and carrier specific most common 0, 1, 8
- VCI (virtual channel identifier)
  - common values 32, 33, 35
- VLAN ID
- Identifies the VLAN associated with this alias

Functions

Same as listed in LTE menu above

Tools

Same as listed in LTE menu above plus Ethernet ARP table tool, which displays associations
The displays which IP addresses are associated with which MAC addresses.

VDSL-only options

(For reference see the VDSL specification)

VDSL-only options

- Annex Mode (equivalent to Line Type)
- Configuration type (protocol)
  - PPPoE
  - PPPoA
  - RFC1483DHCP
  - RFC1483StaticIP
  - IPA
- Connect on demand (checkbox)
  - Enable this feature to ensure that backup channels connected to time-billed services are only connected as needed
- Username
- Password
- MTU
- Maximum transmission unit. MTU size = packet size. The default is 0, indicating that a value is selected automatically (1500 for ethernet modules, different sizes depending on the configuration type for ADSL). This setting only needs to be modified for modules connected to external modems with no MSS clamping. MSS means maximum segment size. Clamping in this case refers to the MSS value's restriction on TCP traffic. Troubleshooting note: if a timed channel using this module always disconnects on connect, it may be a sign that the MTU value has been set too high.
- ATM VPI (virtual path identifier)
  - ADSL carrier give country and carrier specific most common 0, 1, 8
- VCI (virtual channel identifier)
  - common values 32, 33, 35
- VLAN ID
- Multiplexing Mode (must be set as appropriate for your provider)
  - LLC
  - VC
- Enabled

Functions

As in LTE menu

Tools

As in LTE menu

➔➔ VDSL Module Expert Settings

➔➔ Port Options

- I43 Carrier Set
- V43 Carrier Set
- A43 Carrier Set
- B43 Carrier Set
- D43 Carrier Set
- J43 Carrier Set
- Short CLR Support

➔➔ Line Type Configuration

All settings in this menu are checkboxes

➔➔ VDSL Module Expert Settings

- DSL1 DMT Annex A
- ADSL1 DMT Annex B
- ADSL1 DMT Annex C
- ADSL2 DMT Annex J
- ADSL2 DMT Annex A
- ADSL2 DMT Annex B
- ADSL2+ Annex A
- ADSL2+ Annex B
- ADSL2+ Annex J
- ADSL+ Annex M
- VDSL 1
- VDSL2 Profile 8A
- VDSL2 Profile 8B
- VDSL2 Profile 8C
- VDSL2 Profile 8D
- VDSL2 Profile 12A
- VDSL2 Profile 17A
- VDSL2 Profile 30A
- ADSL T1E1 issue 2
- VDSL Profile 12B

➔➔ BME Provision Settings

- Customer ID
- Key 0
- Key 1
- Key 2

Stacking

Requires an add-on license; see Appendix 6

Status

- MasterIP address
  - The IP address of the Master Node in the stack
- Status
  - The status of the current master; see full list in section 2.5.1.5.0, *Module slots / WAN interfaces*

Properties

- Enabled (checkbox)
  - Whether stacking is enabled on this Node
- Stacking group ID
  - The ID for the Node stack
- Password
  - The authentication password for stacked Nodes

➔➔ Stacked routers

Properties

Stacking

- Current master
- Matrix of stacked routers:
- Name + serial #
- Connected
- IP address

Properties

Designated master (dropdown of stacked router serial numbers)

➔➔➔➔ Multichannel VPN Router [SERIAL #] (stacked Node)

- Serial
- Name
- Connected
- IP address

➔➔➔➔➔➔ Stacked router modules

The same as in Module Slots/WAN Interfaces

➔➔ LAN IP address aliases

Used to allow the LAN interface to be part of multiple LANs

The same as non-stacked LAN IP address aliases

➔➔ Additional LAN Routes

Used to route VPN connections to a different LAN gateway; this menu includes a matrix list of LAN routes, including the properties below:

Properties

- Name
- Network
  - The IP subnet which should be reachable via the route.
- Gateway
  - The IP address of the host, which has additional routing information to reach the IP subnet. For example: you are in the network 192.168.1.0/24 and you want to reach a host at 10.0.0.0/8. You must enter an additional LAN route that means “Network 10.0.0.0/8 is reachable by local gateway 192.168.1.254”.
- VLAN ID
  - Used to identify the VLAN of a packet coming from this LAN, if segmentation is enabled; DHCP can only be used with VLAN 0.

2.5.1.5.1 Hub-specific menus

VPN Clients / Road Warriors

Although the VPN Client menu and its associated submenus also appear on Nodes, these properties should only be edited on the Hub they are associated with. One client license is provided with your router; licenses must be bought to enable additional client accounts. See Appendix 6. For directions on setting up VPN client service, see section 5.1

Properties

VPN Clients / Road Warriors

- Client IP address pool
  - Addresses are dynamically allocated to VPN client users

Functions

- Copy QoS templates to here

Tools

- Backup QoS settings
- Restore QoS settings

➔➔ VPN Client users

Properties

- SSL certificate fingerprint
  - The SSL certificate number associated with this Hub
- Number of licensed client accounts
  - Total
- Number of licensed client accounts still left
  - Remaining VPN client accounts
- Matrix of users
  - Username
  - Enabled
  - Connected

➔➔ License manager

Total number of licensed client accounts

Functions

- Add a license (*RuggedVPN*: Add an activated license file)
- Activate a license key online
- Contact license server and update licenses

➔➔ QoS Traffic classes – classic firmware

Matrix list of properties:

- Name
- Channel selection/bonding mode
  - See section 6.0.1.1 for more detail on this feature.
- Minimum guaranteed bandwidth
  - This class must have access to at least this amount of bandwidth
- Maximum allowed bandwidth
  - The maximum amount of bandwidth you are willing to devote to this traffic class
- Maximum bonding latency
  - The highest level of latency that is acceptable for this traffic class, measured in milliseconds.

➔➔ QoS Traffic classes (revised in RuggedVPN)

Properties

➔➔ QoS Traffic classes (revised in RuggedVPN)

- Name
- Packet queue moderation (checkbox)
  - If this function is enabled and the packet queue for this traffic class is about to overflow, TCP flows will be moderated using the „Random Early Detection" algorithm. If this function is not enabled, then „Tail drop" will be used. For TCP traffic and most other protocols with transmission rate adaptation, Packet queue moderation should be enabled. For latency-sensitive protocols (e.g. VoIP), it should be disabled.
- Log new connections
  - This setting should only be enabled to check a newly created QoS rule set for errors. Disable it as soon as debugging is complete. Never use it for a class associated with system log traffic as an endless loop will ensue. Check the AdminDesk log. If there is an error, connections will not appear in the system log.
- First bonding priority
  - The options for this and the other bonding priorities are:
    - Link stability
    - Packet loss
    - Cost
    - Latency
    - Bandwidth
    - None
- Second bonding priority
- Third bonding priority
- Preferred number of channels
  - This is the number of channels that you would prefer this QoS class use. The router will always preferentially select those that best match the bonding priorities you have configured. More than one channel must be used for Forward Error Correction to work effectively, even if this requires you to use inferior channels.
  - FEC (forward error correction) level
    - Single
    - Double
    - Duplicate (not FEC; sending extra copies of packets as with Bonding Diversity)
    - Triplicate (not FEC, extra copies)
    - Quadriplicate (not FEC, extra copies)
    - FEC settings define how many channel dropouts FEC can compensate for. See section 6.0.3.1 and figure 6.5 for more information.
  - Minimum guaranteed bandwidth
    - The lowest level of bandwidth traffic in this class can tolerate
- Maximum allowed bandwidth
  - The maximum amount of bandwidth you will permit this class to use
- Maximum bonding latency
  - The highest level of latency that is acceptable for this traffic class, measured in milliseconds.
- Required Link Stability
  - The maximum packet loss in percent that a channel may have and still be used by this traffic class. If no channel in the tunnel meets this requirement, this setting will be ignored so data can still be transmitted.
- Guaranteed Delivery
  - Enable Guaranteed delivery to ensure that transmissions in this class will not lose packets. If forward error correction is unable to recover a lost packet, the packet will be retransmitted. The router will also be able to use more effective compression algorithms.
- Data compression (checkbox)
  - When Data compression is enabled, the router will periodically analyze traffic flows in this class to determine if the data being transmitted is compressible, and compress it. The amount of compression used is based on how much unused CPU capacity is available on the routers processing this traffic flow. If you know that traffic in this class will never be compressible—for example because it is encrypted—you should not enable this feature.

➔➔ Client's routing and DNS settings

➔➔➔➔ Segmented VPN Clients (if Hub Segmentation add-on enabled)

➔➔➔➔➔ [Segment name]

- Name
- Client IP address Pool
- Tunnel Segmentation ID

Functions

- Copy QoS templates to here

Tools

- Backup QoS Settings
- Restore QoS Settings

WAN/VPN Routing and NAT

- Transfer network (router internal)
- IPv6 Transfer network (router internal)

➔➔ WAN/VPN routing rules

- Default WAN/VPN interfaces
- Allow route-back (checkbox)

➔➔ Masquerading (outbound NAT) Entries

This menu also appears on Nodes. Most of the time, these settings should be configured on the Hub.

- Matrix of entries

➔➔➔ [NAT Entry]

- Name
- Network
  - Network segment associated with this NAT in CIDR notation
- IP address to mask with
  - In many circumstances, the Hub does NAT for the LANs it is connected to.
- Tunnel segmentation ID

➔➔ Port forwarding entries

- Name
- Original destination IP address
- IP address protocol
- Original destination port
- New destination IP address
- New destination port

➔➔ VLAN Management *(revised in RuggedVPN)*

This menu also appears on Nodes, but these settings should be configured on the Hub.

- VLAN ID
- Description

➔➔➔➔ [VLAN number]

- Description
- VLAN ID

WAN Settings

Properties

- WAN IP address
  - The IP address of the router’s WAN interface
- WAN netmask
- Default gateway IP address
  - The IP address to which this interface should send all traffic. This IP address is likely a switch or router.

Tools

- Ping
- Traceroute
- Download test
  - A test of downstream speeds that works directly on the WAN interface without QoS settings or encryption, and not through the VPN tunnel
- Ethernet interface info
  - Lists the link modes used, along with other characteristics of the WAN interface and the Hub of which it is part
- Ethernet ARP table tool
  - List of IP addresses associated with different MAC addresses

Redundancy settings

Requires an add-on license; see Appendix 6 for license installation instructions
See section 6.4

Properties

- Redundancy system enabled (checkbox)
- Redundancy Group ID
  - This is a number between 1 and 65535; only routers using the same ID will be able to see each other. Changing this setting will allow you to smoothly remove this router from a redundancy group without it being replaced by a hotspare.
- Group Password
  - This password is used to encrypt traffic between Hubs in the group and needs to be identical for all Hubs sharing the same group ID. It must be 8 characters long and including mixed upper and lowercase letters. Change this setting to remove this router from a redundancy group without it being replaced by a hotspare.

Functions

- Convert router to hotspare
  - See section 6.4

Tools

- Map of routers seen

➔➔➔➔ Router map for redundancy group [ID ##]

Sorting order selection

- Serial number
- Operation mode/status
    - Active
    - Replacement
    - Hotspare
    - Probe
- Health status

Router information list

    - Router serial
    - Router type
    - Router status
    - Last heartbeat received
    - Up for [period of time]
    - Previously up for [period of time] (hotspare)
- Router is reporting the following ICMP ping results (hotspare only)

➔➔ Hosts to ping by ICMP (via LAN, active Hubs only)

- Matrix of hosts:
    - Sorting order
    - Serial #
    - Operation mode/status
        - Hotspare
        - Probe
        - Active
        - Replacement

➔➔➔➔ [IP address]

(List of IP addresses for Hubs in this group)

➔➔ Matrix of "Hosts to ping by ICMP" (via WAN, active Hubs only)

This matrix lists three properties; the only data you enter here is a ping target. If the target cannot be reached by any Hub, a hotspare will take over for it

- Sorting order
- Serial #
- Operation mode/status
    - Active
    - Hotspare
    - Replacement
    - Probe

➔➔➔➔ [IP address]

List of Hubs by IP address

Hub Tunnel Segmentation

There is no individual menu for this function, which is covered in sections 6.8 and 6.5.

2.5.1.5.2 Options for both Nodes and Hubs

VPN Tunnels

Status

- SSL certificate fingerprint
- Matrix list of tunnels:
  - Tunnel name
  - Tunnel segmentation ID
  - Enabled
  - Connected
  - Total channel bandwidth from WAN
    - The upstream bandwidth this channel can offer
  - Total channel bandwidth to WAN
    - The total downstream bandwidth this channel can offer

[Tunnel name]

Properties

- Tunnel name
- Remote router‘s serial
- Connected (checkbox)
- Number of connected channels
- Total channel bandwidth to WAN
- Total channel bandwidth from WAN
- Total reliable channel bandwidth to WAN
- Total reliable channel bandwidth from WAN
- Fastest channel bandwidth to WAN
- Fastest channel bandwidth from WAN
- Fastest reliable channel bandwidth to WAN
- Fastest reliable channel bandwidth from WAN
- Remote router‘s SSL certificate fingerprint
- Require valid fingerprint
- Connection password
- Enabled (checkbox)
- IP address for this router to connect to (only for VPN Nodes´)
- Minimum number of connected channels
- Minimum backup score
  - See section 6.3 for information about backup scores

[Tunnel name]

Functions

- Copy QoS templates to here
- Reconnect

Tools

- Backup QoS settings
- Restore QoS settings

➔➔➔➔ Tunnel channels

- Matrix of channels:
  - Channel name (cannot include spaces)
  - Status
    - See full list in section 2.5.1.5.0, Module slots / WAN interfaces; additional statuses only relevant to channels include
    - Connected Ping Test
    - Connected Ping Test Wait
  - Enabled (checkbox)
  - Backup channel /checkbox)
    - This value is "True" if this is a backup channel and "False" if it isn't
  - Maximum allowed bandwidth to WAN
    - Data transfer limit per second for this channel
  - Link stability
    - An estimate of connection stability based on packet loss percentages for the past 60 minutes, expressed as a value from 0-100%, with 0 meaning no packets were successfully sent, and 100% meaning no packets were lost. A low-loss link type, such as DSL, should have a stability of 99-100%. Cellular data links should have a stability of above 90%.

➔➔➔➔➔➔➔ [Channel name]

Status

- Status
  - See full list in section 2.5.1.5.0, Module slots / WAN interfaces
- Last connection error
  - This is the last connection error message for this channel. If it is empty, no error has been reported since the last restart.
- Packet loss
  - The current packet loss for this channel, represented as a percentage. If this tunnel channel is using a low-loss link, such as most wired connections, any value higher than 1% is usually evidence of connection problems between the Hub and the Node. Values up to 5% are normal for wireless connections.
  - Link stability This is an estimate of the stability of the connection used by this channel, based on packet loss percentages for the past 60 minutes, expressed as a value from 0-100%, with 0 meaning no packets were successfully sent, and 100% meaning no packets were lost. A low-loss link type, such as DSL, should have a stability of 99-100%. Cellular data links should have a stability of above 90%.

Properties

➔➔➔➔➔➔➔ [Channel name]

- Channel name
- IP address for this channel to connect to (Nodes only)
  - WAN IP address of the Hub this Node connects to
- Enabled (checkbox)
- Backup channel (checkbox)
- Backup score
  - This is the score that will be counted (multiplied with the channel stability value) if this channel is connected. Using the tunnels Minimum Backup Score setting you can control on how many channels need to be connected. This way, if a non-backup channel drops out, and due to that the backup score is no longer reached, backup channels will be brought up until the Minimum Backup Sore is reached again.
- Cost
  - This is the cost of using this link. A value of 0 here indicates cost is not a concern with this channel. A channel with 100 in this field is very expensive (e.g. satellite). As long as lower-cost channels are sufficient to meet bandwidth demands, they will be preferred.
- Data encryption (checkbox)
  - If this option is enabled, all data passing through this channel will be encrypted using 256 bit AES and secured against modification. If it is disabled, only the connection handshake (password exchange) will be encrypted.
- Bandwidth autotuning (checkbox)
  - When this function is enabled, the router will automatically determine the highest traffic load this channel can support without saturation occurring. That will ensure low latency. To avoid speed test traffic on monthly limited or high-cost lines, you need to select an appropriate autotuning setting (one option is passive autotuning). Please see Performance Finetuning Settings below.
- Minimize autotuning traffic (checkbox)
  - Limit the amount of bandwidth that may be dedicated to autotuning tests
- Latency autotuning (checkbox)
  - This function calculates the maximum allowed latency and optimal latency below value, in an automated way.
- Maximum allowed bandwidth to WAN
  - Top upstream bandwidth value this channel can support; should be set below its actual capacity
- Minimum required bandwidth to WAN
  - The lowest bandwidth value that traffic using this channel can tolerate
- Maximum allowed latency
  - The highest latency value that traffic using this channel can tolerate
- Optimal latency below
  - If this value is reached, this router will stop allocating additional bandwidth to this channel prevent packet loss

Functions

- Reconnect
  - Reconnect the channel

➔➔➔➔ Performance finetuning

- Autotuning algorithms
  - See section 6.1
- Speed test starting value
  - This value determines the bandwidth level at which the router will begin doing speed tests with artificial traffic. It matches or is close to the Minimum required bandwidth to WAN; the default is 32. This value is not auto-detected.
- Congestion control [algorithm]
  - See Appendix 10
- Quick congestion response (checkbox)
  - If this function is enabled, the maximum allowed bandwidth value will be automatically adjusted to fit the TCP congestion window as needed to ensure that connections experiencing bursts of packet loss do not become overloaded. The router may take longer to return the channel to normal service when this setting is used with high-latency links. Enabled by default.
- Rapid reconnects (checkbox)
  - Especially relevant for situations where the router is moving rapidly from cell to cell, such as in high-speed trains; also see the Rapid autotuning mode. A reconnect is triggered when no successful transmission is sent or received for 3 seconds.
- Save traffic when idle
  - In a scenario where a Viprinet VPN tunnel is established but not used, Viprinet can reduce the amount of keep alive traffic on the tunnel channels and preserve data volume (for example for mobile environment).
- Optimal Latency Multiplier
  - This option gives you additional control over latency autotuning. A higher value here may allow you to access more bandwidth, but at the cost of higher latency during uploads and downloads. This setting accepts fractional numbers. Make changes in small increments and check the result after reconnecting the channel.
- Retransmission Multiplier
  - The router multiplies this value by its Optimal Latency Below setting. If the product exceeds the Optimal Latency Below setting, all packets sent through this channel will be retransmitted on another channel. For example, a multiplier of 3 for a channel with an Optimal Latency Below setting of 100 means that all packets will be retransmitted if latency reaches 300ms.
- Link stability checks
  - This function is enabled by default. The router monitors link stability in 60 minute chunks. Disconnects and packet loss reduce the link stability value. This channel will only be used to support traffic in QoS classes whose Required Link Stability values it can match. Warning: If this function is disabled, link stability will always appear at 100%, even if it is not.
- Warn if Link Stability is below
  - If the stability of this channel drops below this value, a warning will be sent to the logging system. For DSL, this setting should be 90-95%. Mobile links, depending on signal strength and movement from cell to cell, range from 50-90%. The default value is 75. Enter 0 to turn off this feature.
- Log speed tests
  - This setting should only be enabled to run channel performance diagnostics.

➔➔➔➔ QoS traffic classes

➔➔ QoS Traffic classes – classic firmware

- Matrix list of properties:
- Name
- Channel selection/bonding mode
  - See section 6.0.1.1 for more detail on this feature.
- Minimum guaranteed bandwidth
  - This class must have access to at least this amount of bandwidth
- Maximum allowed bandwidth
  - The maximum amount of bandwidth you are willing to devote to this traffic class
- Maximum bonding latency
  - Base value for the calculation of highest acceptable channel latency for this class, measured in milliseconds.

➔➔ QoS Traffic classes (revised in RuggedVPN)

Properties

- Name
- Packet queue moderation (checkbox)
  - If this function is enabled and the packet queue for this traffic class is about to overflow, TCP flows will be moderated using the „Random Early Detection" algorithm. If this function is not enabled, then „Tail drop" will be used. For TCP traffic and most other protocols with transmission rate adaptation, Packet queue moderation should be enabled. For latency-sensitive protocols (e.g. VoIP), it should be disabled.
- Log new connections
  - This setting should only be enabled to check a newly created QoS rule set for errors. Disable it as soon as debugging is complete. Never use it for a class associated with system log traffic as an endless loop will ensue. Check the AdminDesk log. If there is an error, connections will not appear in the system log.
- First bonding priority
  - The options for this and the other bonding priorities are:
    - Link stability
    - Packet loss
    - Cost
    - Latency
    - Bandwidth
    - None
- Second bonding priority
- Third bonding priority
- Preferred number of channels
  - This is the number of channels that you would prefer this QoS class use. The router will always preferentially select those that best match the bonding priorities you have configured. More than one channel must be used for Forward Error Correction to work effectively, even if this requires you to use inferior channels.

➔➔ QoS Traffic classes (revised in RuggedVPN)

- FEC (forward error correction) level
    - Single
    - Double
    - Duplicate (not FEC; sending extra copies of packets as with *Bonding Diversity*)
    - Triplicate (not FEC, extra copies)
    - Quadriplicate (not FEC, extra copies)
    - FEC settings define how many channel dropouts FEC can compensate for. See section 6.0.3.1 and figure 6.5 for more information.
  - Minimum guaranteed bandwidth
- The lowest level of bandwidth traffic in this class can tolerate
- Maximum allowed bandwidth
  - The maximum amount of bandwidth you will permit this class to use
- Maximum bonding latency
  - The highest level of latency that is acceptable for this traffic class, measured in milliseconds.
- Required Link Stability
  - The maximum packet loss in percent that a channel may have and still be used by this traffic class. If no channel in the tunnel meets this requirement, this setting will be ignored so data can still be transmitted.
- Guaranteed Delivery
  - Enable *Guaranteed delivery* to ensure that transmissions in this class will not lose packets. If forward error correction is unable to recover a lost packet, the packet will be retransmitted. The router will also be able to use more effective compression algorithms.
- Data compression (checkbox)
  - When *Data compression* is enabled, the router will periodically analyze traffic flows in this class to determine if the data being transmitted is compressible, and compress it. The amount of compression used is based on how much unused CPU capacity is available on the routers processing this traffic flow. If you know that traffic in this class will never be compressible—for example because it is encrypted—you should not enable this feature.

➔➔➔➔ QoS traffic sorting rules

Matrix list of rules:

- Name
- Matching IP protocols
  - Options
    - TCP
    - UDP
    - ICMP
    - IGMP
    - EGP
    - IGP
    - RSVP
    - GRE
    - ESP
    - AH
    - EIGRP
    - OSPF
    - VRRP
    - L2TP
    - SCTP
    - FC
    - IPIP
    - IPV6

➔➔➔➔ QoS traffic sorting rules

- How to match IP addresses
  - Options:
    - Ignore
    - Source
    - Destination
    - Source or Destination
- How to match TCP/UDP ports
  - Options:
    - Ignore
    - Source
    - Destination
    - Source or Destination
    - Source and Destination
- TCP/UDP port range
  - The port or ports this traffic enters from
- Target class
  - The target traffic class, e.g. Web surfing, Interactive, etc.

➔➔➔➔ Receive dejitter buffer fine-tuning

Realtime applications, like VoIP, are very sensitive to jitter. This setting helps to alleviate jitter's impact on quality

Properties

These settings are used to fine tune the dejitter buffer of the receiving side for the lossy bonding mode.

- Minimum dejitter buffer
  - Default is 100ms. Setting this to a higher value will increase stability, but at the cost of increasing latency.
- Maximum dejitter buffer size
  - Default is 2000ms. Setting this to a higher value will give you a more stable data stream even on very unstable links (e.g. bonded 3G while moving), but increase latency. A lower value will permit dropouts but reduce latency.

LAN Settings

This set of menus allows you to configure and troubleshoot your LAN interface

Properties

- LAN IP address
  - The IP address of the router's LAN interface
- LAN netmask
  - The netmask of the router's LAN interface
- DNS hostname
  - If you have configured a DNS hostname associated with this LAN IP address, enter it here so you can use it to access the router. The SSL certificate for this router must be associated with its LAN IP or hostname.
- Default gateway IP address
  - Nodes don't usually need default gateways because their VPN tunnels serve that purpose. In Node stacks, the shared stack IP address is designated as the default gateway.
  - Hubs usually connect to a router at your ISP:
- Allow routeback (checkbox)
  - When this setting is ticked, traffic in the LAN network associated with this router can be forwarded via its LAN interface, for example to reach a different VLAN.

LAN Settings

- Announce prefix (IPv6 only) ***RuggedVPN***
  - This function makes it possible for hosts on a LAN to auto-configure their IP addresses without using DHCP. It should always be turned off on Hubs.
- Route filtering (checkbox)
  - This feature is only useful for Nodes; don't use it on Hubs. If this feature is active, the sources of all incoming packets are checked to prevent address spoofing. Turn this on whenever you are connecting to an untrusted network or using AccessPoint to provision wifi access through this router.
- All VLANs may talk to VPN tunnels
  - Allows virtual LANs to connect to un-segmented VPN tunnels (see section 6.8 for details on tunnel segmentation)

Tools

Use these utilities to troubleshoot connectivity problems by assessing all channels in the tunnel at once. If you only want to diagnose problems with a specific channel, use the tools menu for the module associated with it. See Appendix 1 for details about individual tools.

- Ping
- Traceroute
- Download test
  - See figure 2.9
- Ethernet interface info
  - See figure 2.21
- Ethernet ARP table tool
  - See figure 2.10

➔➔ LAN IP address aliases

- Matrix list
  - IP address
  - Netmask
  - Default gateway (VLANs only, Hubs only)
  - VLAN ID
- Name ***RuggedVPN***
- Announce prefix (IPv6 only) ***RuggedVPN***
  - This function makes it possible for hosts on a LAN to auto-configure their IP addresses without using DHCP. It should always be turned off on Hubs.

➔➔➔➔ [Alias IP address]

Properties

- IP address
- Netmask
- Default gateway (VLANs only, Hubs only)
- VLAN ID
  - Only used with Hub segmentation add-on

Tools

- Ethernet ARP table

➔➔ Additional LAN Routes

- Matrix list of routes. Column heads:
- Name
- Network
- Default gateway
- VLAN ID

➔➔➔➔ [Route name]

Properties

- Name
- Network
- Gateway
  - Nodes: The VPN Hub IP address
  - Hubs: Usually your ISP's router IP address
- VLAN ID

➔➔➔➔ Ethernet speed and auto-negotiation settings

- Auto-negotiation
- Duplex mode
  - Half
  - Full
- Speed (in Mbit/s)
  - 10
  - 100
  - 1000

➔➔➔ Traffic counters

- Incoming packets
  - The number of packets received by this Node since last counter reset or router reboot
- Outgoing packets
  - The number of packets sent by this Node since last counter reset or router reboot
- Outgoing dropped packets
  - Packets transmitted by this Node that have not been received at their destination
- Incoming bytes
  - Bytes of traffic received by this Node since last counter reset or router reboot
- Outgoing bytes
  - Bytes of traffic transmitted by this Node since last counter reset or router reboot

Functions

  - Reset counters
  - Zeroes out traffic record values

➔➔ DHCP server settings

Properties

- DHCP Server enabled (checkbox)
  - DHCP can only be used with VLAN 0.
- Operation mode
  - Server
    - If this router should serve addresses via DHCP, choose this setting.
  - RelayAgent
    - This setting is used to forward DHCP requests arriving at this Node's LAN interface to a DHCP server on another network. If you select this option, do not enter settings in this menu; enter them on the server you are relaying requests to.
- DHCP Server IP address pool range
  - This is the range within which addresses can be dynamically assigned in this LAN
- Gateway IP address
  - This is the IP address that hosts configured via DHCP should use as a gateway. Use this router's LAN IP address or one of its aliases here. This IP address needs to be part of the same network segment as the DHCP Server IP address.
- Netmask
- IP address of primary DNS
  - Preferred nameserver
- IP address of secondary DNS
  - Backup nameserver
- DHCP Domain name
  - Optional
- DHCP server to relay to
- Lease time (seconds)
  - How long this router's DHCP leases last

Functions

- Clear dynamic leases
  - Revokes dynamic IP addresses given to all hosts

Tools

- DHCP current lease table tool
- This tool allows you to generate a table of active leases. These values are only meaningful if the DHCP service is currently running and assigning addresses. DHCP can only be used on VLAN 0.

➔➔➔➔ DHCP Static Leases

If you need to give static IP addresses to any hosts associated with the LAN this Node manages, do it in this menu.

- MAC address
- Hostname
- Lease time

➜➜ LAN IP address aliases

- Matrix list
- IP address
- Netmask
- Default gateway (VLANs only, Hubs only)
- VLAN ID
- Name ***RuggedVPN***
- Announce prefix (IPv6 only) ***RuggedVPN***
  - This function makes it possible for hosts on a LAN to auto-configure their IP addresses without using DHCP. It should always be turned off on Hubs.

➜➜➜ Traffic counters

- Incoming packets
  - The number of packets received by this Node since last counter reset or router reboot
- Outgoing packets
  - The number of packets sent by this Node since last counter reset or router reboot
- Outgoing dropped packets
  - Packets transmitted by this Node that have not been received at their destination
- Incoming bytes
  - Bytes of traffic received by this Node since last counter reset or router reboot
- Outgoing bytes
  - Bytes of traffic transmitted by this Node since last counter reset or router reboot

Functions

- Reset counters
  - Zeroes out traffic record values

➔➔ Ethernet speed and auto-negotiation settings

- Auto-negotiation
- Duplex mode
  - Half
  - Full
- Speed (in Mbit/s)
  - 10
  - 100
  - 1000

Integrated services

These Access Control Lists are the same for all services
Enhanced SNMP optimization are accessible here

➔➔ AdminDesk service settings

Attention: If you regenerate or change the SSL certificate while you are connected to this web interface via HTTPS, the HTTPS web interface will become unavailable until the new certificate is ready. This may take up to a minute. To be on the safe side, always make sure that you can reach the HTTP interface (see ACL settings) so you can access the AdminDesk via HTTP if you are locked out via HTTPS.

Properties

- Automatically generate self-signed SSL certificate [checkbox]
- CA certificate
  - The certificate issuing authority's certificate
- Intermediate CA certificate
- Certificate
  - The SSL certificate for this AdminDesk instance
- Certificate private key
  - Used to decrypt this certificate
- Certificate private key password
  - Password needed to change this certificate

➔➔ SNMP settings

- Enabled (checkbox)
  - Activates or deactivates SNMP
- Community
  - The community name, which is transferred unencrypted, authenticates SNMP clients. This value must be customized for security reasons; SNMP clients are only able to read information from this Node if they have its community name
- Location information
  - The location of the Node; you might want to indicate its building/floor/rack
- Contact information
  - The administrator's email and phone number

➔➔ DNS service settings

See glossary for more on DNS and nameservers

- DNS server operation type
- Nameservers
- Enabled (checkbox)

➔➔➔➔ Access Control Lists

Properties

- Warn on unauthorized access (checkbox)

➔➔➔➔➔➔ Allow ACL

- Name – location (e.g. from VPN, from anywhere)
- Source Network or Host IP address (CIDR)
- VLAN ID
  - Only used with Hub segmentation or enterprise feature license.
- From LAN
- From VPN

➔➔➔➔➔➔ Deny ACL

By default, there are no deny rules

➔➔ NTP service settings

As this is an internal service only, there is no need for ACLs

- NTP servers to query
  1. Network Time Protocol servers to consult
- NTP server pools to query
- Enabled (checkbox)

➔➔ SSH CLI service settings

- Hostkey
  - The code used to identify this host when you connect via SSH on the command line
- Enabled (checkbox)

Functions

- Generate new hostkey
- Color Scheme ***RuggedVPN*** only
  - Plain
  - Mono
  - Bright
  - Dark

➔➔ Additional LAN Routes

- Matrix list of routes. Column heads:
- Name
- Network
- Default gateway
- VLAN ID

➔➔➔➔ [Route name]

Properties

- Name
- Network
- Gateway
- VLAN ID

➔➔➔ Traffic counters

- Incoming packets
  - The number of packets received by this Node since last counter reset or router reboot
- Outgoing packets
  - The number of packets sent by this Node since last counter reset or router reboot
- Outgoing dropped packets
  - Packets transmitted by this Node that have not been received at their destination
- Incoming bytes
  - Bytes of traffic received by this Node since last counter reset or router reboot
- Outgoing bytes
  - Bytes of traffic transmitted by this Node since last counter reset or router reboot

Functions

- Reset counters
  - Zeroes out traffic record values

➔➔ Ethernet speed and auto-negotiation settings

- Auto-negotiation
- Duplex mode
  - Half
  - Full
- Speed (in Mbit/s)
  - 10
  - 100
  - 1000

Logging and maintenance

This is where you can set what items will be logged and where logs will be sent to

Properties

Logging and maintenance

- Router name
- Time zone
  - The time zone the router is located in
- Remote logging: Syslog collector IP address
  - Routers' log files are temporary and dumped on reboot. This setting determines the IP address of the server that will collect system log files so they can still be viewed after a router reboot.
- Remote logging: Syslog minimum level
  - The lowest level of alert (see table 5.0, section 5.4) that will be sent to the logging server
- Remote logging: syslog RFC 3164 compliance
- Allow HTTP test downloads (checkbox)
  - This function should only be enabled for bandwidth tests. It enables the *Download Test* tool ("download from Hub traffic generator") in the LAN settings menu.
- Allow remote debugging connections (checkbox)
  - This should only be enabled when you are testing the router. This makes it possible for Viprinet Support to deliver direct dial-in services via SSH.
- Router model ***RuggedVPN only***
- Router serial ***RuggedVPN only***
- Firmware version ***RuggedVPN only***

Functions

- Reboot router

Tools

- Connectivity diagnostics tool
  - See figure 2.15
- Backup configuration
  - See figure 2.11
- Restore configuration
  - When using this function, it is important to ensure that you do not delete add-on licenses. This is done by checking the box labeled "Do not overwrite existing licenses." See figure 2.12

➔➔ Router Health menu

- CPU temperature (celsius)
- System temperature (celsius)
- Fan [#] status
- Fan [#] RPM speed
- Memory Usage (in KB)
- Quiet mode
- Fan [#] enabled (checkbox)

➔➔➔➔ CPU Load

- Current CPU Load in %
- Average CPU Load in %

➔➔ Router Firmware update

- Update status
- List of available updates
- Automatic update mode
- Time of day to install updates
- Downgrade to classic firmware ***RuggedVPN only***

Functions

- Check for updates
- Download available updates
- Install available updates
- Refresh

Functions

- Manual Firmware Upload
- Commit Interval
  - How often sampled traffic data is committed to the reporting server, in minutes. Samples are taken once per minute, which also is the minimum value for the commit interval. The default value is 5 minutes.
- Reporting Server URL
  - This is the URL of the server sampled traffic data should be sent to. Both http:// and https:// (SSL) URLs are supported. Example: https://myserver.com/data.php
- Reporting Server Username
  - This is the account username to be used when committing data to the accounting server and must match an existing account on the chosen server.
- Reporting Server Password
  - The account password for the username given
- Server Reporting Enabled (checkbox)

Tools

- Real-time 24 hour traffic statistics
  - Click this button to see detailed traffic statistics for the past day for each tunnel connected to this Node or Hub

QoS rules and classes templates

Functions

- Restore Manufacturing Defaults

Tools

- Backup QoS settings
- Restore QoS settings

Product features license manager

Also see Appendix 6

Status

- Under Maintenance Contract
- Extended SNMP Monitoring licensed
- VPN Hub Redundancy licensed
- VPN Hub Tunnel Segmentation licensed
- Streaming Optimization licensed
- Node Stacking licenses
- Trial running
- Trial token
- License key
- Type of license

Functions

- Add a license / Add an activated license file
- Activate a License Key online RuggedVPN only
- Contact license server and update license RuggedVPN only

➔➔ [License key]

- License key
  - The sixteen-character code associated with this license
- Generation date
- Expiration date
- Expiration date (in local time zone)
- Valid (for this router) (checkbox)
- Type of license

Properties

- License file
  - Paste the long license code generated when you buy a license here

Administration

You can control access to every individual menu in the AdminDesk with the controls in their Permissions panes. All AdminDesk permissions are group rather than user-based.

Properties

- AdminDesk root password.

➔➔ Users

Properties

Administration

- Username
- Date/Time of creation (blank for root)
- Date/Time of last modification (blank for root)
- Date/Time of last login
- Username
- Password
- Public Key
  - One key is associated with each user for verification purposes

➔➔➔➔ [user account]

- Date/Time of creation (blank for root)
- Date/Time of last modification (blank for root)
- Date/Time of last login

➔➔ Groups
Properties

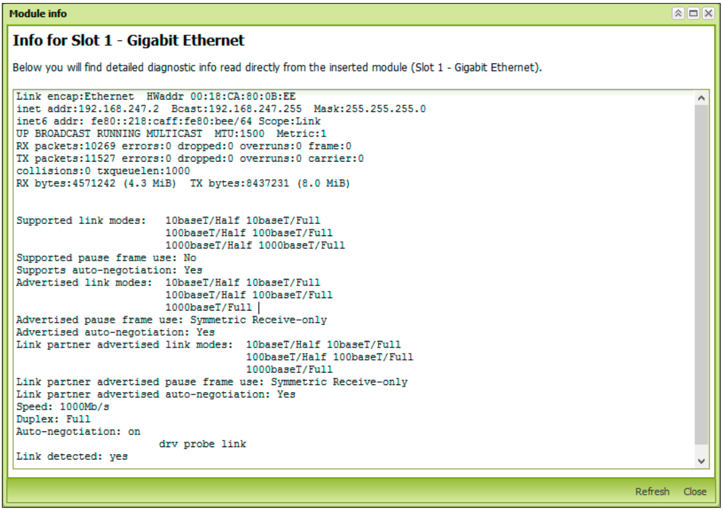
- Group name
- Group description
- Members

➔➔➔➔ [group]

- Group name
- Group description
- Members

2.5.2 Tool overview

This section includes screenshots of all the tools you can use in Hub the AdminDesk. All tools executed directly from module menus and submenus reflect values unaffected by QoS settings. This is because they are not assessing the tunnel, only the module where you access them. Tools executed from LAN settings do assess the tunnel and are therefore affected by QoS settings.



Module info

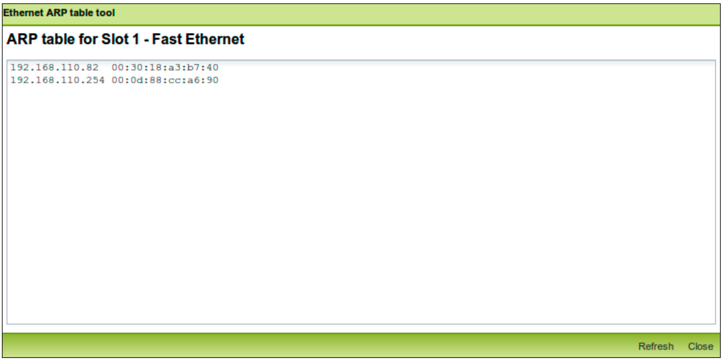
Info for Slot 1 - Gigabit Ethernet

Below you will find detailed diagnostic info read directly from the inserted module (Slot 1 - Gigabit Ethernet).

```
Link encap:Ethernet  HWaddr 00:18:CA:80:0B:EE
inet addr:192.168.247.2  Bcast:192.168.247.255  Mask:255.255.255.0
inet6 addr: fe80::218:caff:fe80:bee/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:10269 errors:0 dropped:0 overruns:0 frame:0
TX packets:11527 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4571242 (4.3 MiB)  TX bytes:8437231 (8.0 MiB)


Supported link modes:   10baseT/Half 10baseT/Full
                        100baseT/Half 100baseT/Full
                        1000baseT/Half 1000baseT/Full
Supported pause frame use: No
Supports auto-negotiation: Yes
Advertised link modes:  10baseT/Half 10baseT/Full
                        100baseT/Half 100baseT/Full
                        1000baseT/Full
Advertised pause frame use: Symmetric Receive-only
Advertised auto-negotiation: Yes
Link partner advertised link modes:  10baseT/Half 10baseT/Full
                                     100baseT/Half 100baseT/Full
                                     1000baseT/Full
Link partner advertised pause frame use: Symmetric Receive-only
Link partner advertised auto-negotiation: Yes
Speed: 1000Mb/s
Duplex: Full
Auto-negotiation: on
                       drv probe link
Link detected: yes
```

Figure 2.9 The module info tool provides detailed diagnostic information

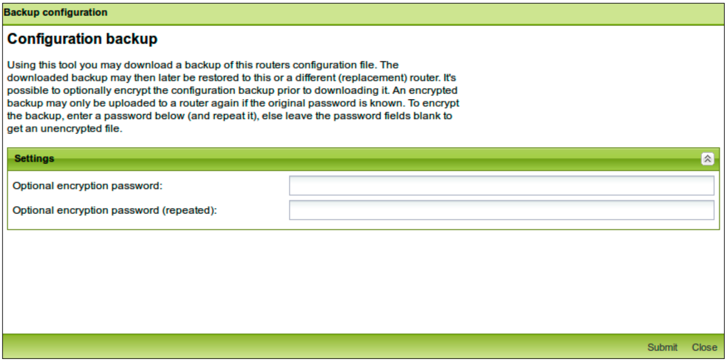


Ethernet ARP table tool

ARP table for Slot 1 - Fast Ethernet

```
192.168.110.82   00:30:18:a3:b7:40
192.168.110.254  00:0d:88:cc:a6:90
```

Figure 2.10 Ethernet ARP table tool. Used to see which IP addresses are associated with which MAC addresses. Appears in the following menus: Ethernet and DSL modules; WAN settings; LAN settings; LAN IP address aliases



Backup configuration

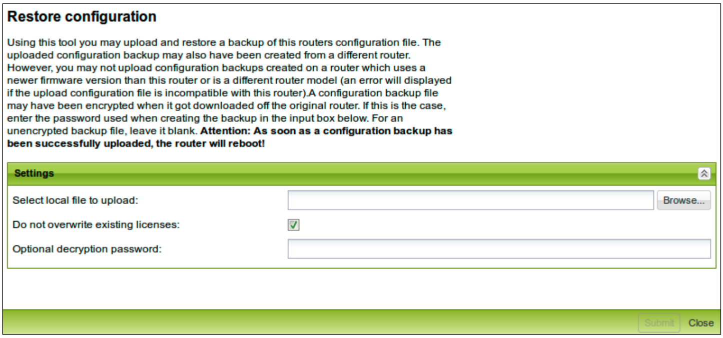
Configuration backup

Using this tool you may download a backup of this routers configuration file. The downloaded backup may then later be restored to this or a different (replacement) router. It's possible to optionally encrypt the configuration backup prior to downloading it. An encrypted backup may only be uploaded to a router again if the original password is known. To encrypt the backup, enter a password below (and repeat it), else leave the password fields blank to get an unencrypted file.

Settings

Optional encryption password:	
Optional encryption password (repeated):	

Figure 2.11 Configuration backup. Use this tool to create files that can be used to copy configuration settings from one router to another and for backup purposes. Accessible in the Logging and maintenance menu.



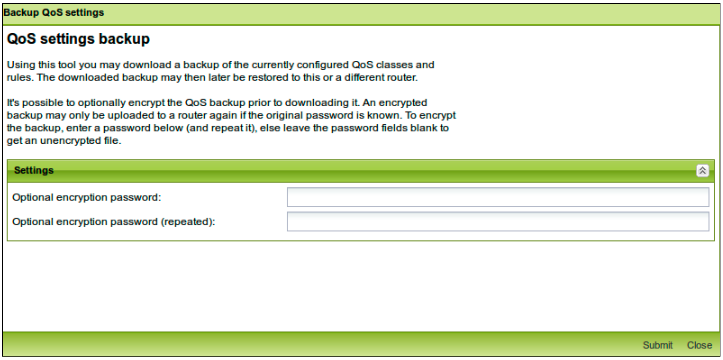
Restore configuration

Using this tool you may upload and restore a backup of this routers configuration file. The uploaded configuration backup may also have been created from a different router. However, you may not upload configuration backups created on a router which uses a newer firmware version than this router or is a different router model (an error will displayed if the upload configuration file is incompatible with this router).A configuration backup file may have been encrypted when it got downloaded off the original router. If this is the case, enter the password used when creating the backup in the input box below. For an unencrypted backup file, leave it blank. **Attention: As soon as a configuration backup has been successfully uploaded, the router will reboot!**

Settings

Select local file to upload:	Browse...
Do not overwrite existing licenses:	☑
Optional decryption password:	

Figure 2.12 Restore configuration. You can use this tool to reconfigure a router that has been reset or copy settings from one router to another. To avoid deleting existing licenses, tick the box "Do not overwrite existing licenses."



Backup QoS settings

QoS settings backup

Using this tool you may download a backup of the currently configured QoS classes and rules. The downloaded backup may then later be restored to this or a different router.

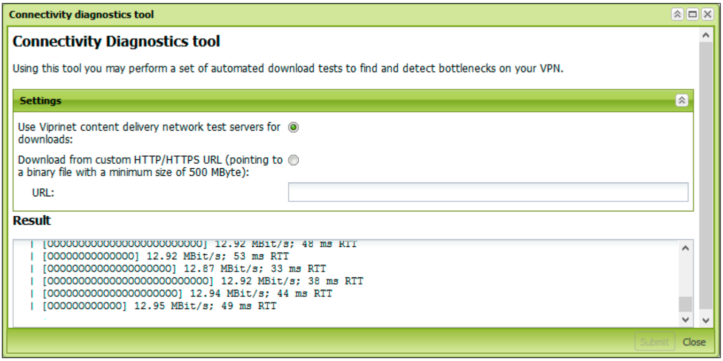
It's possible to optionally encrypt the QoS backup prior to downloading it. An encrypted backup may only be uploaded to a router again if the original password is known. To encrypt the backup, enter a password below (and repeat it), else leave the password fields blank to get an unencrypted file.

Settings

Optional encryption password:

Optional encryption password (repeated):

Figure 2.13 Quality of Service settings backup. Use this tool to create files that can be used to copy QoS settings from one router to another, as well as for backup purposes. Accessible from the VPN clients, Segmented VPN clients, Tunnel, and QoS rules and classes templates menus



Connectivity diagnostics tool

Connectivity Diagnostics tool

Using this tool you may perform a set of automated download tests to find and detect bottlenecks on your VPN.

Settings

Use Viprinet content delivery network test servers for downloads: ●

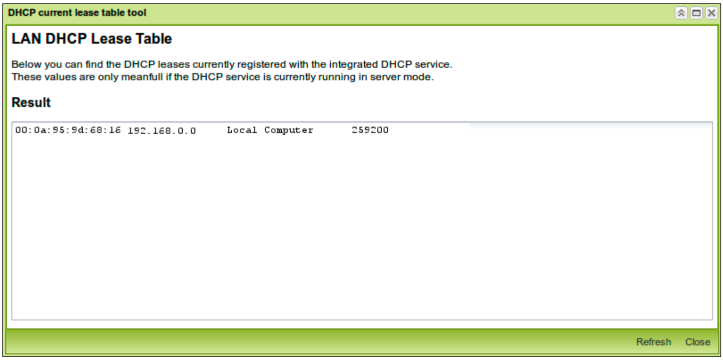
Download from custom HTTP/HTTPS URL (pointing to a binary file with a minimum size of 500 MByte): ○

URL:

Result

```
  | [0000000000000000000000000] 12.92 MBit/s; 48 ms RTT
  | [00000000000000] 12.92 MBit/s; 53 ms RTT
  | [00000000000000000000] 12.87 MBit/s; 33 ms RTT
  | [00000000000000000000000000] 12.92 MBit/s; 38 ms RTT
  | [000000000000000000000] 12.94 MBit/s; 44 ms RTT
  | [000000000000] 12.95 MBit/s; 49 ms RTT
    .
```

Figure 2.14 Connectivity Diagnostics. An O in the output progress bar means that data was received, while a period means no packets were received for 50ms. This can indicate packet loss. Accessible from the Logging and maintenance menu.



DHCP current lease table tool

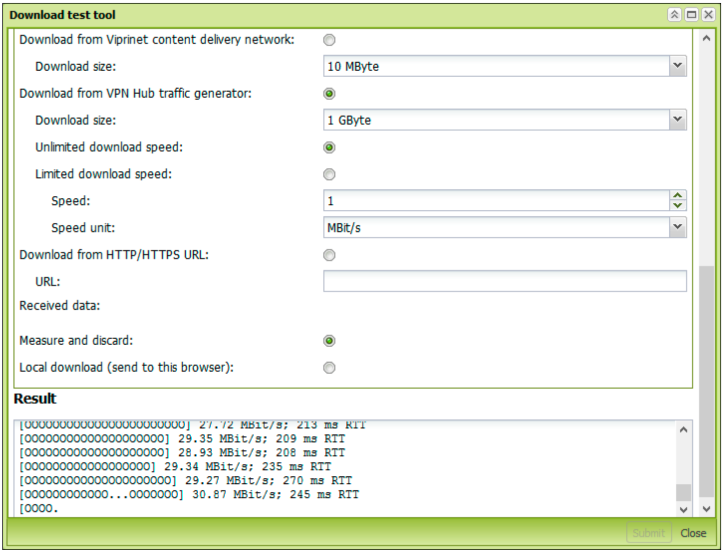
LAN DHCP Lease Table

Below you can find the DHCP leases currently registered with the integrated DHCP service.
These values are only meanfull if the DHCP service is currently running in server mode.

Result

```
00:0a:95:9d:68:16 192.168.0.0      Local Computer      259200
```

Figure 2.15 Lists DHCP associations this Node's network; accessible from DHCP server settings.



Download test tool

Download from Viprinet content delivery network: ○

Download size: 10 MByte

Download from VPN Hub traffic generator: ●

Download size: 1 GByte

Unlimited download speed: ●

Limited download speed: ○

Speed: 1

Speed unit: MBit/s

Download from HTTP/HTTPS URL: ○

URL:

Received data:

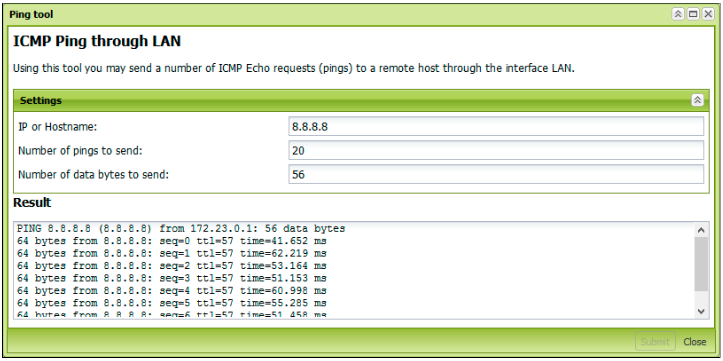
Measure and discard: ●

Local download (send to this browser): ○

Result

```
[000000000000000000000000] 27.72 MBit/s; 213 ms RTT
[00000000000000000000] 29.35 MBit/s; 209 ms RTT
[00000000000000000000] 28.93 MBit/s; 208 ms RTT
[000000000000000000] 29.34 MBit/s; 235 ms RTT
[000000000000000000000] 29.27 MBit/s; 270 ms RTT
[000000000000...0000000] 30.87 MBit/s; 245 ms RTT
[0000.
```

Figure 2.16 Download test. This tool can be accessed from all module menus as well as WAN settings and LAN settings. It is used to test the speed of individual channels in the VPN tunnel as they operate without QoS settings, unlike the Connectivity Diagnostics tool, which operates on the tunnel level. An 0 in the output progress bar means that data was received within the past 50ms. A . (period) means no packets were received for the same length of time; this can indicate packet loss. Can be accessed from all module type menus as well as the WAN settings and LAN settings menu.



Ping tool

ICMP Ping through LAN

Using this tool you may send a number of ICMP Echo requests (pings) to a remote host through the interface LAN.

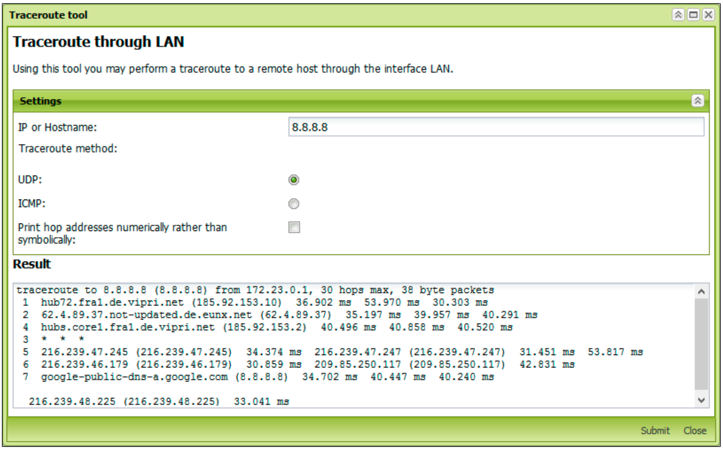
Settings

IP or Hostname:	8.8.8.8
Number of pings to send:	20
Number of data bytes to send:	56

Result

```
PING 8.8.8.8 (8.8.8.8) from 172.23.0.1: 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=57 time=41.652 ms
64 bytes from 8.8.8.8: seq=1 ttl=57 time=62.219 ms
64 bytes from 8.8.8.8: seq=2 ttl=57 time=53.164 ms
64 bytes from 8.8.8.8: seq=3 ttl=57 time=51.153 ms
64 bytes from 8.8.8.8: seq=4 ttl=57 time=60.998 ms
64 bytes from 8.8.8.8: seq=5 ttl=57 time=55.285 ms
64 bytes from 8.8.8.8: seq=6 ttl=57 time=51.458 ms
```

Figure 2.17 Ping tool. This tool helps you identify whether individual modules are connected to the internet and can reach specific domains. It is accessible from all module type menus as well as WAN and LAN settings menus.



Traceroute tool

Traceroute through LAN

Using this tool you may perform a traceroute to a remote host through the interface LAN.

Settings

IP or Hostname: 8.8.8.8

Traceroute method:

UDP: ●

ICMP: ○

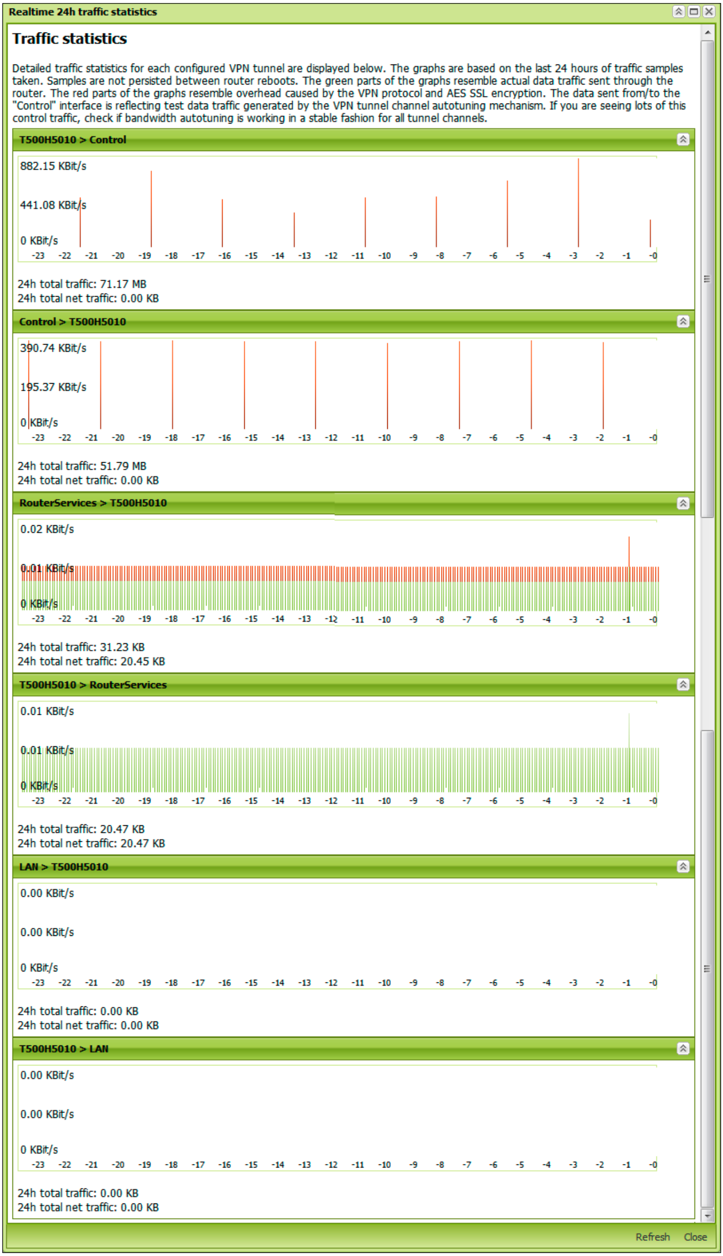
Print hop addresses numerically rather than symbolically: □

Result

```
traceroute to 8.8.8.8 (8.8.8.8) from 172.23.0.1, 30 hops max, 38 byte packets
 1  hub72.fra1.de.vipri.net (185.92.153.10)  36.902 ms  53.970 ms  30.303 ms
 2  62.4.89.37.not-updated.de.eunx.net (62.4.89.37)  35.197 ms  39.957 ms  40.291 ms
 4  hubs.core1.fra1.de.vipri.net (185.92.153.2)  40.496 ms  40.858 ms  40.520 ms
 3  *  *  *
 5  216.239.47.245 (216.239.47.245)  34.374 ms  216.239.47.247 (216.239.47.247)  31.451 ms  53.817 ms
 6  216.239.46.179 (216.239.46.179)  30.859 ms  209.85.250.117 (209.85.250.117)  42.831 ms
 7  google-public-dns-a.google.com (8.8.8.8)  34.702 ms  40.447 ms  40.240 ms

  216.239.48.225 (216.239.48.225)  33.041 ms
```

Figure 2.18 Traceroute tool. This utility displays the number of transfers from router to router (hops) between the Node or Hub where you are running this tool and a given IP address or hostname. The more hops between your router and the host, the longer a packet will take to travel the distance between them. It can be accessed from all module menus, WAN settings and LAN settings menus.



Realtime 24h traffic statistics

Traffic statistics

Detailed traffic statistics for each configured VPN tunnel are displayed below. The graphs are based on the last 24 hours of traffic samples taken. Samples are not persisted between router reboots. The green parts of the graphs resemble actual data traffic sent through the router. The red parts of the graphs resemble overhead caused by the VPN protocol and AES SSL encryption. The data sent from/to the "Control" interface is reflecting test data traffic generated by the VPN tunnel channel autotuning mechanism. If you are seeing lots of this control traffic, check if bandwidth autotuning is working in a stable fashion for all tunnel channels.

T500H5010 > Control

24h total traffic: 71.17 MB
24h total net traffic: 0.00 KB

Control > T500H5010

24h total traffic: 51.79 MB
24h total net traffic: 0.00 KB

RouterServices > T500H5010

24h total traffic: 31.23 KB
24h total net traffic: 20.45 KB

T500H5010 > RouterServices

24h total traffic: 20.47 KB
24h total net traffic: 20.47 KB

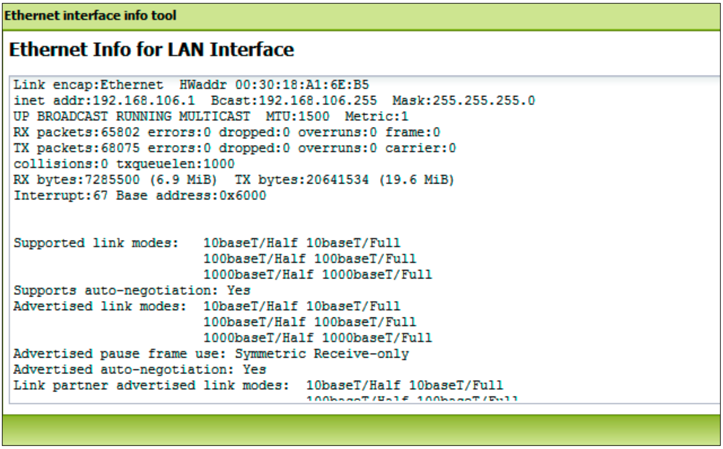
LAN > T500H5010

24h total traffic: 0.00 KB
24h total net traffic: 0.00 KB

T500H5010 > LAN

24h total traffic: 0.00 KB
24h total net traffic: 0.00 KB

Figure 2.19 Traffic statistics tool



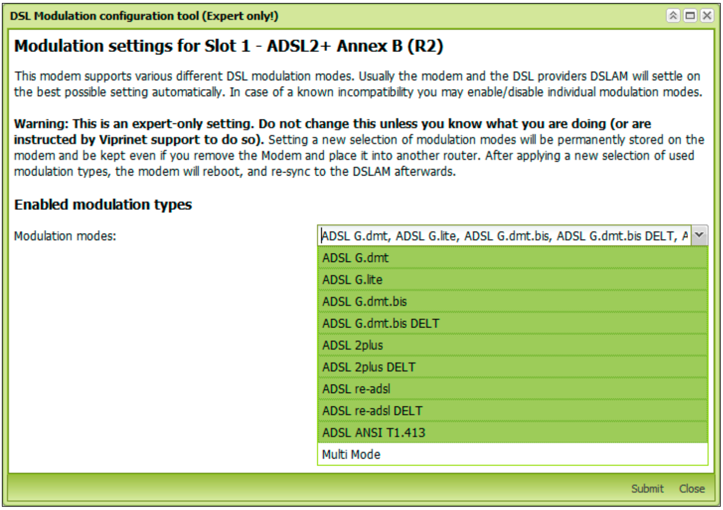
Ethernet interface info tool

Ethernet Info for LAN Interface

```
Link encap:Ethernet  HWaddr 00:30:18:A1:6E:B5
inet addr:192.168.106.1  Bcast:192.168.106.255  Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:65802 errors:0 dropped:0 overruns:0 frame:0
TX packets:68075 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:7285500 (6.9 MiB)  TX bytes:20641534 (19.6 MiB)
Interrupt:67 Base address:0x6000


Supported link modes:   10baseT/Half 10baseT/Full
                        100baseT/Half 100baseT/Full
                        1000baseT/Half 1000baseT/Full
Supports auto-negotiation: Yes
Advertised link modes:  10baseT/Half 10baseT/Full
                        100baseT/Half 100baseT/Full
                        1000baseT/Half 1000baseT/Full
Advertised pause frame use: Symmetric Receive-only
Advertised auto-negotiation: Yes
Link partner advertised link modes:  10baseT/Half 10baseT/Full
                                     100baseT/Half 100baseT/Full
```

Figure 2.20 The Ethernet Interface info tool, found in the LAN settings menu



DSL Modulation configuration tool (Expert only!)

Modulation settings for Slot 1 - ADSL2+ Annex B (R2)

This modem supports various different DSL modulation modes. Usually the modem and the DSL providers DSLAM will settle on the best possible setting automatically. In case of a known incompatibility you may enable/disable individual modulation modes.

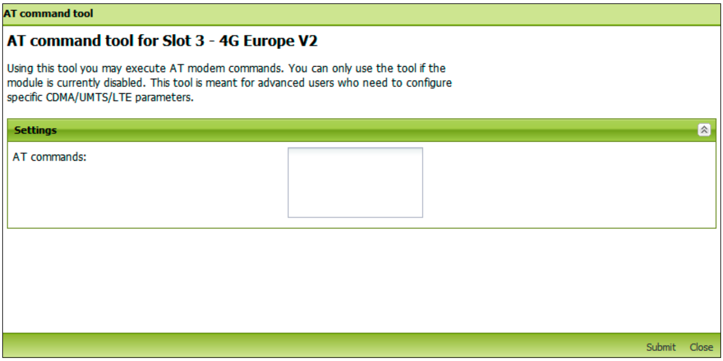
Warning: This is an expert-only setting. Do not change this unless you know what you are doing (or are instructed by Viprinet support to do so). Setting a new selection of modulation modes will be permanently stored on the modem and be kept even if you remove the Modem and place it into another router. After applying a new selection of used modulation types, the modem will reboot, and re-sync to the DSLAM afterwards.

Enabled modulation types

Modulation modes: ADSL G.dmt, ADSL G.lite, ADSL G.dmt.bis, ADSL G.dmt.bis DELT, A

- ADSL G.dmt
- ADSL G.lite
- ADSL G.dmt.bis
- ADSL G.dmt.bis DELT
- ADSL 2plus
- ADSL 2plus DELT
- ADSL re-adsl
- ADSL re-adsl DELT
- ADSL ANSI T1.413
- Multi Mode

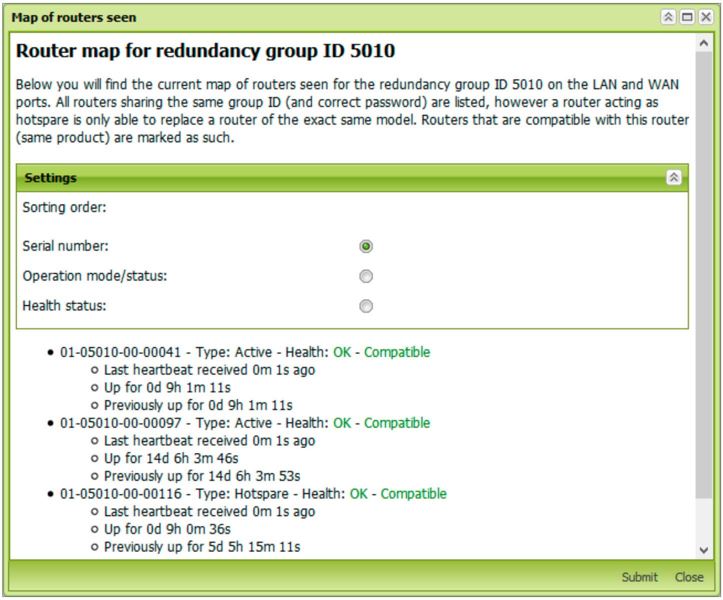
Figure 2.21 DSL Modulation Tool, only found in ADSL module menus



AT command tool for Slot 3 - 4G Europe V2

Using this tool you may execute AT modem commands. You can only use the tool if the module is currently disabled. This tool is meant for advanced users who need to configure specific CDMA/UMTS/LTE parameters.

Figure 2.22 AT Command Tool. This tool only appears in disabled LTE module menus. The relevant commands vary from module type to module type depending on the vendor. Contact Support for a list of commands for your module.



Router map for redundancy group ID 5010

Below you will find the current map of routers seen for the redundancy group ID 5010 on the LAN and WAN ports. All routers sharing the same group ID (and correct password) are listed, however a router acting as hotspare is only able to replace a router of the exact same model. Routers that are compatible with this router (same product) are marked as such.

Settings

Sorting order:

Serial number: ●

Operation mode/status: ○

Health status: ○

- 01-05010-00-00041 - Type: Active - Health: OK - Compatible
  - Last heartbeat received 0m 1s ago
  - Up for 0d 9h 1m 11s
  - Previously up for 0d 9h 1m 11s
- 01-05010-00-00097 - Type: Active - Health: OK - Compatible
  - Last heartbeat received 0m 1s ago
  - Up for 14d 6h 3m 46s
  - Previously up for 14d 6h 3m 53s
- 01-05010-00-00116 - Type: Hotspare - Health: OK - Compatible
  - Last heartbeat received 0m 1s ago
  - Up for 0d 9h 0m 36s
  - Previously up for 5d 5h 15m 11s

Figure 2.23 Map of routers seen. This tool can be found in the Redundancy menu on Hubs.

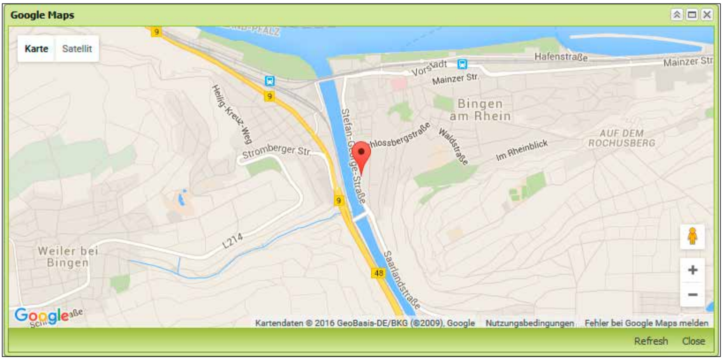


Figure 2.24 Google Maps tool, found in the GEO Tracking menu

2.5.3 Technical requirements

In order to access all of the AdminDesk's features, you need a browser released within the past five years that has Javascript enabled.

2.6 Viprinet Monitor

This tool is used to keep track of the status of three different connection types

- VPN tunnels
- Modules and channels—including signal quality and band info for wireless modems
- VPN Client sessions

2.6.0 Creating an account

The *Manage Accounts* menu includes the options *New Account, Edit Account*, and *Delete Account*.

To create a new account you'll need to enter:

- Account name
  - A name for the account so you can find it in the dropdown list
- Host
  - IP address of the device you are connecting to; you'll need to have administrator privileges
- Username
  - Your username on the device you are connecting to
- Password
  - Your password on the device you are connecting to

Select a data view in the dropdown; available options are:

- *Ask on connect* – a pop-up window will let you select what to do when you connect
- *VPN tunnel (Node or Hub)* – You will see data for a VPN tunnel
- *VPN client (Hub only)* – You will see data for VPN client connections
- *Module slots (Node only)* – You will see data for the module slots in your Node

2.6.1 Connecting

Select a configured account in the dropdown. Click *Connect.*

If you have specified the *Ask on connect* option for data view, a pop-up window will appear prompting you to select a source. The options here are the same three standard views listed in the account setup menu.

⚠ **Attention**
If the IP address you are connecting to includes a port forwarding value (e.g. :8888) you can't use the „Ask on connect" option. Instead, you must set the data view to *Tunnel*.

In module slots mode you will have access to the following tabs; all but three show waveform traces:

- Link stability (in percent)
  - Shows a list rather than a waveform
  - A list of channels and how reliable they are
- Maximum allowed bandwidth from WAN (in Kbit/s)
  - Maximum traffic incoming from the Hub
- Maximum allowed bandwidth to WAN (in Kbit/s)
  - Maximum traffic outgoing to the Hub
- Maximum allowed latency (in ms)
  - Shows a list rather than a waveform
  - Displays latency values set for each channel in the AdminDesk or by autotuning
- Packet loss (in percent)
  - The smaller these waveforms are, the better
- Status
  - Shows a list rather than a waveform
  - Indicates whether channels are connected or inactive
- Tunnel info
  - Shows a several traces on the same screen
    - Current total channel bandwidth from WAN (Kbit/s)
    - to WAN
    - Fastest from
    - Fastest to
    - Fastest reliable
- Current bandwidth from WAN (in Kbit/s)
  - by channel
- Current bandwidth to WAN (in Kbit/s)
  - By channel
- Current latency
  - By channel

In VPN Tunnel mode, one tab is accessible; it lists

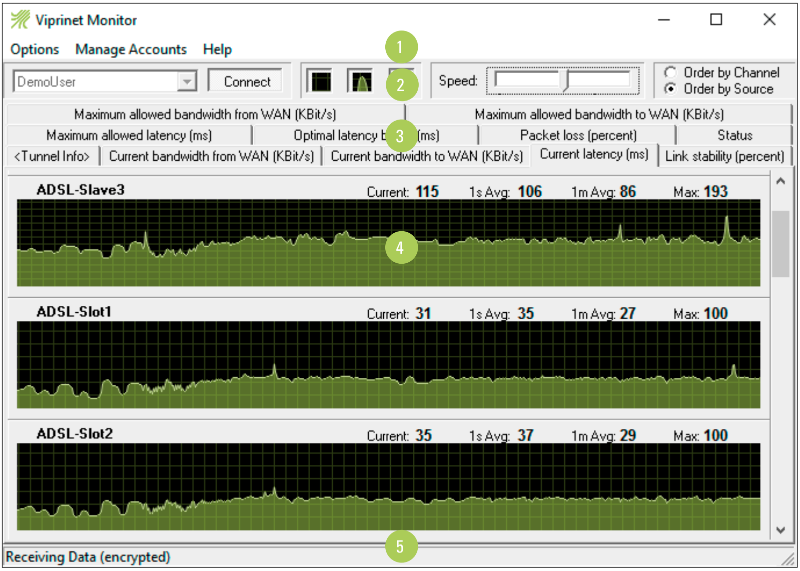
- connected channels
- current total channel bandwidth from WAN
- most reliable channel bandwidth to WAN
- most reliable channel bandwidth from WAN
- fastest channel bandwidth from WAN
- fastest channel bandwidth to WAN
- fastest reliable bandwidth to WAN

- fastest reliable bandwidth from WAN
- total reliable bandwidth to WAN
- total reliable bandwidth from WAN

To access VPN Client mode, you need administrator access to the Hub with which the accounts are associated. You can view all of your active users.

2.6.2 GUI Anatomy

As shown in figure 2.25, this tool has three dropdown menus, a toolbar, a monitor window, and a status bar, along with viewing tabs that vary by the mode selected and only appear when the tool is active.



ADSL-Slave3 Current: 115 1s Avg: 106 1m Avg: 86 Max: 193

ADSL-Slot1 Current: 31 1s Avg: 35 1m Avg: 27 Max: 100

ADSL-Slot2 Current: 35 1s Avg: 37 1m Avg: 29 Max: 100

Receiving Data (encrypted)

Figure 2.25 Viprinet Monitor
1. Dropdown menus; 2. Toolbar; 3. View tabs; 4. Monitor window; 5. Status bar

At the top right, there are two radio buttons for organizing the readouts in the monitor:

- Order by Channel
- Order by Source

The three dropdown menus are *Options*, *Manage Accounts*, and *Help*.

The *Options* menu is structured as follows:

- Options
  - Connect/Disconnect (this refers to the channel you are monitoring)
    - Connect
    - Module Status shows detailed information for each module

    - VPN tunnels
    - VPN clients
  - Settings (these attributes refer to the appearance of the monitoring grids)
    - Show Grid (allows you to precisely measure curve deltas)
    - Interpolation (calculate and add in data points so you can zoom in manually)
    - Auto- (zoom in automatically when you change the size of the monitor window)
    - Scroll speed (the speed with which the tracking graph moves off the screen)
    - Very fast
    - Fast
    - Medium
    - Slow
    - Very slow
  - Exit (quit software)

The *Manage Accounts* menu has already been described.

The *Help* menu is empty, except for the item *About*, which leads to information about the version of the tool you are using.

The items on the toolbar include:

- A dropdown for selecting accounts, with a Connect button
- Buttons that duplicate items from the Settings list
  - Show Grid
  - Interpolation
  - Auto-
  - Speed

The status bar is at the bottom of the Monitor window and indicates the state of the tool. If it is not being used, it reads *Idle*. Other states include:

- Connecting
- Receiving data

2.6.3 System requirements

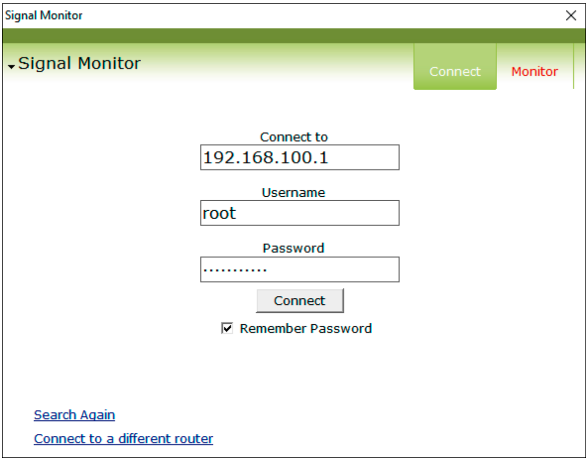
Windows Vista, 7, 8, or 10.

2.7 Viprinet Signal Monitor

This tool makes it possible to assess the strength of wireless signal connections to six providers at once.

2.7.0 GUI Anatomy

The tool includes two tabs, *Connect* and *Monitor*, and a dropdown menu that appears when you click the down arrow next to the software name, at the top left of the window.



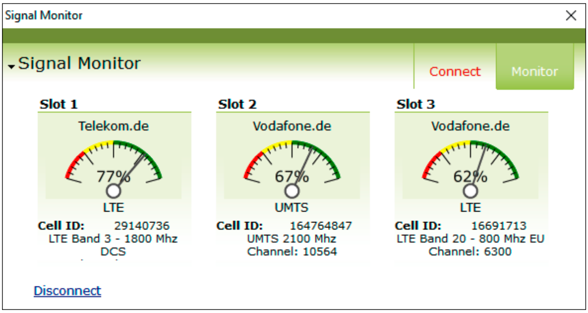
Connect to: 192.168.100.1

Username: root

Password: ....

☑ Remember Password

Figure 2.26 The Signal Monitor Connection Screen



Slot 1
Telekom.de
77%
LTE
Cell ID: 29140736
LTE Band 3 - 1800 Mhz
DCS

Slot 2
Vodafone.de
67%
UMTS
Cell ID: 164764847
UMTS 2100 Mhz
Channel: 10564

Slot 3
Vodafone.de
62%
LTE
Cell ID: 16691713
LTE Band 20 - 800 Mhz EU
Channel: 6300

Figure 2.27 Monitoring Screen

When you first open the software, it will display the Connect tab and the message “Searching for router”. If you are not connected to a Viprinet Node or Hub either via your computer’s ethernet interface or a local LAN, the message “No router was found, please enter target host” will appear, and you can connect to a remote Node or Hub if you have its IP address and a username and password for it. The software can save your password if you wish.

The *Monitor* tab displays each active wireless connection on your Node, to a maximum of six.

Each listing includes

- the name of the provider
- the type of connection
  - its status
- the cell ID
- the frequency band
- the channel assigned
- the signal quality
- a graphical “speedometer” needle

The “speedometer” shows the signal strength the mobile connection is operating at as a percentage. There is a *Disconnect* link on the bottom left hand corner of the screen.

The dropdown menu includes the following commands:

- Connect
- Search for routers
- Advanced
  - Clear Password Cache
  - About
- Quit

2.7.1 System requirements

Windows Vista, 7, 8, or 10.

2.8 VPN Client

The VPN Client is a user-friendly way for remote users to access internal resources by connecting to a tunnel from your network. Appendix 7 describes how to install and set up your VPN client software.

2.8.0 GUI Anatomy

As shown in figure 2.29, this tool has three dropdown menus and four tabs.

The three dropdown menus are *File, View,* and *Help*.

The *File* menu includes

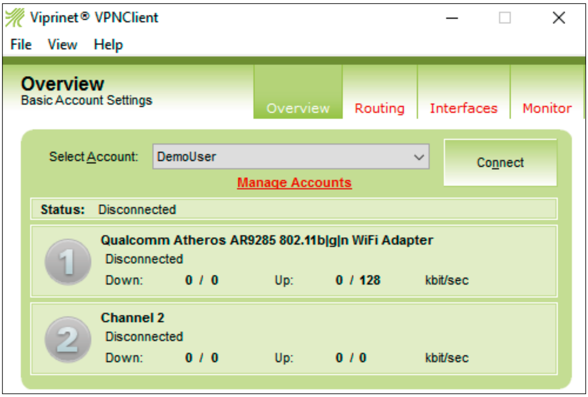
- Connect
- Account Settings (which brings you to the same menu as the Manage Accounts link)
- Quit

The *View* menu allows you to navigate between the tabs, just as you can by clicking them

- Overview
- Routing
- Interfaces, which in this context means your network connections and the devices used to access them
- Monitor

The *Help* menu includes

- About



Select Account: DemoUser

Status: Disconnected

Qualcomm Atheros AR9285 802.11b|g|n WiFi Adapter
Disconnected
Down: 0 / 0 Up: 0 / 128 kbit/sec

Channel 2
Disconnected
Down: 0 / 0 Up: 0 / 0 kbit/sec

Figure 2.28 Overview tab

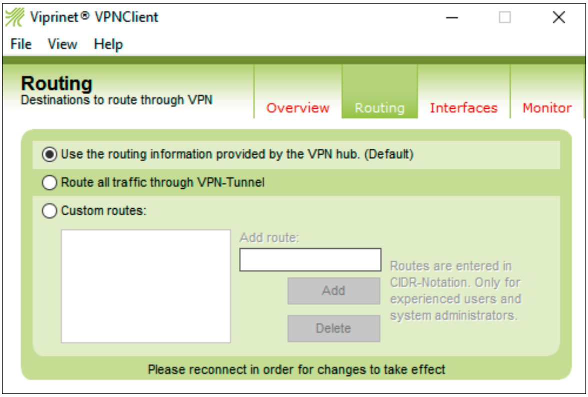
The *Overview* tab allows the user to

- select an account to connect with
- edit the accounts available
- manage which channels are being used to establish a VPN connection
- Connect and disconnect

It also includes a status line that indicates whether the user is connected or not and a list of the connections being used.

Connections are listed by priority, and non-active connections' are gray. Active connections' numbers are green.

The *Manage accounts* menu includes two tabs. The first, *Account Management*, is a list of accounts, with their name, username, password, and target Hub associated with them. The second, *Startup* has a checkbox that you can tick to indicate the client should connect to whichever account is selected in the dropdown. There's another box you can tick to specify that the client should stay minimized in your toolbar when it starts.



● Use the routing information provided by the VPN hub. (Default)

○ Route all traffic through VPN-Tunnel

○ Custom routes:

Routes are entered in CIDR-Notation. Only for experienced users and system administrators.

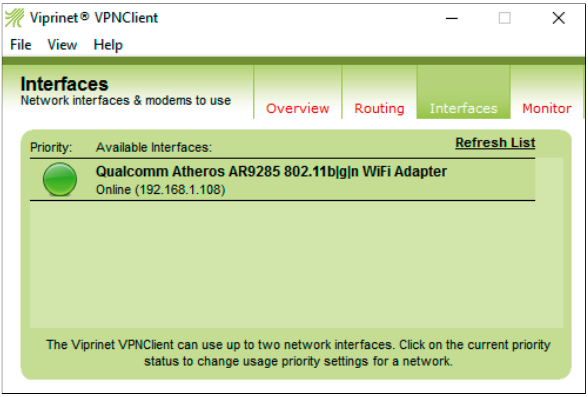
Please reconnect in order for changes to take effect

Figure 2.29 Routing tab

Controls in the *Routing* tab are only usable if *Allow* Clien*t to override routing settings* is enabled in the *VPN Client settings* menu on the Hub. Otherwise, the radio button next to *Use the Routing Information Provided by the VPN Hub* will be selected. Route all traffic through VPN tunnel will send all packets into a VPN tunnel between the client machine and the Hub. *Custom Routes* allows you to designate other specific locations the client will connect to.

Keep in mind

Each time the VPN Client starts, the routing is reset according to the client account configuration on the Hub, no matter how these settings may have been changed the last time the Client was active.



Qualcomm Atheros AR9285 802.11b|g|n WiFi Adapter
Online (192.168.1.108)

The Viprinet VPNClient can use up to two network interfaces. Click on the current priority status to change usage priority settings for a network.

Figure 2.30 Interfaces tab

The *Interfaces* menu lists the hosts connecting to channels that have been established, as well as their priority. It also includes a *Refresh List* button to allow you to update the view as needed.

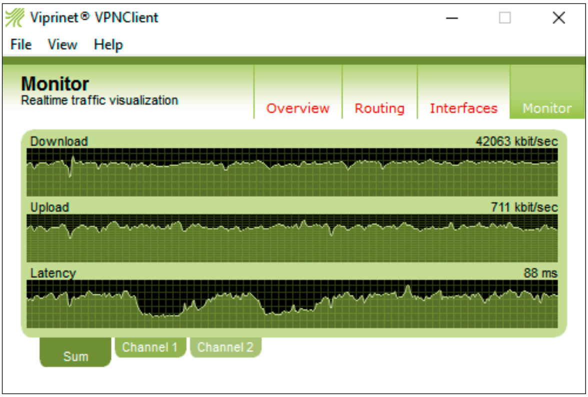


Figure 2.31 Monitor tab

The readouts on the Monitor tab are used to keep track of the upload and download speeds for the user's connection, along with latency. These figures are measured in seconds. The Monitor can display either each individual channel or the sum of all bonded channels.

2.8.1 System requirements

The VPN Client requires Windows Vista, 7, 8, or 10. The Mac version will run natively on OS X versions 10.6 through 10.9 as of this writing. It is possible to run the Client under emulation using VMWare, Parallels, or VirtualBox, but this is not supported by Viprinet. It is not possible to run the Client using Wine or the emulator QEMU given the way those tools interface with the computer's OS.

2.8.2 Troubleshooting

If the VPN Client is having trouble connecting, before trying anything else, navigate to the program folder and double-click *Reinstall VPN Interface*. You will lose any existing connection information configured in the client and will have to re-enter it. To view the logfile for the client in aid of troubleshooting, open the GUI and type CTRL+ALT+L.

Chapter 3. Software installation

You can get the setup tool, VPN client, Monitor, and Signal Monitor on your computer in one of two ways:

- Copy them from the disc you receive with your hardware
  or
- Download them from the Viprinet website at: http://www.viprinet.com/en/support/downloads.

The AdminDesk software is always available on your router, and you will access it from your computer via a browser after you have run the setup tool.

3.0 Setup tool

This tool can only be run on Windows XP, Vista, 7, 8, or 10. It is possible to run it under Wine, but that is not supported by Viprinet. If you have downloaded the setup tool from the website, double-click on its icon to run it. If you are using a CD or ISO, a welcome menu will automatically appear; click the Setup Tool link. Section 4.0.9 discusses how to use the setup tool to configure your Node or Hub.

3.1 Viprinet Monitor and Viprinet Signal Monitor

The Monitor and Signal Monitor require Windows Vista, 7, 8, or 10. These two pieces of monitoring software have a very simple installation process: just drag them onto your computer from the disc, or unpack the zip file you have downloaded, and they are ready to use. The connection monitor is called monitor.exe, and the wireless signal monitor is called SignalMonitor.exe. Use this tool to see signal strengths for a variety of wireless media.

Both monitors' system requirements and their GUI anatomy are described in Chapter 2. For the Monitor, see section 2.6. For the Signal Monitor, see section 2.7.

3.2 VPN Client

The VPN Client requires Windows Vista, 7, 8, or 10. To install the VPN Client, double-click its icon in the unpacked archive or select the VPN Client option in the CD or ISO auto-run menu. An installation wizard will launch that will ask you where you wish to install the client, and if you want to create a shortcut for it. The wizard will also install a virtual network interface for the tunnel.

You must either be logged in as an administrator or enter your administrator password when prompted to install the software. Unless the Client has be configured to start on system boot, you should be also be prompted to enter your administrator password when starting it up. For more on this see “Keep in mind”, in section 2.8. This section also describes the VPN client GUI and administrator settings. A guide to the VPN Client software for non-administrative users is provided in Appendix 7.

Chapter 4. Setup

If you are not sure what the terms Node and Hub mean, you should start by reading Chapter 2.
This section includes a quickstart guide and more advanced setup instructions.

4.0 Quickstart guide

This reference for standard Node (local router) configuration is suitable for help desk and non-IT staff. Some elements of this tutorial are specific to our most popular router model series. For information on configuring additional Node and module types, see section 4.1.0.

This guide will be useful to you if you are:
- configuring a 300, 511, or 512 model Node (our most popular units as of this writing)
- using a computer running Windows XP, Vista, 7, 8, or 10
- connecting the device directly to your computer via one of its ethernet connections

4.0.0 Advanced configuration guidance

If you are configuring:
- your Node in another way (e.g. over a network)
- different module types
- a Hub (central router)
- or need to enable advanced functions

contact your network engineer(s) for assistance. If you do not have a network engineer on staff, please ask your vendor for support. If you are a network engineer, see section 4.1 through 5 for information about most of these scenarios; section 6.9 covers stacking.

4.0.1 Overview

There are 8 stages in the process of setting up your router:
- Getting the information and tools you need
- Attaching the antennas
- Inserting your SIM cards
- Plugging your router into your computer
- Turning on your router
- Installing the Setup Tool
- Resolving security alerts
- Running the Setup Tool to configure the unit
- Finishing configuration in the AdminDesk

4.0.2 Getting the information and tools you need to set up your router

You will need the following pieces of information before you configure the device:

Software	Where to get it
The Viprinet Setup Tool	From the Viprinet website. See step 6.

Hardware	Where to get it
An ethernet cable to connect your computer to the router	Your network engineer(s) or any reputable computing vendor
A Phillips head screwdriver, gauge PH1, to open the SIM card slot in the device	Your network engineer(s) or any reputable hardware store or computing vendor
Your router and the peripherals provided with it (especially antennas and power cables)	Your vendor

System access	Where to get it
• Access to a pre-configured Hub (central router) • A VPN tunnel that has been configured on that Hub with a number of channels matching the number of connections you will be using	Your network engineer(s) or Viprinet certified service provider
Administrative access to your machine, or a support person with that access, to: • Run the Setup software • modify your Windows firewall settings so you can connect the router you are configuring to your computer	If you do not have this access, contact your IT support office so they can assist you

Information about your Node (local router)	Where to get it
An IP subnet	Your network engineer(s), vendor, or Viprinet certified service provider
A netmask	Same as above
The name you would like to assign, which should provide helpful information about the router, e.g. NewYorkOffice. Do not use passwords as names.	Your network engineer(s)—or choose a name yourself
A password you will use to access the router's AdminDesk (web-based administration tool)	Your network engineer(s)—or choose a password yourself
LAN IP address; this is the address you will go to when you need to use your router's AdminDesk	Your network engineer(s), ISP, or Viprinet certified service provider
LAN netmask	Same as above
DNS hostname	Same as above
WAN IP address	Same as above
WAN netmask	Same as above

Note: WAN IP address and WAN netmask settings are only needed when Ethernet Modules with a Static IP address configuration are used. Providers assign other module IP addresses automatically with DHCP.

SIM cards and mobile data connection info	Where to get it
Your APN (access point name; only if auto-APN-detection doesn't work in the Setup Tool)	Your mobile wireless service provider
At least two and no more than four SIM card(s). You will use these to access mobile data connections with your router. You can also use the router's Gigabit Ethernet connection.	A mobile wireless service provider of your choice who offers affordable data plans
The PINs for the SIM cards you will be using, if applicable	Your mobile wireless service provider
Any username or password needed to use the SIM card or access mobile data (usually not in the United States)	Same as above

Hub (central router) connection info	Where to get it
Hub (central router) connection info	Where to get it
Default gateway for WAN configuration	Your network engineer(s), vendor, Viprinet licensed service provider, or ISP
The name of the VPN tunnel you will be connecting to	Your network engineer(s), vendor, or Viprinet licensed service provider
The password for the VPN tunnel	Same as above
The names of the channels in the VPN tunnel	Same as above
A QoS (Quality of Service settings) file from the Hub; QoS settings on the Node must match those on the Hub for a connection to be established; if an encryption password was used to protect these settings, you will need it as well	Same as above

Table 4.0 Preparing to configure your router

4.0.3 Attaching the antennas

This is what your router looks like:

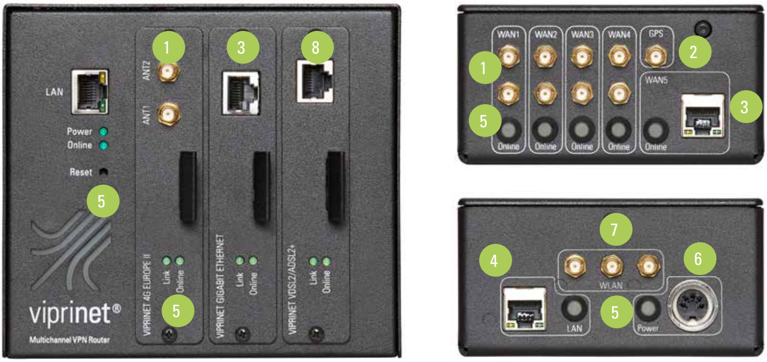


Figure 4.0 1. Mobile connections antenna sockets for 3G/4G WAN interfaces; 2. GPS antenna socket; 3. Gigabit Ethernet WAN interface; 4. LAN interface; 5. Status LEDs; 6. Power cable connector (on the back of the modular router); 7. Wireless LAN antenna sockets; 8. VDSL WAN interface

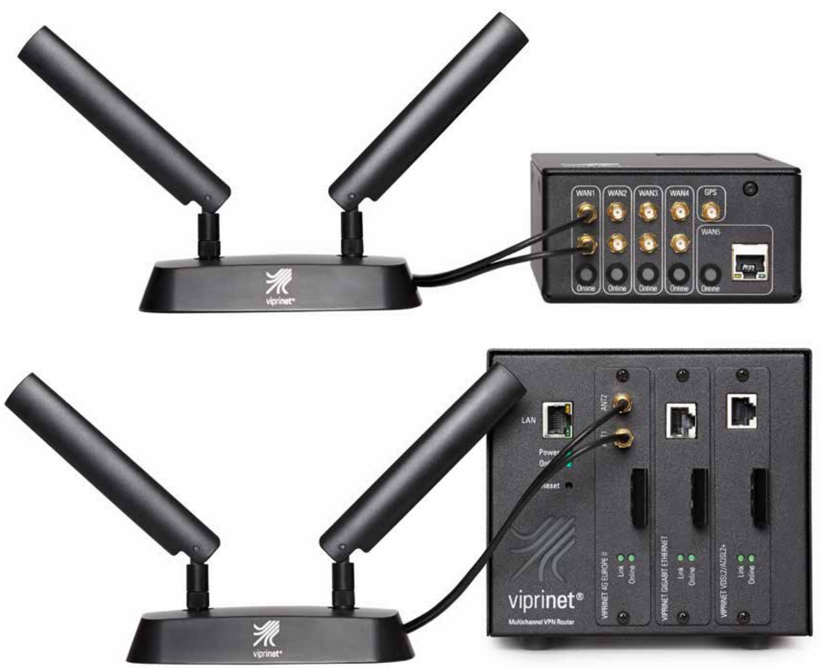


Figure 4.1 Connecting antennas to your router

To each 3G or 4G module, antenna bases and knuckle antennas are included in the router package. Screw 2 knuckle antennas into each base. You will need one base for each module. Make sure to face the antennas away from each other and unfold them at 45 degree angles, as pictured above. Connect the 2 long coaxial cords attached to the bottom of each base to a pair of WAN socket.

4.0.4 Inserting your SIM cards

Remove the SIM card module cover plate on the top of your device as pictured, using the type of screwdriver noted in the “What you need” list.

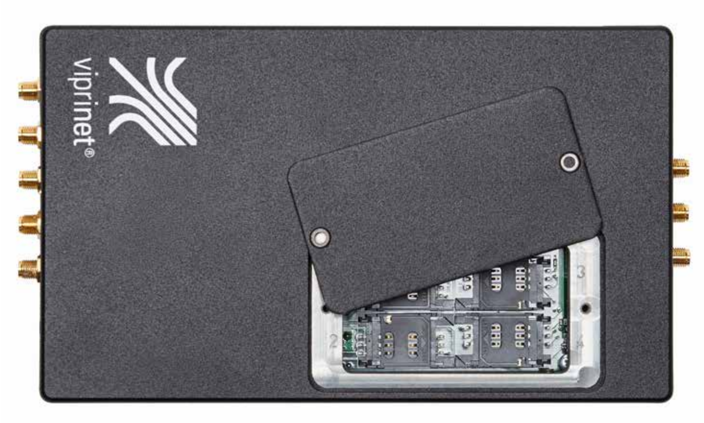


Figure 4.2 Removing the SIM module cover plate

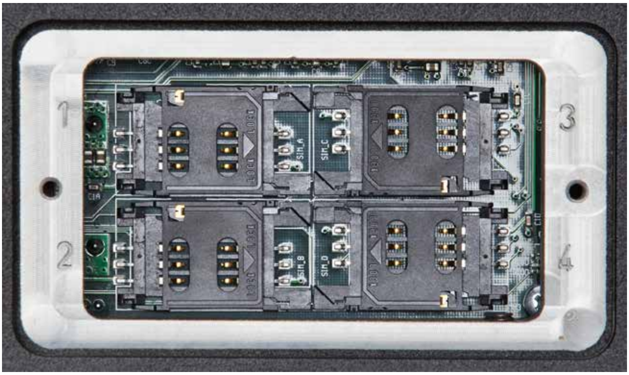


Figure 4.3 SIM modules

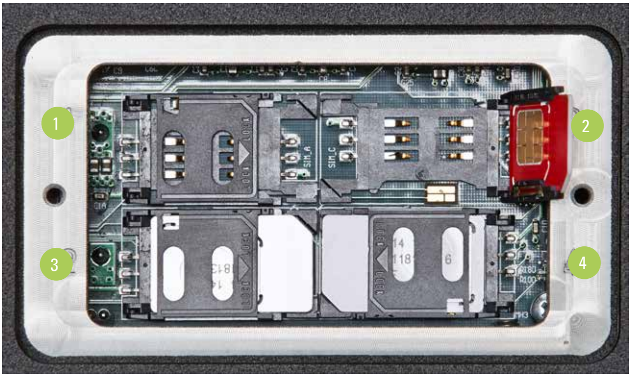


Figure 4.4 Opening and closing the SIM card slots

To open a SIM card slot, slide the lid away from the base first (1). Lift it up and put the SIM card inside as illustrated (2). To cloase the slot, fold its lid toward the bottom again (3), then press down gently and slide it back to lock it (4). Please note that the engraved numbers (1 to 4) on the silver frame belong to the four available wireless modules
4.0.5 Plugging your router into your computer

4.0.5 Turning on your router

Plug the end of the power cable into the unit's power cable connector. Plug the other end into a standard wall power outlet or car outlet with the appropriate cable. These devices are only authorized for use with the power supply supplied by Viprinet. **Never connect them to positive ground systems, such as those found in very old cars.**

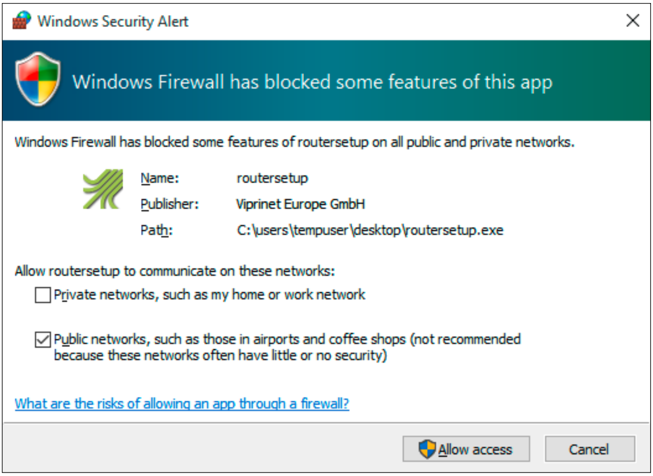
The LEDs on the LAN interface of your router should illuminate after you have connected the device to the computer. This indicates that the ethernet cable is correctly connected. If they do not illuminate, make sure that the cable is securely plugged in, or try another cable. When data is passing between your router and computer, these LEDs will start to blink. No other LEDs will illuminate on the device at this time.

4.0.6 Installing the Setup Tool

Navigate to the "Viprinet tools" portion of this page on the website: http://www.viprinet.com/downloads. Download the zip labeled "Download Viprinet tools" and double-click to open it. Drag the program labeled "Setup" to your desktop.

4.0.7 Resolving security alerts

Double-click on the Setup Tool program that you have dragged onto your desktop.
A security alert window will appear (see figure 4.9) and ask you to enter an administrator name and password. If your system will still not connect to the router after you or your IT staff enter an administrator name and password, and you are not sure how to make necessary changes, consult your operating system's documentation.



Windows Security Alert

Windows Firewall has blocked some features of this app

Windows Firewall has blocked some features of routersetup on all public and private networks.

Name: routersetup
Publisher: Viprinet Europe GmbH
Path: C:\users\tempuser\desktop\routersetup.exe

Allow routersetup to communicate on these networks:

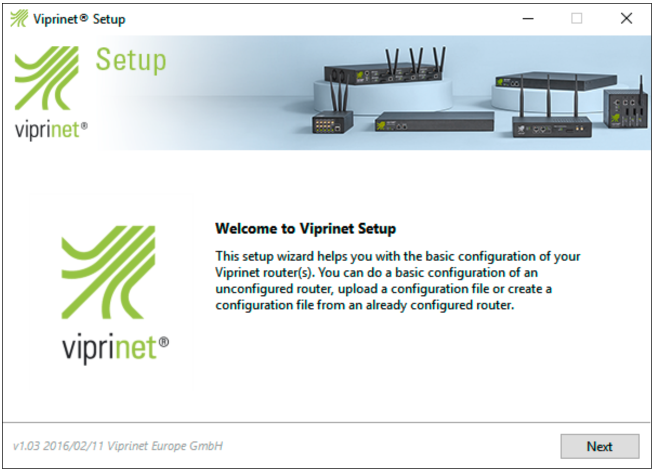
□ Private networks, such as my home or work network

☑ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

Figure 4.5 Firewall alert

4.0.8 Using the Setup Tool to configure your router

- Remember that the setup tool can only be run on Windows XP, Vista, 7, 8, or 10.
- Select a language—English or German.
- On the following screen, click Next, and the tool will scan your network segment for Viprinet routers using MAC broadcasts.



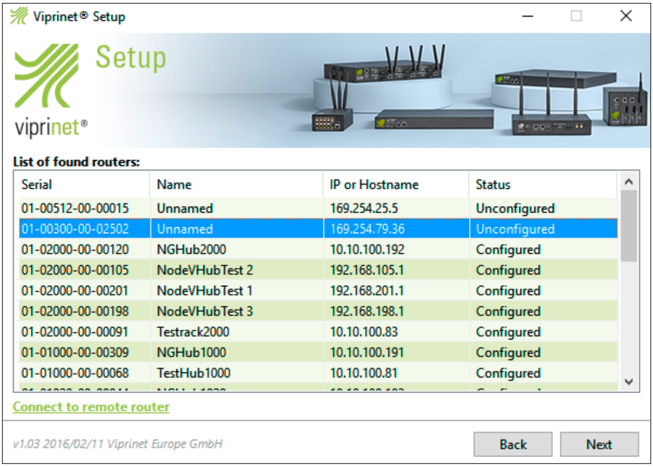
Viprinet® Setup

Welcome to Viprinet Setup

This setup wizard helps you with the basic configuration of your Viprinet router(s). You can do a basic configuration of an unconfigured router, upload a configuration file or create a configuration file from an already configured router.

v1.03 2016/02/11 Viprinet Europe GmbH

4.6 Welcome page



Viprinet® Setup

Setup

List of found routers:

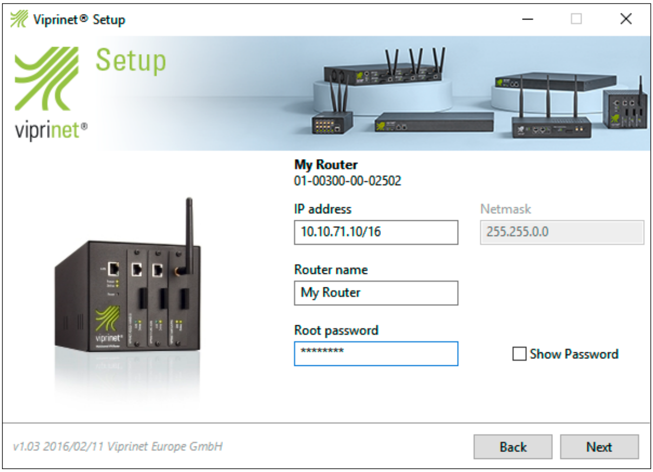
Serial	Name	IP or Hostname	Status
01-00512-00-00015	Unnamed	169.254.25.5	Unconfigured
01-00300-00-02502	Unnamed	169.254.79.36	Unconfigured
01-02000-00-00120	NGHub2000	10.10.100.192	Configured
01-02000-00-00105	NodeVHubTest 2	192.168.105.1	Configured
01-02000-00-00201	NodeVHubTest 1	192.168.201.1	Configured
01-02000-00-00198	NodeVHubTest 3	192.168.198.1	Configured
01-02000-00-00091	Testrack2000	10.10.100.83	Configured
01-01000-00-00309	NGHub1000	10.10.100.191	Configured
01-01000-00-00068	TestHub1000	10.10.100.81	Configured

Connect to remote router

v1.03 2016/02/11 Viprinet Europe GmbH

Figure 4.7 List of routers

1) A list of routers will appear. Units are identified by their serial number (S/N) and IP address, followed by "(unconfigured)" for Nodes and Hubs that are not set up yet. Select the appropriate unconfigured router and click Next.



Viprinet® Setup

Setup

My Router
01-00300-00-02502

IP address: 10.10.71.10/16

Netmask: 255.255.0.0

Router name: My Router

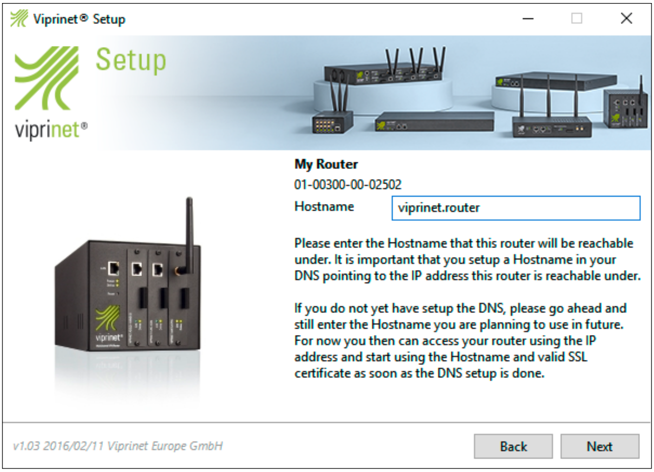
Root password: ********

□ Show Password

v1.03 2016/02/11 Viprinet Europe GmbH

Figure 4.8 Assigning an IP address

2) Enter the IP address for the router, a corresponding netmask, the password you will use to access the AdminDesk, and a device name. Legal password characters fall within the ranges a-z, A-Z, and 0-9; you can use the symbols - +. _ # () / , as well. The password should have more than 8 characters, including a mix of upper and lowercase letters and numbers. All passwords are case-sensitive. Then click Next.



My Router

01-00300-00-02502

Hostname viprinet.router

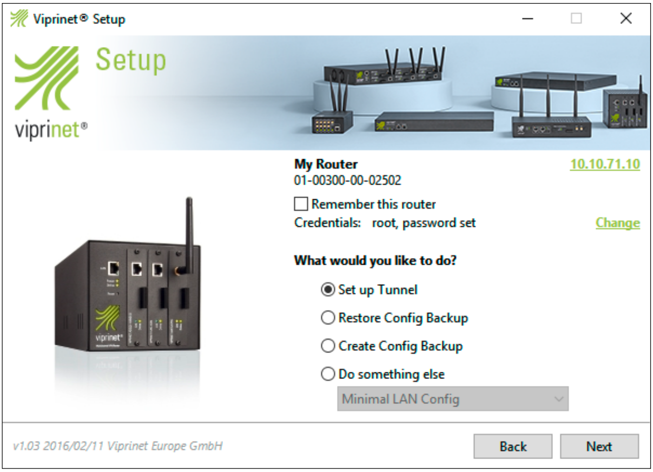
Please enter the Hostname that this router will be reachable under. It is important that you setup a Hostname in your DNS pointing to the IP address this router is reachable under.

If you do not yet have setup the DNS, please go ahead and still enter the Hostname you are planning to use in future. For now you then can access your router using the IP address and start using the Hostname and valid SSL certificate as soon as the DNS setup is done.

v1.03 2016/02/11 Viprinet Europe GmbH

Figure 4.9 Setting a hostname

3) If you want to reach the router by a hostname instead of using the IP address, please enter it here.



My Router 10.10.71.10

01-00300-00-02502

□ Remember this router

Credentials: root, password set Change

What would you like to do?

● Set up Tunnel

○ Restore Config Backup

○ Create Config Backup

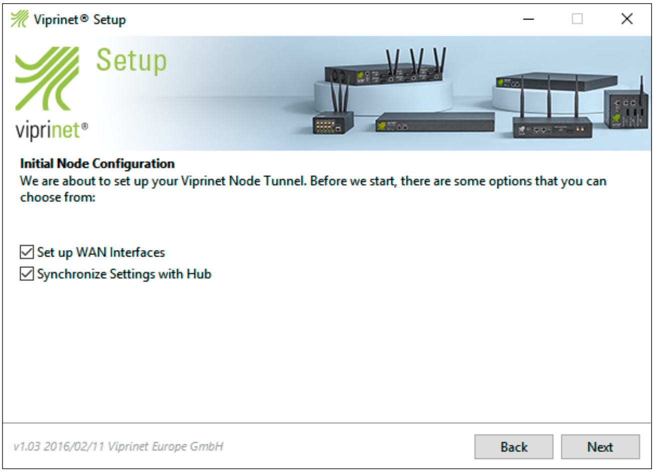
○ Do something else

Minimal LAN Config

v1.03 2016/02/11 Viprinet Europe GmbH

Figure 4.10 Selecting a router mode

4) In this step you can decide if you want to set up a new tunnel, if you want to restore or create a configuration backup or simply create a minimal configuration of the LAN interface to continue the setup process on the AdminDesk.



Viprinet® Setup

Initial Node Configuration

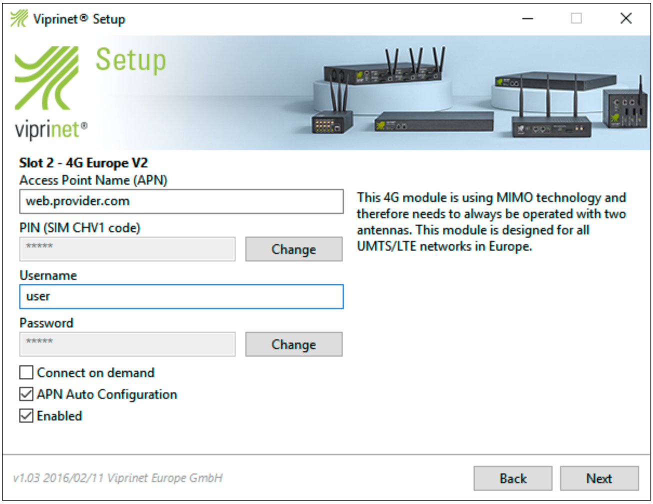
We are about to set up your Viprinet Node Tunnel. Before we start, there are some options that you can choose from:

☑ Set up WAN Interfaces

☑ Synchronize Settings with Hub

Figure 4.11 Initial Node Configuration

5) Tick the checkbox for "Set up WAN Interfaces" if you already know your WAN configuration details, such as SIM card PINs, DSL access data or an IP address configuration to connect to an external modem. The "Synchonize Settings with Hub" checkbox allows you to enter the Hubs credentials, so the Setup Tool is able to send the parameters to it. Except of finetuning settings, the Hub will be automatically configured.



Viprinet® Setup

Slot 2 - 4G Europe V2

Access Point Name (APN): web.provider.com

PIN (SIM CHV1 code): *****

Username: user

Password: *****

□ Connect on demand

☑ APN Auto Configuration

☑ Enabled

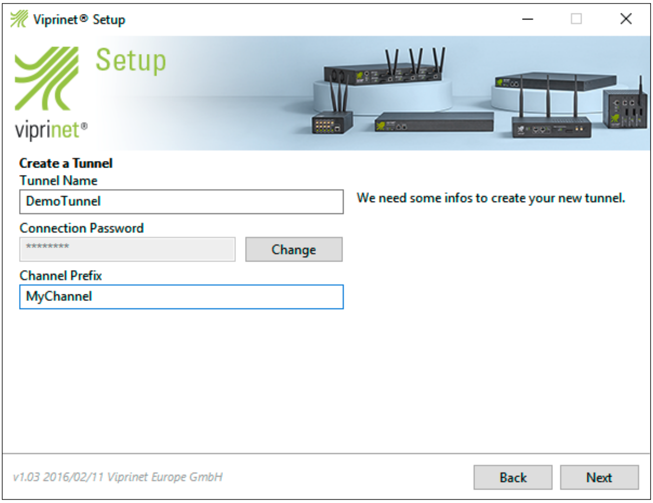
This 4G module is using MIMO technology and therefore needs to always be operated with two antennas. This module is designed for all UMTS/LTE networks in Europe.

Figure 4.12 Configuring SIM modules

6) Configure the WAN SIM card module slot. If the Setup Tool software does not detect a module, ensure that the relevant SIM card has been correctly inserted. Modules are not switched on by default, so tick Enabled in the configuration menu to activate them. (Viprinet Nodes can detect the correct APN—access point name—automatically. To do so, tick

"APN Auto Configuration". If this does not work, contact your wireless service provider. Enter a SIM PIN, username, and password associated with the SIM card's data account, if applicable. Click Next.

7) Each module slot will be configured in the same way.



Create a Tunnel

Tunnel Name: DemoTunnel

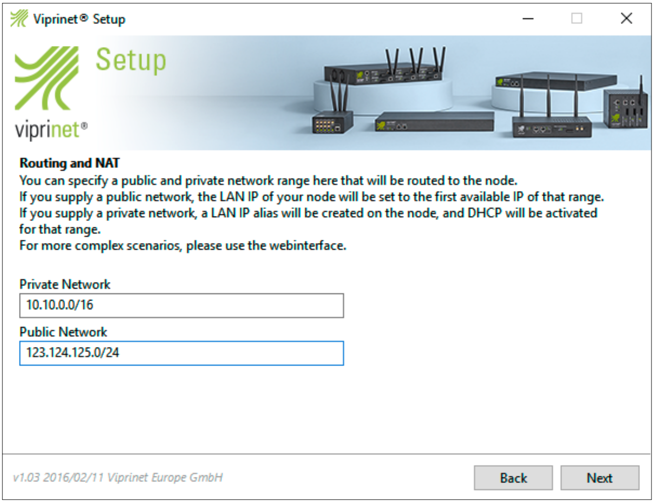
We need some infos to create your new tunnel.

Connection Password: ********

Channel Prefix: MyChannel

Figure 4.13 Configuring the tunnel

8) Enter the name of the VPN tunnel on the Hub that this Node will connect to, along with the password for that tunnel and a Channel Prefix. In this example, all channels would be named MyChannel1, MyChannel2, and so on. Click Next.



Routing and NAT

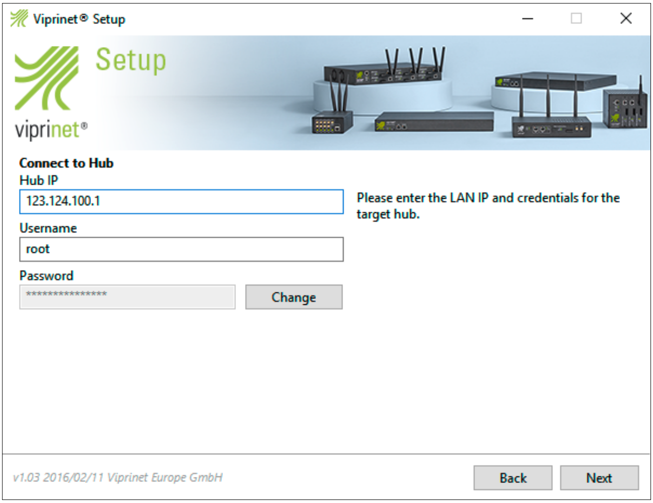
You can specify a public and private network range here that will be routed to the node.
If you supply a public network, the LAN IP of your node will be set to the first available IP of that range.
If you supply a private network, a LAN IP alias will be created on the node, and DHCP will be activated for that range.
For more complex scenarios, please use the webinterface.

Private Network: 10.10.0.0/16

Public Network: 123.124.125.0/24

Figure 4.14 Configuring routing and NAT

9) Please enter a private and/or public network range that you want to use in your LAN. A routing rule and a NAT entry will be automatically configured on the Hub for this. If you're using a public address space, please make sure that the routing in your Hub location is also pointing to the LAN interface of the Hub.



Connect to Hub

Hub IP

123.124.100.1

Username

root

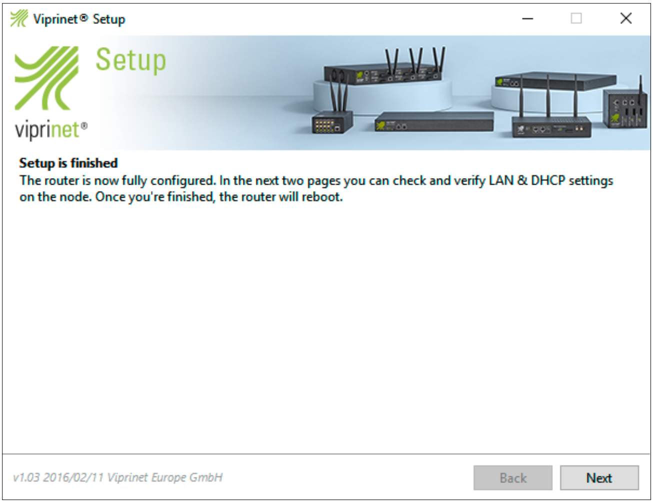
Password

****

Please enter the LAN IP and credentials for the target hub.

Figure 4.15 Entering the Hub credentials

10) Here you have to enter the Hub credentials as described in step 5.

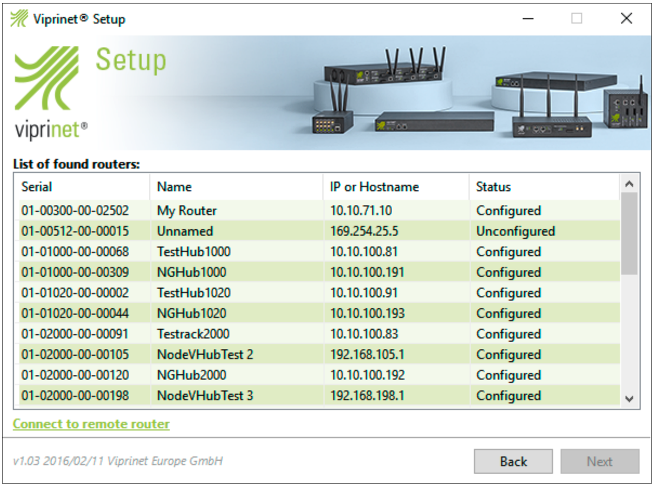


Setup is finished

The router is now fully configured. In the next two pages you can check and verify LAN & DHCP settings on the node. Once you're finished, the router will reboot.

Figure 4.16 Setup Tool finished

11) The Setup process is finished and the router will reboot.



List of found routers:

Serial	Name	IP or Hostname	Status
01-00300-00-02502	My Router	10.10.71.10	Configured
01-00512-00-00015	Unnamed	169.254.25.5	Unconfigured
01-01000-00-00068	TestHub1000	10.10.100.81	Configured
01-01000-00-00309	NGHub1000	10.10.100.191	Configured
01-01020-00-00002	TestHub1020	10.10.100.91	Configured
01-01020-00-00044	NGHub1020	10.10.100.193	Configured
01-02000-00-00091	Testrack2000	10.10.100.83	Configured
01-02000-00-00105	NodeVHubTest 2	192.168.105.1	Configured
01-02000-00-00120	NGHub2000	10.10.100.192	Configured
01-02000-00-00198	NodeVHubTest 3	192.168.198.1	Configured

Figure 4.17 Discovery page

12) After a successful reboot of the device, your router should show up on the discovery page with status *Configured.*

4.0.9 Finishing configuration in the AdminDesk

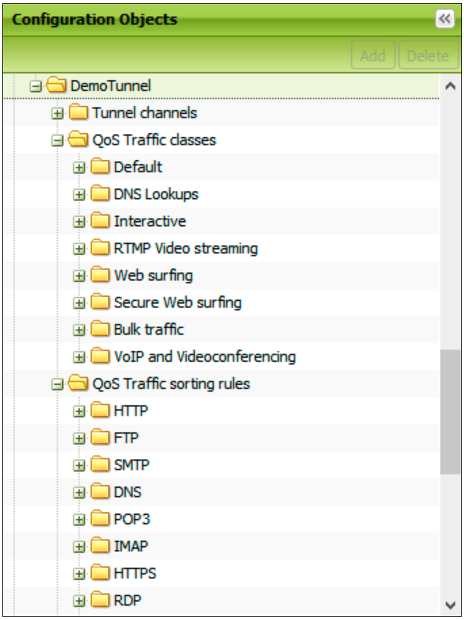
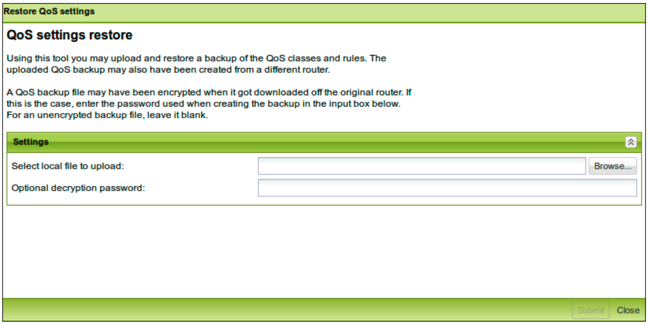


Figure 4.18 The QoS menu

Now you will upload the QoS (Quality of Service) settings file that you have been provided with, to ensure that these settings on your Node match those for the Hub you will be connecting to.

1) Enter the LAN IP address of your router into your browser's URL field. Log in as root using the password you entered in the Setup Tool. Expand the VPN Tunnels directory in the menu tree. Select the relevant tunnel. Click Restore QoS. A pop-up window will appear. Upload the QoS file. Remember to click Apply after the restore window has closed.



Restore QoS settings

QoS settings restore

Using this tool you may upload and restore a backup of the QoS classes and rules. The uploaded QoS backup may also have been created from a different router.

A QoS backup file may have been encrypted when it got downloaded off the original router. If this is the case, enter the password used when creating the backup in the input box below. For an unencrypted backup file, leave it blank.

Settings

Select local file to upload:

Optional decryption password:

Figure 4.19 Restoring QoS settings

2) Click "Select local file to upload" and choose the QoS file you have been given. If a decryption password was used, enter that as well. Click Submit. The settings will now have been applied. You can close your browser.
The antenna socket LEDs on the front of the router will begin blinking as the SIMs connect to the mobile data network. Once the modules are connected, the LEDs will stop blinking and stay lit.

4.1 Advanced setup

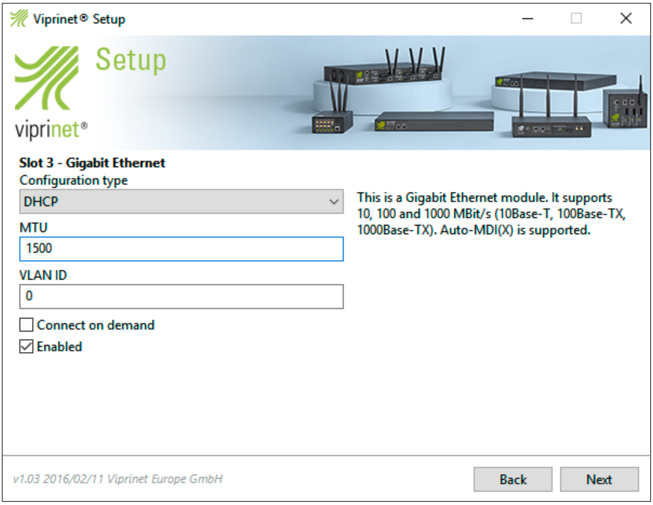
This section includes information on configuring additional module types, creating a network plan, IP addresses, and setting up non-local routers and Hubs.
For information about setting up Node stacks, see section 6.9.

4.1.0 Configuring all module types

The three major module type divisions are standard ethernet, VDSL, and wireless. Wireless module configuration is covered earlier in this chapter in section 4.0.9, although additional information is provided later in this section.

4.1.0.0 Gigabit ethernet connections (all wired media except VDSL)

Gigabit Ethernet modules are configured with ethernet network data—IP address, netmask, gateway, nameservers. Those that connect directly to provider networks include a username and password and configuration properties specific to the medium they are associated with.



Slot 3 - Gigabit Ethernet

Configuration type: DHCP

MTU: 1500

VLAN ID: 0

□ Connect on demand

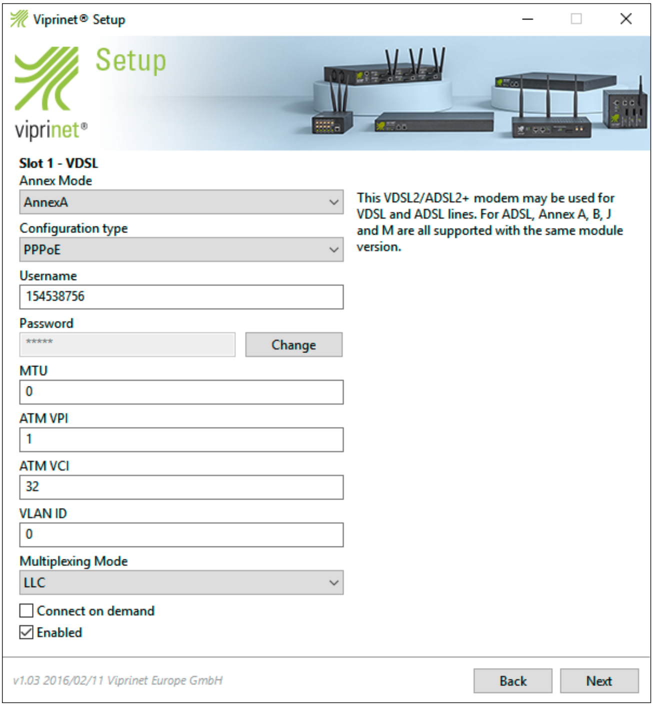
☑ Enabled

This is a Gigabit Ethernet module. It supports 10, 100 and 1000 MBit/s (10Base-T, 100Base-TX, 1000Base-TX). Auto-MDI(X) is supported.

v1.03 2016/02/11 Viprinet Europe GmbH

Figure 4.20 Configuring Gigabit Ethernet modules

4.1.0.1 VDSL



Slot 1 - VDSL

Annex Mode: AnnexA

Configuration type: PPPoE

Username: 154538756

Password: *****

MTU: 0

ATM VPI: 1

ATM VCI: 32

VLAN ID: 0

Multiplexing Mode: LLC

□ Connect on demand

☑ Enabled

This VDSL2/ADSL2+ modem may be used for VDSL and ADSL lines. For ADSL, Annex A, B, J and M are all supported with the same module version.

v1.03 2016/02/11 Viprinet Europe GmbH

Figure 4.21 Configuring VDSL modules

VDSL module properties include a username and password as well as properties specific to the medium.

4.1.0.2 Additional information about wireless modules

For private networks (e.g. police) or SIMs bought through resellers, automated APN detection may not work well, so in those cases obtain the PIN from your provider. In some cases you may need a dial string, which you can obtain from your provider.

4.2 Creating a network plan

When you create your network plan, you will need to decide how many hosts may be included in the LANs associated with each Node, and select a range of IP addresses (also referred to as network segments) for these hosts to use. Generally one segment is assigned to each branch office or building. These subnets may be, if you wish, part of a larger subnet including all branch office LANs.
If you are not going to use a star topology, consult with Viprinet Support before proceeding.

4.3 IP addresses

IP address management for modules is typically a fully automatic process. The IP addresses needed for each hot-plug module in your network will most likely be dynamically assigned by your ISP. As Viprinet Nodes only use outgoing TCP connections to establish a VPN tunnel and can support duplicate IP addresses for their modules, it is not necessary to obtain static or public IP addresses.

4.4 Configuring non-local routers

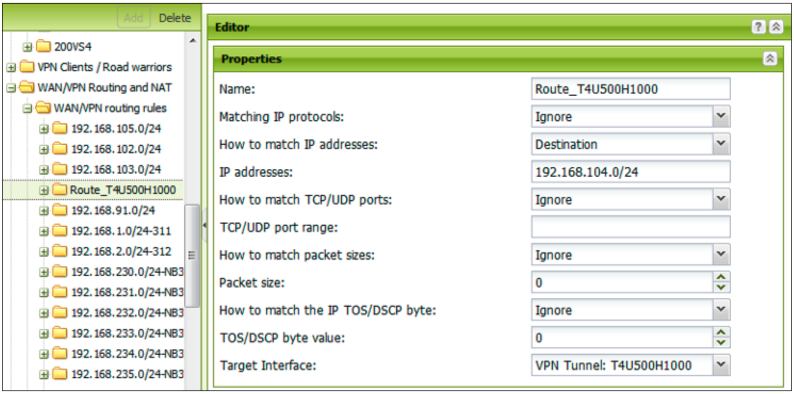
Your computer either must be physically connected to the router you are configuring or be in the same network segment.

4.5 Configuring Hubs

The Setup Tool portion of Hub configuration is the same as that for Nodes, except that you won't be configuring modules and will need to enter WAN interface information.

1) Enter the Hub's WAN IP address and corresponding netmask, along with the gateway IP address for the ISP or other Hub it will be connecting to.

2) A routing rule must be created for each tunnel this Hub will be connecting to. NAT entries can also be configured but are not always necessary. A setup can work without NAT if public addresses are used or if hosts with private IP addresses only need to access hosts on the same segment or to IP subnets connected to the same Viprinet infrastructure.



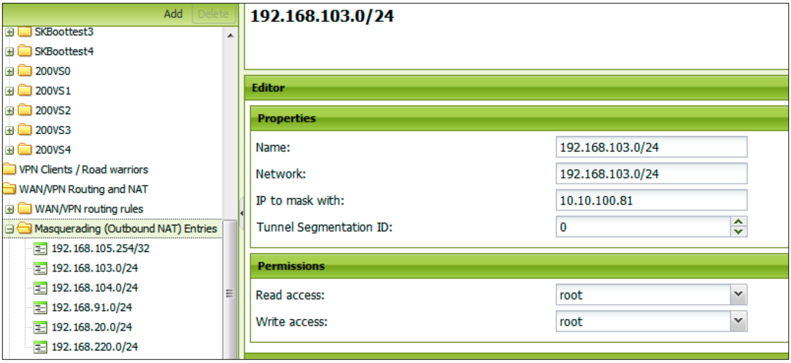
Name:	Route_T4U500H1000
Matching IP protocols:	Ignore
How to match IP addresses:	Destination
IP addresses:	192.168.104.0/24
How to match TCP/UDP ports:	Ignore
TCP/UDP port range:	
How to match packet sizes:	Ignore
Packet size:	0
How to match the IP TOS/DSCP byte:	Ignore
TOS/DSCP byte value:	0
Target Interface:	VPN Tunnel: T4U500H1000

Figure 4.22 Editing routing rules

In the Routing Rules menu, you will associate a LAN IP subnet with each tunnel. See Figure 4.22.

3) Navigate to the WAN/VPN Routing and NAT menu. Expand it. Select WAN/VPN Routing Rules. Click the Add button above the menu tree. A pop-up window will appear requesting you to name the new rule. After you create the name, the rule menu will appear, auto-populate, and then you will be sent back to the matrix listing of rules.

4) Scroll down to the bottom of the list, where the newest rules appear. Double-click on the name of your rule. Indicate a network segment in the IP Addresses field, using CIDR notation. Select a target interface—the tunnel—in the dropdown at the bottom of the menu. No other settings in the menu need to be modified. Click the Apply button in the lower right-hand corner.



192.168.103.0/24

Name:	192.168.103.0/24
Network:	192.168.103.0/24
IP to mask with:	10.10.100.81
Tunnel Segmentation ID:	0
Read access:	root
Write access:	root

Figure 4.23 Associating NAT IP addresses with LANs

5) In the Masquerading (Outbound NAT) Entries menu you can associate network segments with a masking IP address. Navigate to the WAN/VPN Routing and NAT menu. Expand it. Select Masquerading (Outbound NAT) Entries. Click the Add button above the menu tree. A pop-up window will appear requesting you to name the new entry.

6) After you create the name, the NAT menu will appear and auto-populate, and then you will be sent back to the matrix listing of entries. Scroll down to the bottom of the list, where the newest NAT entries appear. Double-click on the name of your entry. Configure a network segment (the Network field) and IP address to mask with. If you are using Hub tunnel segmentation, enter a segmentation ID.

Chapter 5. Basic configuration

This chapter covers the administration of five areas that are likely to come up frequently: tunnels, VPN Clients, WAN and LAN settings, routing rules, and logging and maintenance. More complex settings you might not use or should not have to reconfigure often are covered in Chapter 6.

Some of these items are also covered in Chapter 4 in a quickstart context, however they may be approached slightly differently when you are working with routers that have already been configured.

5.0 Tunnels and channels

This section explains how to add tunnels and channels in the AdminDesk and modify tunnel and channel settings. It does not provide an exhaustive list of all tunnel and channel settings. Consult section 2.5.1.5 for that list.

Attention
Tunnel and channel names need to be the same on the Hub and the Node. Never change settings on only one end of the VPN tunnel.

5.0.0 Adding VPN tunnels in the AdminDesk

There are 4 steps to creating and activating a new VPN tunnel.

- Create the tunnel on the Hub
- Create channels on the Hub
- Associate the tunnel name and a Node IP subnet by adding a new routing rule on the Hub in the *WAN/VPN routing and NAT* menu
- Connect a Node to the tunnel

5.0.0.0 Create the tunnel on the Hub

To add a new VPN tunnel, open the AdminDesk for the relevant Hub and select the *VPN Tunnels* directory in the menu tree. Click *Add* at the top of the menu tree pane and enter a name in the pop-up window that appears. Navigate to the new tunnel within the *VPN Tunnels* directory and set a password. Click on *Copy QoS templates to here* and *OK*. Then tick *Enabled* in the top *VPN Tunnels* menu to switch on the tunnel. For the tunnel to be operational, you will also need to add channels (see the next section) and WAN routing settings (see section 5.3).

5.0.0.1 Create the channels

Once you have created the tunnel you need to add tunnel channels. Select the newly created tunnel and then its sub-object *Tunnel channels*. Click the *Add* button at the top of the menu tree pane. Give the channels names and associate them with the appropriate *Module slot / WAN Interface to use*, then tick *Enabled* on those that should be active. Configure all other channel parameters as needed; see 2.5.1.5 for a detailed list. When all of the settings are correct, click *Apply*. Repeat as needed. More channels can always be added to an existing tunnel.

5.0.0.2 Add a new routing rule

On the Hub, select *WAN/VPN Routing and NAT*, then its sub-item *WAN/VPN routing rules*, and click *Add*. The new routing rule name should include the tunnel name combined with the IP address range assigned to that tunnel. You'll also need to enter the IP address range that is going to be routed, in CIDR notation. Select the tunnel this subnet will be routed to as the *Target Interface*. If you are using tunnel segmentation (covered in section 6.8) you need to enter the segment ID for this tunnel. If not, leave it set to the default, 0.

5.0.0.3 Connect a Node to an existing VPN tunnel

To connect the new tunnel to a Node, either do so when configuring the Node with the setup tool or in the AdminDesk. To connect the tunnel to a Node in the AdminDesk, select the *VPN tunnel* menu, click the *Add* button, and enter the tunnel name in the pop-up that appears, along with the password and Hub IP address. Then click the *Apply* button. Sync QoS settings with the Hub by using *Copy QoS templates to here*. After you finish editing these settings, tick *Enabled* in the top *VPN Tunnels* menu. This will not interrupt the flow of traffic to and from the Node. Do not change tunnel or channel settings on the Node.

5.0.1 Modifying channel settings

To view tunnel settings, double-click the name of the tunnel in the *VPN Tunnels* menu page on the Hub's AdminDesk. You can modify the channel's name or module slot, enable or disable it, designate it a backup, and modify other settings associated with traffic management that are covered in more detail in section 2.5.1.5 and section 6.0.2. If you have made a change to an active tunnel, click the *Reconnect* button in the Functions pane so the changes can take effect. This will not interrupt the flow of traffic to and from the Node.

5.0.2 Modifying VPN tunnel settings on the Hub and the Node

Expand VPN Tunnels in the Hub's AdminDesk menu tree, then select the sub-item with the name of the tunnel you wish to modify. You can edit the password, whether the tunnel is enabled, and the tunnel name. From a Node's AdminDesk, you can also edit the Hub IP address this tunnel should connect to. Additional details on tunnel settings are available in sections 5.0, 2.5.1.5, and 6.3.

5.1 VPN Clients

This section is a guide for administrators setting up VPN client access. A non-administrative user guide to the tool is provided in Appendix 7, and section 2.8 is an overview of the GUI anatomy. A complete list of routing options is provided there.

VPN client access allows remote users to access an organization's internal networks. No license or product activation information needs to be stored on the users' computers. The client software integrates itself into a user's operating system as a virtual network card and then uses up to two types of network media to connect to one of your organization's Hubs. One free VPN Client account is provided with each router. All additional VPN Clients accounts must be associated with licenses. Contact your vendor to obtain licenses.

These accounts are set up on a Hub; they cannot be set up on a Node. Using a VPN Client is like having your own tunnel. Client accounts only share QoS and routing settings. Clients connecting to the same Hub share one (dynamically assigned) pool of IP addresses, unless you are using Hub Segmentation (see section 6.8). All VPN Clients also share the same routing settings and QoS classes and rules.

There are five steps in the process of setting up VPN client access.
You'll need to:

- Install VPN client user licenses on your Hub
- Designate a pool of IP addresses for VPN users
- Create user accounts
- Configure routing
- Configure QoS rules and classes
- Configure an IP address to mask with in the Masquerading (Outbound NAT) Entries menu in the WAN/VPN routing and NAT section of the AdminDesk.

It is also possible to use VPN Hub Tunnel Segmentation (see section 6.5) with VPN Client accounts if you install an additional add-on license. Segmentation allows you to create multiple pools of identical IP addresses for VPN Client users. Each pool can be assigned to a different segmented group of VPN clients.

5.1.0 Activating VPN Client software licenses

To activate VPN Client account licenses you will need to generate a license code. See Appendix 7 and section 6.9.0.3 for details. Select *VPN Clients / Road warriors* in the menu tree, and then the sub-item *License Manager*. Click the *Add a license* button in the *Functions* pane. Paste the license number in the pop-up window that appears and click *Ok*. The *Total number of licensed client accounts* counter in the *Properties* pane at the top of the page should increment accordingly. The number of unused, available accounts in the current block of licenses is also indicated on that page. Activated licenses are applied immediately; you do not need to reboot your Hub.

5.1.1 Designating a pool of IP addresses

Select *VPN Clients / Road Warriors* in the menu tree. Enter a public or private IP address range in CIDR notation in the *Client IP pool* field in the *Properties* pane. Make sure the network size is greater than the maximum number of concurrent connections that you anticipate, plus one just in case traffic exceeds predictions.

If this IP address pool constitutes a private subnet and you wish to allow VPN client users to access the internet through their VPN connections, make sure to add an outbound NAT entry for it in the *WAN/VPN Routing and NAT menu sub-item Masquerading (outbound NAT) Entries.*

5.1.2 Creating user accounts

To add a user, select the *VPN Client users* sub-item and click the Add button in the menu tree pane. Designate a password and a username, and tick *Enabled*. You can access user accounts that have already been created by double-clicking their names on the *VPN Client users* properties page. That also lists if their accounts are enabled and if they are currently connected to the Hub.

5.1.3 Configuring routing

Select *Clients' Routing Settings* in the menu tree; it is a sub-item of *VPN Clients / Road Warriors*. For the menu, see section 2.8. If you wish to enable your users to access the internet through their VPN connection, you will need to route all their traffic through the VPN tunnel using NAT IP addresses as noted in section 5.1.

5.1.4 Configuring QoS rules and classes

See sections 6.0 through 6.2 for instructions on configuring QoS rules and classes. You can configure special QoS settings for VPN users or use the Hub's existing QoS classes for them.

5.2 WAN and LAN settings

This section covers settings for the permanent physical network interfaces on your router; complete lists of all options are available in Chapter 2. Both Hubs and Nodes have LAN interfaces, but only Hubs have WAN interfaces. Hubs' LAN interfaces are labeled Uplink and their WAN interfaces are labeled WAN/VPN.

Apply new LAN IP alias settings and Additional LAN routes by clicking „Restart LAN interface".

5.2.0 LAN settings

To view the *LAN settings menu*, consult section 2.5.1.5.2.

5.2.0.0 Adding LAN IP address aliases

To access several LANs at once, you will need to associate multiple IP addresses with your router's LAN interface. This is especially likely to come up if a Node is serving more than one LAN.
To add an alias, select *LAN IP Aliases* in the menu tree and click the *Add* button. Enter the relevant properties and click *Apply.*

5.2.0.1 Adding additional LAN routes

Additional LAN routes are more often used on Nodes than on Hubs, and allow you to send traffic through your router's LAN interface outside of a tunnel. They are primarily relevant for complex topologies. To add a LAN route, select the *Additional LAN Routes* item in the menu tree, and click the *Add* button. Enter the relevant properties and click *Apply*.

5.2.1 WAN settings

See section 2.5.1.5.1 for the *WAN settings* menu.

5.3 Routing rules

This section describes some common uses of routing settings in the *WAN/VPN routing and NAT* menu, and important things to remember about them. To see an exhaustive list of options for this set of menus, consult section 2.5.1.5.
Each Node must be associated with a tunnel name in the *Default WAN/VPN Interface* field. If you are using private IP addresses on your LAN, you will need to set up a NAT entry for the LAN on the Hub it is connected to; NAT entries on Nodes will not work properly. While in the *Masquerading* menu, click *Add* and indicate the entry name, network, masking IP address (also called the NAT IP address, usually the same as the Hub's LAN interface IP address), and if relevant, a tunnel segmentation ID.

5.3.0 Port forwarding entries

Port forwarding is used to reach clients with private addresses remotely. In the AdminDesk for the Hub, select *WAN/VPN Routing* and its sub-item *Port forwarding entries* in the menu tree. Click the *Add* button at the top of the menu tree frame. Name the rule something that indicates this host will have a public IP address, like "Public network branch 1", then set *IP Protocols* to Ignore so routing decisions will be based on the destination (or target IP address) of incoming packets, rather than on traffic type.

Forwarding properties should be configured as follows:

- Original Destination IP address
  - The Hub LAN IP address or alias
- Original Destination Port
  - A user-defined port which is not already being used to connect to this host. For HTTP connections (port 80) common port numbers include 8080, 8888, and 8001, because that is easy to remember.
- New Destination IP address
  - The private IP address at the branch office that the alias will point to, e.g. the Node's LAN IP address
- New Destination Port
  - The port you would like to forward the original IP address to. To reach GUI via HTTP use port 80

Port forwarding entries may use IP addresses associated with the Hub's LAN interface. However, it is also possible to configure it for IP addresses that are not locally bound, for example an address in a block associated with one of the VPN Tunnels.

Attention
When creating port forwarding entries for addresses associated with a Hub where you are adjusting settings, be very careful. If you set IP Protocol to Ignore or forward to a port that the Hub uses locally (like port 80 and 443 for the AdminDesk), this Hub will become unreachable, because ALL ports will be forwarded!

5.4 Logging and maintenance

Logging and maintenance options work the same way on Hubs and Nodes. Consult section 2.5.1.5.2 to view the entire *Logging and maintenance* menu.

The *Backup* button launches a pop-up window that allows you to download a copy of the router configuration settings in a .bin file. You can later upload them to this or another device using *Restore*. If you wish, you can encrypt the backup file with a password. When you click the *Restore* button, it launches a pop-up window that allows you to upload a settings .bin file to the device. An encrypted file can only be uploaded to a new device if the password is known.

Level	Explanation
Emergency	Alert affecting multiple sites and servers
Alert	The network has stopped functioning due to a problem that must be corrected immediately by admins
Critical	A failure that will not stop the network from functioning but should be addressed right away, such as the loss of a backup channel
Error	Less time-sensitive failures
Warning	Notice that an error will occur if no corrective action is taken
Notice	Unusual events with no functional effect
Informational	Normal operational events
Debug	Should not appear on a functioning router; only used during software development

Table 5.0 Log message severity levels, from the RFC 5424 standard. Log severity levels are used to distinguish mundane long-term monitoring messages from urgent alerts about network faults

Chapter 6. Advanced configuration

If you have not used a Viprinet system before, please read Chapter 2 before following these instructions.

In this chapter, as in the rest of this manual, material that is not labeled as specific to either the classic firmware or RuggedVPN firmware is relevant to both.

6.0 Quality of Service settings; bonding modes and priorities; traffic sorting rules

QoS settings give you powerful control over what combinations of channels different traffic types are transmitted over, how much bandwidth you will allocate to each traffic type, what latency levels you will allow to affect them, and how you will compensate for packet loss. In the classic firmware you use bonding modes, which combine packages of traffic-handling characteristics such as packet redundancy and TCP ACK manipulation. In the RuggedVPN firmware, your priorities (such as cost, stability, and latency) determine traffic handling. A different QoS configuration can be applied to each Viprinet VPN tunnel in your network. All VPN Client users on the same Hub share one QoS configuration unless they are on different segments.

6.0.0 QoS settings – Overview

Viprinet's QoS system allows you to prioritize and optimize traffic flows entering and departing from your network. QoS settings take priority over cost. If a specific traffic class requires low latency, for example VoIP traffic, then a low-cost channel with high latency is not used for that class, even if this means that channel remains idle.

Traffic sorting rules give the router the information it needs to identify traffic types that should be associated with each class. Traffic classes associate a specific type of internet use (for example video streaming, web surfing, or VoIP) with a bonding mode or set of priorities.

Your router ships with a default QoS setting template that you can modify to suit your needs. When you create a new tunnel in the AdminDesk, this default QoS configuration is not applied. If you want to use it, click *Copy QoS templates to here* in the *VPN tunnel* menu. To edit these templates, navigate to the *QoS Rules and Classes Templates* item in the menu tree. Instructions on how to edit these templates and create new ones are provided in sections 6.0 and 6.1. To view screenshots of QoS settings, see section 6.0.1.

QoS settings must be consistent on each end of the tunnel. For example, if you change bonding modes for a tunnel on a Hub in Classic but do not change them on the related Node, it will lead to connectivity issues. The best way to configure QoS settings is to copy them from Hubs to Nodes. Begin applying QoS settings to whichever router is farthest away from you in the network. If you change one Node's settings and copy its settings to a Hub, connectivity may be disrupted for all of the other Nodes connecting to that Hub until you update their settings as well. Non-matching source or destination subnet addresses can also cause problems.

In situations where your dataflows will be very sensitive to latency variations or consume large quantities of bandwidth, you should do a traffic analysis for your network before configuring your QoS, using the utilities listed in Chapter 2 and Appendix 1, some of which are available right in the AdminDesk (see section 2.5.2). It is possible to create a traffic class for IP telephony, for example, and assign attributes that will dedicate the lowest-latency lines you are bonding to this use. This class would not use a satellite link for a VoIP call, even though the same line would be fine for web-surfing. You can also use QoS settings to throttle low-priority traffic. In order to optimize your settings as appropriate for your connections' latency and bandwidth, you need to know what kind of traffic is going through your tunnels. Explaining the procedures for doing a traffic analysis is beyond the scope of this manual, so please refer to the following source for more information:

Tanenbaum, Andrew S.,Wetherall, David J.
Computer Networks. 5th ed.
New Jersey: Prentice Hall, 2010.
ISBN-13: 9780132126953
http://computernetworks5e.org/blogs/

Keep in mind

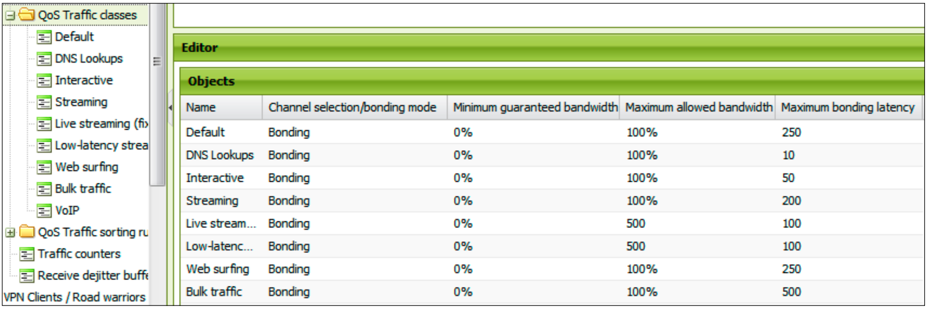
You must configure traffic sorting rules and associate them with classes for the QoS system to work. You cannot just set up either classes or rules.

The QoS system identifies service type by:
- Protocol
- IP address header's QoS/ToS bit

It identifies source or destination by:
- TCP or UDP port number
- Originating or target network and IP address range

- For bi-directional data streams, such as HTTP connections, you cannot use different bonding modes for incoming and outgoing traffic.
- When you create a new QoS rule or class, always use the Log new connections feature to validate that your traffic is correctly matched and that the same QoS classes are being used on the Hub and on the Node.
- Datastreams in the same class compete with one another; avoid sorting data streams with very different requirements into the same QoS class
- Example: Interactive traffic, such as SSH connections, has been paired with high-bandwidth video downloads in your settings. You discover that SSH connections have suddenly become very slow, because there is not sufficient bandwidth to support them.

6.0.1 QoS settings – classic firmware



- QoS Traffic classes
  - Default
  - DNS Lookups
  - Interactive
  - Streaming
  - Live streaming (fix
  - Low-latency strea
  - Web surfing
  - Bulk traffic
  - VoIP
- QoS Traffic sorting ru
- Traffic counters
- Receive dejitter buffe
- VPN Clients / Road warriors

Editor

Objects

Name	Channel selection/bonding mode	Minimum guaranteed bandwidth	Maximum allowed bandwidth	Maximum bonding latency
Default	Bonding	0%	100%	250
DNS Lookups	Bonding	0%	100%	10
Interactive	Bonding	0%	100%	50
Streaming	Bonding	0%	100%	200
Live stream...	Bonding	0%	500	100
Low-latenc...	Bonding	0%	500	100
Web surfing	Bonding	0%	100%	250
Bulk traffic	Bonding	0%	100%	500

Figure 6.0 Classic firmware Traffic classes *list*

6.0.1.0 Adding a new class

Expand the VPN *Tunnels* menu for the tunnel who settings you will be adjusting. Select *QoS traffic classes* and click the *Add* button. A dialog box will pop up with the title *Add item* and a field where you can enter the name of the traffic class. Do so and click *Ok*. The *Properties* pane for the new class will load in the control window of the AdminDesk.

6.0.1.1 Modifying a new or existing class

To view the full traffic class menu, refer to section 2.5.1.5. The most important things you will do in this menu are choose a bonding mode, specify *Minimum* and *Maximum* allowed *bandwidth, Maximum bonding latency*, and *Required link stability*. Select a bonding mode in the dropdown next to *Channel selection/bonding modes*:

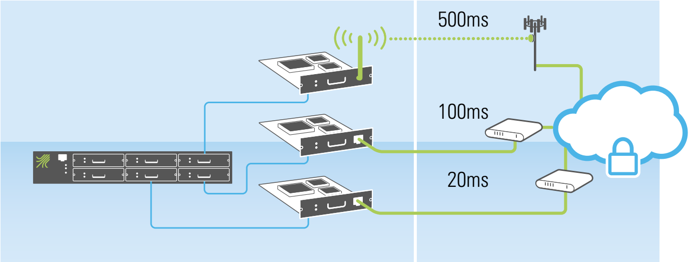
Bonding mode	Characteristics
Bonding	• If you do not modify any of your default settings, this mode splits traffic flows over all available links. If you have manually configured your QoS settings, it assigns flows based on their *Maximum Bonding Latency*. • The best choice for most traffic types • Compatible with every current IP protocol
Bonding TCP Optimizer	• Better for high-latency, high-bandwidth connections • Allows you to optimize your use of TCP data streams • Avoids problems with TCP window size • Ideal for high-latency links (e.g. UMTS) • Best for traffic demanding a lot of bandwidth for a long period of time • Only bonds TCP connections • Can cause issues with some encrypted connections • This mode uses fake ACK packets to improve throughput. It is not a good match for very lossy LAN connections between a host and the Viprinet router, such as low-quality wifi access points. Because If a packet is lost between the Node and the LAN, any re-transmission request from the LAN will result in an error because the sending host will already have received an ACK packet. See the paragraph directly after this table for more information.

Bonding mode	Characteristics
Bonding diversity	• This mode requires a Streaming Optimization license • Most appropriate for situations when you have more bandwidth available than you need and low latency with 0% packet loss is important • Sends multiple copies of the same data over different channels • Best for high-quality bidirectional traffic
Lossy Bonding	• This mode requires a Streaming Optimization license • Disables re-transmission of UDP packages if a channel breaks down • Activates a configurable dejitter buffer • Best for optimizing live radio and video conferences where packet loss is more acceptable than jitter and can be compensated for by the application layer

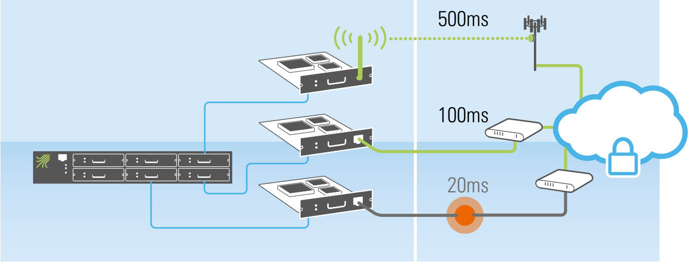
Table 6.0 Bonding modes

Bonding TCP Optimizer uses fake ACK (acknowledgment) packets to speed up data transfer. The way this works is analogous to how a proxy server reduces network load and speeds up DNS requests. With fake ACKs, the router running *Bonding TCP Optimizer* acts like a proxy server. For example: a host on one of the LANs the router serves needs to connect to a remote host—a communications satellite. The first packet travels from the host to the Node, from the Node to the Hub, and from the Hub to the satellite. Even before the satellite responds, the Hub sends a fake ACK to the host so won't wait for a receipt confirmation (an ACK packet) from the satellite. That way the host will keep sending packets, not stop each time it has sent one and wait for a request. Waiting for the satellite will introduce additional latency to the session. Sending fake ACKs can increase the bandwidth of a TCP connection, even on higher latency links.

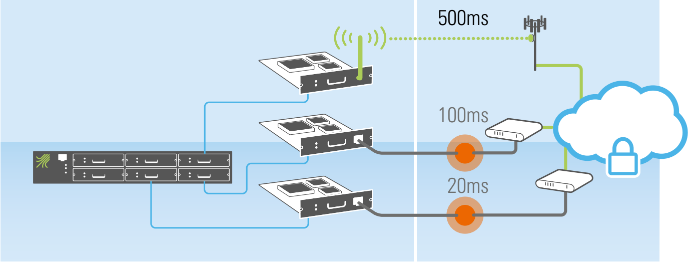
The *Minimum Required Bandwidth* setting allows you to specify the lowest amount of consistently available bandwidth that services and traffic types associated with this class need to be usable and function correctly. If this traffic class is meant for a service that needs a fixed amount of bandwidth (for example, a video stream), enter it as an absolute number in kbits. If you only wish to give traffic in this class priority over other classes, use a percentage value, to a maximum of 100%. Fixed values are problematic when latency and bandwidth fluctuations mean that the assortment of channels being used keeps changing. *Maximum Allowed Bandwidth* should be set as low as possible for classes that include non-critical, bandwidth-hungry traffic types.



200 + 20 = 220. (Maximum bonding latency 220, current bonding latency 100ms)



200 + 100 = 300. (Maximum bonding latency 300, current bonding latency 100ms)



200 + 500 = 700. (Maximum bonding latency 700, current bonding latency 500ms)

Figure 6.1 Maximum bonding latency

In order to protect the quality of latency-sensitive services like VoIP and video streaming, set a low *Maximum Bonding Latency*. The name of this setting is a bit misleading, because the real *Maximum Bonding Latency* value is the product of this entry and the addition of the lowest latency channel which is available.

For example: you set this value to 200ms.

- As in the illustration, one available channel is running at a latency of 20ms, another at 100ms, and a third at 500ms.
- The lowest latency line is 20ms so the router will use it preferentially.
- This setting will always equal the latency of the lowest-latency line available plus the value you have entered. So if you add 200ms (the Maximum Bandwidth setting) to 20ms (the lowest latency channel available) 220ms will become your *Maximum Bonding Latency*.

- 100ms is under 220ms, so that line will also be used
- The 500ms channel will only be used if the 100ms and the 20ms channel drop.
- Now, let's say the 20ms line drops. What's the lowest latency line?
- 100ms. 200ms + 100ms = 300ms. 300ms will be your new *Maximum Bonding Latency*.

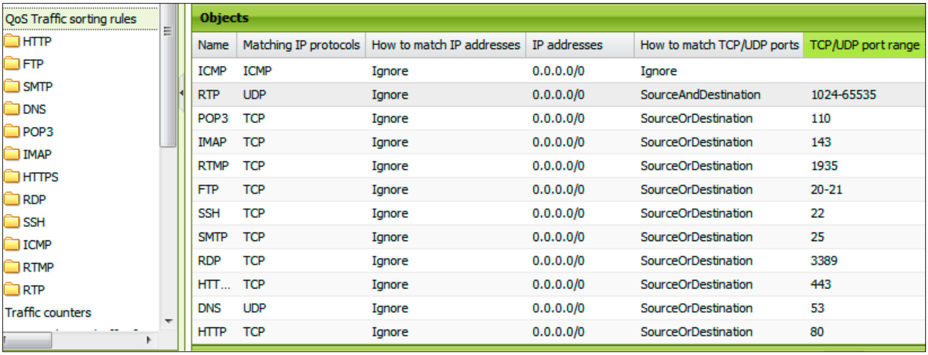
Required Link Stability is a measure of how reliable a connection the class needs. Channels with stability percentages below this value will not be used to transmit traffic in this class. The router measures packet loss over the past 60 minutes to determine the stability percentage. An entirely reliable line with no packet loss has a stability of 100%. Lines with more packet loss will have lower percentage values. A low-loss link type, such as DSL, should have a stability of 99-100%. Cellular data links should have a stability of above 90%. Traffic traveling over UDP will not need as stable a link as that traveling over TCP/IP.

6.0.1.1.0 Streaming optimization

If you install this add-on, you'll have access to two additional bonding modes, *Bonding Diversity* and *Lossy Bonding*. For *Diversity*, you'll need to set *Minimum* and *Maximum Diversity* values for each of your classes. See Appendix 6 for instructions on setting up software licenses. After the *Streaming Optimization* license is installed, an additional submenu, *Receive Dejitter Buffer fine tuning*, will appear in the menu tree within the *VPN Tunnel* directory. Consult section 2.5.1.5 to view the entirety of this menu.

You should not set the *Maximum Diversity* value higher than the number of connected channels.

The *Minimum diversity* setting determines the minimum number of copies of each packet that your Viprinet deployment will transmit. If this value is set to 0, when WAN links are stable, no additional copies of any packet will be sent. If you want to guard against occasional dropouts, set this value to 1; in this case every packet in this QoS class will be sent twice, doubling the amount of bandwidth used. *Maximum Diversity* determines the highest number of copies that will be sent if your WAN links are unstable.



Name	Matching IP protocols	How to match IP addresses	IP addresses	How to match TCP/UDP ports	TCP/UDP port range
ICMP	ICMP	Ignore	0.0.0.0/0	Ignore	
RTP	UDP	Ignore	0.0.0.0/0	SourceAndDestination	1024-65535
POP3	TCP	Ignore	0.0.0.0/0	SourceOrDestination	110
IMAP	TCP	Ignore	0.0.0.0/0	SourceOrDestination	143
RTMP	TCP	Ignore	0.0.0.0/0	SourceOrDestination	1935
FTP	TCP	Ignore	0.0.0.0/0	SourceOrDestination	20-21
SSH	TCP	Ignore	0.0.0.0/0	SourceOrDestination	22
SMTP	TCP	Ignore	0.0.0.0/0	SourceOrDestination	25
RDP	TCP	Ignore	0.0.0.0/0	SourceOrDestination	3389
HTT...	TCP	Ignore	0.0.0.0/0	SourceOrDestination	443
DNS	UDP	Ignore	0.0.0.0/0	SourceOrDestination	53
HTTP	TCP	Ignore	0.0.0.0/0	SourceOrDestination	80

Figure 6.2 Classic firmware QoS Traffic sorting rules list

6.0.2 Traffic sorting rules – classic firmware

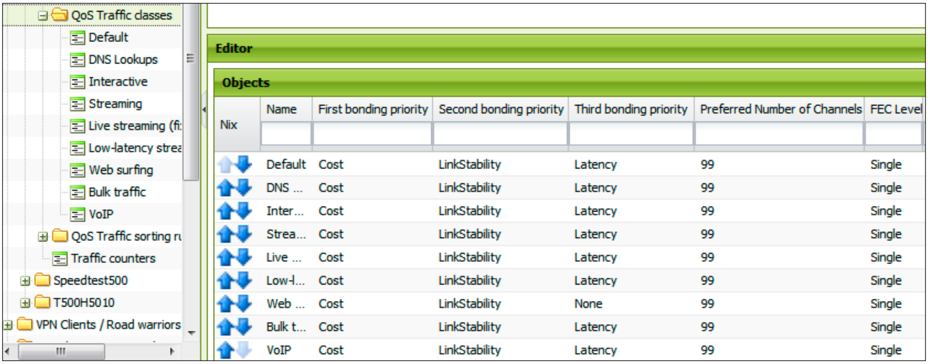
6.0.2.0 Adding a new traffic sorting rule

To create a new traffic sorting rule, navigate to the *QoS traffic sorting rules* directory for your tunnel or VPN Client pool and click *Add*. A dialog box will pop up saying *Add item*. Enter the name of the traffic class and click *Ok*. The *Properties* pane for this rule will then load in the configuration pane of the AdminDesk.

6.0.2.1 Modifying an new or existing traffic sorting rule

In this menu you will configure IP protocols, address and port ranges, packet sizes, and relevant header information that your router will use to identify specific traffic types and associate them with traffic classes. To view the full list of menu items, go to section 2.5.1.5.

6.0.3 QoS settings – RuggedVPN



Nix	Name	First bonding priority	Second bonding priority	Third bonding priority	Preferred Number of Channels	FEC Level
	Default	Cost	LinkStability	Latency	99	Single
	DNS ...	Cost	LinkStability	Latency	99	Single
	Inter...	Cost	LinkStability	Latency	99	Single
	Strea...	Cost	LinkStability	Latency	99	Single
	Live ...	Cost	LinkStability	Latency	99	Single
	Low-l...	Cost	LinkStability	Latency	99	Single
	Web ...	Cost	LinkStability	None	99	Single
	Bulk t...	Cost	LinkStability	Latency	99	Single
	VoIP	Cost	LinkStability	Latency	99	Single

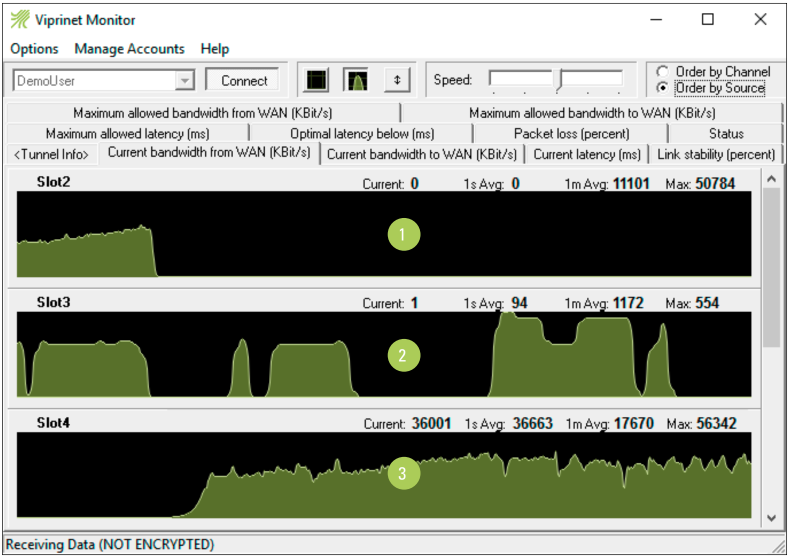
Figure 6.3 RuggedVPN Traffic classes *list*

6.0.3.0 Adding a new class

New traffic classes are added the same way in the new firmware as they are with the classic firmware.

6.0.3.1 Modifying a new or existing class

In the new firmware, instead of setting bonding modes, you will set priorities. There are also three new functions available to support faster transfer speeds and more effective packet delivery. The rest of the menu items remain the same.



```
DemoUser
○ Order by Channel
● Order by Source

Maximum allowed bandwidth from WAN (KBit/s) | Maximum allowed bandwidth to WAN (KBit/s)
Maximum allowed latency (ms) | Optimal latency below (ms) | Packet loss (percent) | Status
<Tunnel Info> | Current bandwidth from WAN (KBit/s) | Current bandwidth to WAN (KBit/s) | Current latency (ms) | Link stability (percent)

Slot2        Current: 0       1s Avg: 0       1m Avg: 11101   Max: 50784
Slot3        Current: 1       1s Avg: 94      1m Avg: 1172    Max: 554
Slot4        Current: 36001   1s Avg: 36663   1m Avg: 17670   Max: 56342

Receiving Data (NOT ENCRYPTED)
```

*Figure 6.4 A screenshot from the Monitor and the related menu from the AdminDesk showing extra high-cost channels being brought in to satisfy circuit load when an affordable channel becomes unreliable.(**Rugged VPN** firmware)*
1. Expensive channel - only used if stable channel drops out
2. Fluctuating channel - several dropouts within seconds
3. Stable channel - active usage for most of the throughput

Your bonding priority options are:

Name	Description
Link Stability	How reliable connections for this traffic type need to be.
Packet Loss	How much packet loss is acceptable. Protocols like UDP, which is designed to prioritize low latencies over high fidelity, tolerate higher levels of packet loss than TCP.
Cost	This option makes it possible to limit your use of costly or limited, volume-billed connections.
Latency	This should be a high priority for traffic like VoIP, videoconferencing, and video streaming, See sections 1.6.1 and 6.1.0 for more on latency.
Bandwidth	If this is a bandwidth-hungry traffic type, prioritize bandwidth.
None	If you do not wish to use one of the priority slots, you can enter this option

Table 6.1 Bonding priorities in RuggedVPN

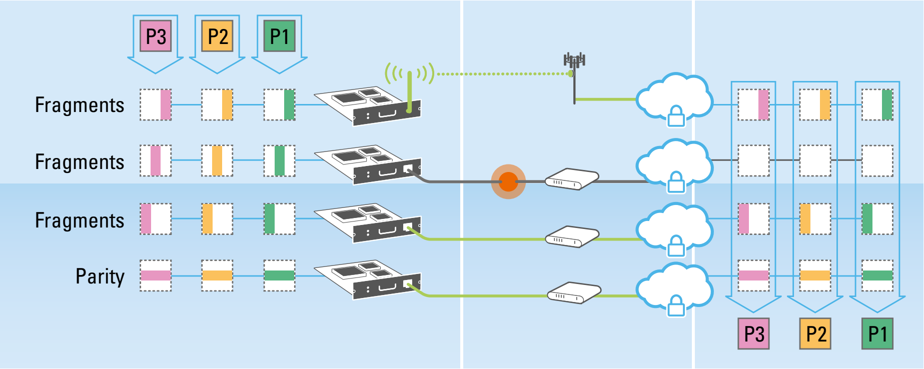


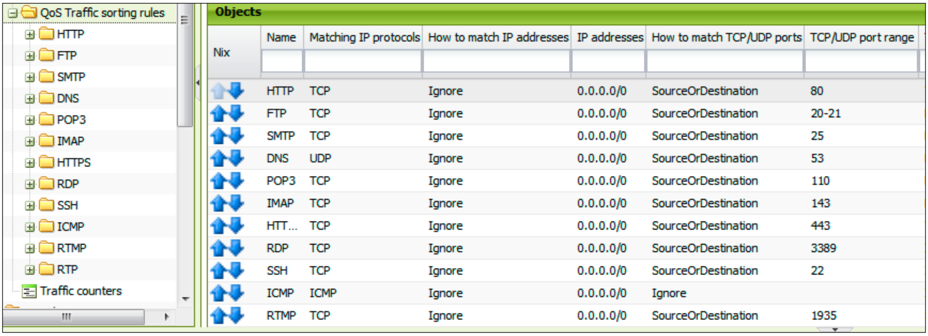
Figure 6.5 Single Forward error correction with packet loss

When *Data compression* is enabled, the router will periodically analyze traffic flows in this class to determine if the data being transmitted is compressible, and compress it. The amount of compression used is based on how much unused CPU capacity is available on the routers processing this traffic flow. If you know that traffic in this class will never be compressible – for example because it is encrypted – you should not enable this feature.

Enable *Guarantee delivery* to ensure that transmissions in this class will never lose packets. If forward error correction is unable to recover a lost packet, the packet will be re-transmitted. The router will also be able to use more effective compression algorithms. If you want to simulate UDP in a TCP-based tunnel, disable this function because you won't need guaranteed delivery.

The *Preferred number of channels* setting determines how many channels this class should use. The router will always try to use those that best match the bonding priorities you have configured. More than one channel must be used for Forward Error Correction to work effectively, even if this requires you to use inferior channels.

The *Forward Error Correction (FEC)* works more or less like a RAID. So each single Packet will be split into fragments and a parity fragment. To assemble those packets, the receiving side only needs the parity fragment and all fragments minus one or all original framgents.



Nix	Name	Matching IP protocols	How to match IP addresses	IP addresses	How to match TCP/UDP ports	TCP/UDP port range
⇅	HTTP	TCP	Ignore	0.0.0.0/0	SourceOrDestination	80
⇅	FTP	TCP	Ignore	0.0.0.0/0	SourceOrDestination	20-21
⇅	SMTP	TCP	Ignore	0.0.0.0/0	SourceOrDestination	25
⇅	DNS	UDP	Ignore	0.0.0.0/0	SourceOrDestination	53
⇅	POP3	TCP	Ignore	0.0.0.0/0	SourceOrDestination	110
⇅	IMAP	TCP	Ignore	0.0.0.0/0	SourceOrDestination	143
⇅	HTT...	TCP	Ignore	0.0.0.0/0	SourceOrDestination	443
⇅	RDP	TCP	Ignore	0.0.0.0/0	SourceOrDestination	3389
⇅	SSH	TCP	Ignore	0.0.0.0/0	SourceOrDestination	22
⇅	ICMP	ICMP	Ignore	0.0.0.0/0	Ignore	
⇅	RTMP	TCP	Ignore	0.0.0.0/0	SourceOrDestination	1935

Figure 6.6 RuggedVPN Traffic sorting rules list

6.0.4 Adding a new rule and modifying a new or existing rule – RuggedVPN

Traffic rules work the same way in the new RuggedVPN firmware as they do in the classic firmware, except that there are no packet size settings.

6.1 Autotuning

6.1.0 Manually adjusting your bandwidth and latency settings

If you are going to set your bandwidth and latency values manually, remember to turn off bandwidth and latency autotuning by un-ticking the relevant boxes. You'll also want to un-tick *Minimize autotuning traffic* at this point, as it will no longer be relevant.

The values you will need to set are:

- *Maximum allowed latency*
  - If an channels latency is higher than this value, the router will not bond this channel anymore
- *Optimal latency below*
  - The absolut latency ceiling for services using this channel

Data comes downstream from the Hub to the Node, and travels upstream from the Node to the Hub. You can only configure how much data each device sends. Define maximum upstream bandwidth utilization levels at your Node, and downstream ones at your Hub. Settings for Nodes and Hubs that are connected to each other should be compatible with one another and the capacity of the channels that make up the VPN tunnel between them.

Keep in mind

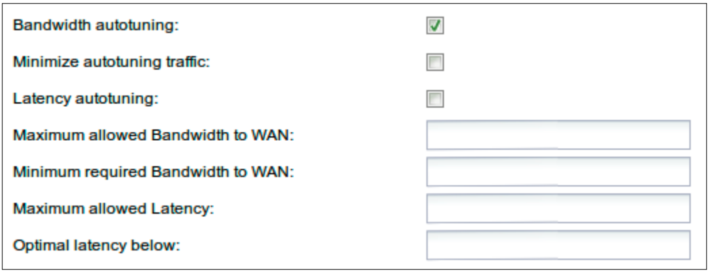
- Shared media like cable have fluctuating latencies and available bandwidths
- As noted in Chapter 1, latency and bandwidth values are inversely related. If you use less of your bandwidth, your packets will move faster.

6.1.1 Configuring autotuning

For an overview of the concepts related to autotuning, see section 1.6.2.

Bandwidth and latency autotuning can be enabled or disabled at the Node or the Hub. Both types are applied on the channel level, not the tunnel level. To access them, navigate to VPN Tunnels → [Tunnel name] → Tunnel channels → [Channel name].

Whether you are using autotuning or setting your latency values manually, if latency exceeds the appropriate value, the connection will be considered unstable by the system, change its status to *connected stalled*, and no longer be used in the VPN tunnel. Never turn off autotuning for shared media connections (such as mobile data). These will always experience frequent latency and available bandwidth changes, so their values should be set accordingly, and with percentages rather than absolute values.



Bandwidth autotuning:	☑
Minimize autotuning traffic:	☐
Latency autotuning:	☐
Maximum allowed Bandwidth to WAN:	
Minimum required Bandwidth to WAN:	
Maximum allowed Latency:	
Optimal latency below:	

Figure 6.7 This is the part of the channel properties menu relevant to this section. For a full list of channel properties, see section 2.5.1.5.2

To apply new bandwidth autotuning settings, navigate to the channel you wish to modify in the menu tree, and click the plus sign. Open the *Performance finetuning* submenu for this channel. Select an algorithm in the dropdown menu; see Table 6.2 for descriptions of your options. Return to the channel menu. Tick the *Bandwidth autotuning* box, scroll down to the bottom of the menu page, click *Apply*, and then click the *Reconnect* button in the Channel or module *Functions* pane.

Bandwidth autotuning algorithm	Algorithm characteristics
Classic	An aggressive method that increases the size of each successive speed test traffic burst geometrically by adding the *Speed test starting value* (the default is 32 bits)
Heuristic	This is the fastest method of tuning your channel, because it increases test traffic exponentially instead of geometrically. It also begins with the *Speed test starting value.*
Passive	This setting does not generate any test traffic. A channel using this algorithm will not reach its full potential until enough real traffic has passed through it. Real traffic enables it to establish appropriate values without running tests. It is primarily used for expensive connections billed by volume and can be used for videoconferencing or streaming if the right codecs are used (consult support) and the connection is opened at least ten minutes before the official start of the conference or stream.
Hybrid	A combination of the passive and heuristic approaches. When this algorithm is enabled, a fast, bandwidth-hungry speed test is run. After that test completes, the software switches to a passive approach that still leaves it room to react to bandwidth oscillations.

Bandwidth autotuning algorithm	Algorithm characteristics
Rapid	This algorithm is designed to be used with Nodes installed in vehicles traveling at high speeds; these move from radio cell to radio cell so quickly that there is not much time to run autotuning tests. As a result, this method does not generate test traffic. The channel's full potential can only be achieved after enough traffic has passed through it to give the algorithm sufficient data to work with. However, this algorithm is adapted to work from a very small volume of data. This autotuning mode is only available if you have licensed the Streaming Optimization feature. In these conditions it is also important to tick the *Rapid Reconnects* checkbox, otherwise frequent cell changes may be read as congestion.

Table 6.2 Autotuning algorithms

After autotuning is enabled, algorithms that allow speed tests will run them. These speed tests usually start at low transfer rates and speeds and rise to higher ones until latency reaches the *Optimal latency below* rate. If the channel is unstable, then speed tests will be frequent. A stable channel will need fewer tests. To run manual speed tests, use the *Download Test* tool available in the module slot and *LAN settings* menus on the AdminDesk.

If you are using expensive connections, or ones with frequent latency and bandwidth variations (for example wireless or cable), you may wish to limit the number of speed tests your device will run. You can either select the Passive algorithm or tick *Minimize autotuning traffic*, which will limit the amount of speed test traffic. You must restart latency autotuning after enabling bandwidth autotuning.

You will also select a *Congestion control algorithm*. See section 1.6.1 for more information about congestion and Appendix 10 for a list of control algorithms.

Keep in mind

- Speed test traffic will always be classed at a lower priority than user traffic, and will be listed separately in the Node's traffic accounting system.
- Do not enable *Auto configuration* in the *Expected internet link capacity* menu on a gigabit ethernet module connected to an external modem, as it will not detect correct values; instead, you will need to set realistic values for your connection manually.

Attention

- If you notice in the Monitor that autotuning tests are eating up a lot of bandwidth, one or more of your connections may be suffering from reliability problems.

6.2 Cost system

If each of your connections costs a different amount, you can assign a value to the channels associated with them that will allow the Node and Hub to prioritize their use appropriately. You also need to consider the restrictions of lower-cost, limited-volume channels that are billed by volume (e.g. a certain amount per megabyte or gigabyte) when you are configuring this setting. As long as lower-cost channels are able to satisfy current bandwidth demands, they will be used preferentially. Channels with the same cost value are used equally.

To use this feature, assign a value between 0 and 100 to each channel in the Cost entry field in the Channel properties menu, with 100 being the most expensive connection you can envision ever using, and 1 the cheapest.

6.3 Channel Backup

To designate a backup channel, tick *Backup channel* in the channel menu. The *Backup score* entry field is just beneath the checkbox.

The higher the backup score, the more significant the channel. The combined backup scores of all channels in a tunnel should add up to something higher than the *Minimum Backup Score* of the tunnel. When channels go offline, the score drops, and backup channels will be brought up until it exceeds the *Minimum Backup Score* once again. Instructions on configuring *Minimum backup* score are provided in section 6.3.

Link stability x backup score = the current backup score of the channel

Example: Backup score of 50 x link stability of 90 = 45 score for the channel

The link stability for each channel is dynamically, automatically calculated, and can be viewed either on the main tunnel configuration page, in the Monitor, or on the configuration page for the channel.

- The firmware evaluates link stability based on the rate of packet loss
  - This is expressed in a range from 0 to 100%. The system reassesses the rate of packet loss once a second
    - 0% means that the link has not been able to transmit data for the last 5 seconds or the channel has twice the maximum allowed latency
    - 100% means that during the last 5 seconds no packets were lost. If *Rapid reconnects* is enabled (found in the *Performance Finetuning* menu), a reconnect is triggered when no successful transmission is sent or received for 3 seconds
  - If this tunnel channel is using a wired connection (DSL, Cable), stability should be 99-100%
  - For wireless connections (WLAN, UMTS/3G) a link stability rating of above 90% may be regarded as normal

When a bad channel comes back online, its stability score will have dropped significantly. Therefore the backup won't be deactivated right away. The backup will only be deactivated after the available bandwidth score becomes greater than the minimum backup score. Channels in *Connecting* status do not count toward the link stability score.

Attention

- Only configure backup channels on Nodes. Do not configure backup channels on Hubs. If you do this, it will disable the channel on that Hub.

6.3.0 Configuring the backup score for your channels

- Determine the bandwidth and stability you can reasonably expect from each of your channels.
- Navigate to the *Channel* menu.
- Enter a number for the *Backup score*.

- Repeat this step for each channel in your tunnel.
- Calculate the totals for each of the backup score settings for your non-backup channels. A good choice for the total backup score might be 100.

6.3.1 Configuring the backup score for the tunnel

- Set the Minimum Backup Score for the tunnel to a value slightly below the sum calculated for all the channels in combination, e.g. 95 or 90. This way, a small drop in link stability will not immediately activate a backup channel.

Keep in mind
If a channel gets stuck in the "Connecting" phase, then
- its stability number will decrease
- it will stop contributing bandwidth
- the backup will be activated

Option A:
1) Navigate to the top menu of the tunnel you are configuring.
Enter a value in the "Minimum number of connected channels" field appropriate for your expectations for this deployment. If you have 3 channels and only need to have two of them up at the same time, type 2 into this field.

2) Expand the tunnel directory to access the configuration menus for its channels.
Visit the menu for each tunnel that needs to be up and tick "Backup channel".
If you only need to have one channel online at a time, type 1 into the "Minimum number of connected channels" field. If this channel goes down, one of the others will become active if doing so is consistent with their cost settings.

Option B:
Navigate to the channel menu for the channel you wish to modify. Tick the "Connect on demand" box. When this function is enabled, backup channel modules that aren't in use are powered off. This option saves on connectivity costs and power. If you tick "Connect on demand" for a module not associated with a backup channel, the "Connect on demand" setting will not have any effect.

6.4 Hub Redundancy

If you set up backup Hubs and configure Hub redundancy, should one of your active Hubs crash or malfunction, its identity and configuration will be automatically assigned to a backup Hub (hotspare).
Multiple active Hubs can be present in a redundancy network.

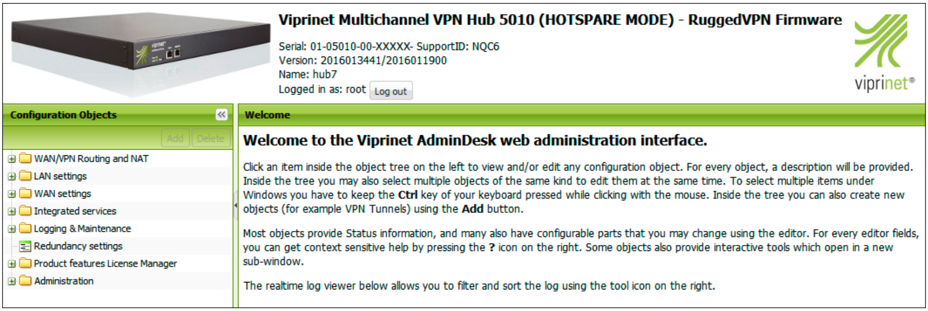
To activate this feature, install a Hub Redundancy license, available from your vendor. Depending on the Hub model, the license is already installed by default. See Appendix A6 for activation instructions.

Hotspare Hubs monitor the status of active Hubs with heartbeat packets. If an active Hub cannot be reached, or the spare can reach a configurable outside address that an active Hub cannot, then the spare becomes active within 90 seconds, already set to the configuration last received from the silent Hub.

All failures will be logged in the AdminDesk, although with the spare online, no special maintenance visit to the Hub is necessary.

Hub-to-spare associations can be configured in the AdminDesk.

The most basic Hub redundancy system involves one active Hub and one spare. Systems with more than ten active Hubs should have two spares. 10-15% of the total should be spares in larger installations.



Viprinet Multichannel VPN Hub 5010 (HOTSPARE MODE) - RuggedVPN Firmware

Serial: 01-05010-00-XXXXX- SupportID: NQC6
Version: 2016013441/2016011900
Name: hub7
Logged in as: root

Welcome to the Viprinet AdminDesk web administration interface.

Click an item inside the object tree on the left to view and/or edit any configuration object. For every object, a description will be provided. Inside the tree you may also select multiple objects of the same kind to edit them at the same time. To select multiple items under Windows you have to keep the **Ctrl** key of your keyboard pressed while clicking with the mouse. Inside the tree you can also create new objects (for example VPN Tunnels) using the **Add** button.

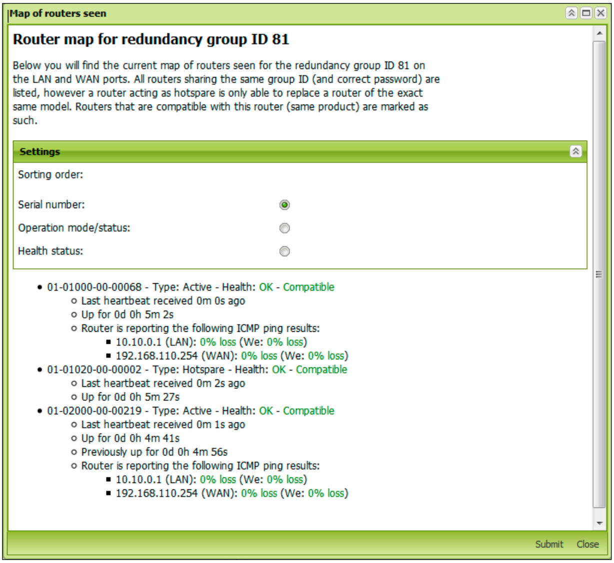
Most objects provide Status information, and many also have configurable parts that you may change using the editor. For every editor fields, you can get context sensitive help by pressing the **?** icon on the right. Some objects also provide interactive tools which open in a new sub-window.

The realtime log viewer below allows you to filter and sort the log using the tool icon on the right.

Figure 6.8 The AdminDesk on a hotspare Hub

Keep in mind

- To manually remove a Hub from a redundancy group without it being replaced by a hotspare, change its redundancy group password or redundancy group ID. If you just disable redundancy, a hotspare will take over.



Router map for redundancy group ID 81

Below you will find the current map of routers seen for the redundancy group ID 81 on the LAN and WAN ports. All routers sharing the same group ID (and correct password) are listed, however a router acting as hotspare is only able to replace a router of the exact same model. Routers that are compatible with this router (same product) are marked as such.

Settings

Sorting order:

Serial number: ●

Operation mode/status: ○

Health status: ○

- 01-01000-00-00068 - Type: Active - Health: OK - Compatible
  - Last heartbeat received 0m 0s ago
  - Up for 0d 0h 5m 2s
  - Router is reporting the following ICMP ping results:
    - 10.10.0.1 (LAN): 0% loss (We: 0% loss)
    - 192.168.110.254 (WAN): 0% loss (We: 0% loss)
- 01-01020-00-00002 - Type: Hotspare - Health: OK - Compatible
  - Last heartbeat received 0m 2s ago
  - Up for 0d 0h 5m 27s
- 01-02000-00-00219 - Type: Active - Health: OK - Compatible
  - Last heartbeat received 0m 1s ago
  - Up for 0d 0h 4m 41s
  - Previously up for 0d 0h 4m 56s
  - Router is reporting the following ICMP ping results:
    - 10.10.0.1 (LAN): 0% loss (We: 0% loss)
    - 192.168.110.254 (WAN): 0% loss (We: 0% loss)

Figure 6.9 A sample map of Hubs (routers, in the AdminDesk) seen by a hotspare Hub

Statuses of Hubs in a redundancy network
Active
• Normal operation. • Administrator options   • *Convert to hotspare*; this will clear the current configuration and reboot the Hub
Replacement
Administered through same IP address as replaced Hub • Info page on replacement status available at prior LAN IP address • Administrator options: • *Convert this replacement into a permanent Hub*: converts this Hub into a normal active Hub using the IP address and configuration of the replaced Hub – permanently   • *Release this Hub from replacing another Hub*: the Hub reboots and returns to hotspare mode so the central Hub can take back over againn
Hotspare
• Hotspares will always keep a copy of the configuration files of all active Hubs in the network • Monitors active Hubs' availability   • Administrator options: • *Convert router to normal/active operation*. This will reboot the Hub as a normal active Hub
Probe
• This is an automatic mode not controlled by the administrator • Hub is not available for administration via the AdminDesk • A failed Hub that restarts goes into this mode by default and checks to see if it has been replaced   • If it has been replaced, it does not become active again until the replacement is released, to prevent IP address conflicts   • If no replacement is detected, the Hub becomes active again • The system logs of other Hubs in a redundancy network record the status of a probe Hub

Table 6.3 Hub Redundancy modes

6.4.0 Configuring Hub redundancy

All settings are adjusted in the *Redundancy settings* menu.

- Convert at least one Hub to a hotspare by clicking *Convert router to hotspare* in the function pane of its *Redundancy settings* menu.
- Set the same *Group ID* and *Group Password* for all Hubs participating in the group you are administering.
- Enable *Redundancy* and click *Apply*
- Navigate to "Redundancy" in the menu tree on a Hub that should be part of the redundancy network. Expand it. Select the "Hosts to ping by ICMP" menu. Enter data for the relevant hosts. If one of the ping targets can't be reached by the master but can be reached by the hotspare, this hotspare will immediately go into replacement mode to replace the master.

Keep in mind

- Hubs will only monitor and replace each other if they share a cluster ID and have identical passwords
- Hotspares are synchronized with all Hubs in the redundancy group so settings are cached up to the minute.

- If a spare is not becoming active when expected or is causing an IP address conflict, check its *Map of routers seen*.
- If it doesn't appear, then Hub redundancy may not be on, or the wrong Group ID has been entered

6.5 Segmented VPN clients

The Hub Tunnel Segmentation feature allows you to segment your VPN client IP address pool and reuse the same address range multiple times. To activate it, install the Hub Tunnel Segmentation license available from your vendor. See Appendix A6 for activation instructions. To add Segmented VPN Clients, open *Segmented VPN Clients* and click *Add*. Then create a new pool of VPN Client IP addresses and specify a *Tunnel Segmentation ID*. See section 5.1 for information on non-segmented VPN clients.

Attention

- Each private IP address range you use needs to have a NAT entry in the Hub or on the backbone router, otherwise it won't be able to communicate with the public internet

6.6 SNMP monitoring

To view SNMP settings for your Node or Hub, navigate to *Integrated Services > SNMP Settings* in the menu tree. To view the entire menu, consult section 2.5.1.5.2. SNMP data type information is stored in an MIB (Management Information Base).

Basic SNMP
This functionality is included with your router by default and implements the MIB-II according to RFC1213 (http://tools.ietf.org/html/rfc1155). This MIB contains a list of all physical (LAN, WAN modules) and virtual adapters (tunnels, tunnel channels).

Extended SNMP
This functionality can be accessed by installing an add-on. It implements a specialized MIB that allows you to view Viprinet-specific information that is not included in MIB-II, and can be obtained from the downloads section of our website. Information that can be accessed with this MIB includes:

- Router Info: name, serial number, firmware version etc.
- Router Health: CPU load, memory usage, system/CPU temperature*
- Router Fans: status of fans*
- Router Interfaces: name, status, bandwidth to/from WAN, traffic
- Router Tunnels: name, status, bandwidth to/from WAN, traffic, remote serial
- Router Tunnel Channels: name, status, bandwidth to/from WAN, Traffic, backup status, packet loss,link stability

** This information will not be read on devices where this hardware is absent.*

Keep in mind

- You can only read values through SNMP, but not alter them. To change router settings, use the AdminDesk or CLI.
- Licenses to access extended functions are available from your supplier. See Appendix 6 for details on activating software licenses.

Attention

- Community and group names should not duplicate sensitive information like passwords
- See Appendix 9 for information on where and how to read SNMP values.

6.7 Traffic accounting

The Viprinet Traffic Accounting System collects data transfer records from all Hubs in your deployment for easy reference and simplifies the task of administering data transfer routing and allocations for individual users or individual Nodes. It is also possible to set thresholds and limits per user or Node and deliver email alerts to users or administrators when those thresholds have been exceeded. ISPs can use this system to track their customers' traffic volumes, and larger companies can use it to evaluate traffic from branch offices.

What you will need :

- A license, which you can purchase from your vendor. See Appendix 6 for activation instructions.
- A Linux-based server on which to run the tool. It should be running Apache 2 with MySQL 5.0 or above and PHP 5.1.x or above. This is where you will install the license. Email support@viprinet.com for the server setup manual.
- When you are setting up traffic accounting on your Hubs, you will need to have the URL of your traffic accounting server and log-in credentials easily accessible. You will also need to activate this functionality by checking the *Server Reporting Enabled* box in the *Traffic Accounting* menu.

The tool generates charts listing traffic loads for each VPN tunnel connected to the Node for the past 24 hours. This data is wiped when the Node reboots, and you can also reset the counts by clicking the *Reset counters* button. Green marks on the graphs correspond to user traffic, and red marks correspond to administrative traffic such as autotuning tests, overhead caused by the VPN protocol, and AES SSL encryption. Troubleshoot your network settings if the amount of administrative traffic is significant. To view the entire traffic accounting menu, see section 2.5.1.5.2.

6.8 Hub tunnel segmentation

This feature allows you to terminate several connections on the same Hub yet keep their data separate, as well as use the same IP addresses in multiple segments. To activate it, install a Hub Tunnel Segmentation license, available from your vendor. See Appendix A6 for activation instructions.

There is no single menu for this feature. Instead, configuration settings must be entered at four places in the Hub's AdminDesk:

- First, enter a *Tunnel Segmentation ID* in *Tunnel* settings.
- Second, in the *WAN/VPN Routing and NAT* > Masquerading (outbound NAT) Entries menu, enter the Tunnel Segmentation ID.
- Third, if applicable, in the *VPN Clients / Road warriors* > *Segmented VPN Clients* menu, you can create VPN client IP address pools with different segmentation IDs (as described in section 6.5).
- This feature is also needed to transport layer 2 VLAN information settings in RuggedVPN, and must be installed on the Node in that context.

6.9 Node stacking

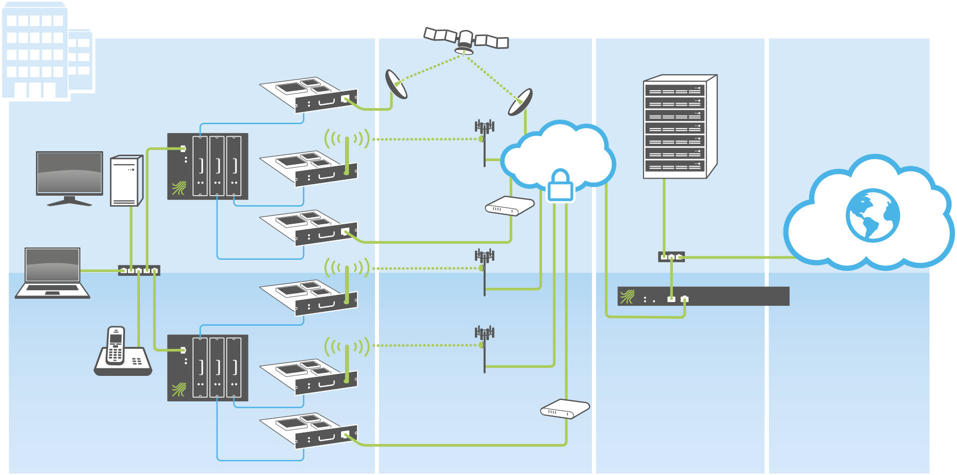


Figure 6.10 Stacked Nodes connect to a Hub

This section describes how to create stack arrays of Nodes. You cannot stack Hubs. Hub Redundancy, which is similar to stacking, is covered in section 6.4. You can view the stacking menu in its entirety in section 2.5.1.5.

Important concepts:

- All Nodes in a stack must be in the same location and on the same segment
- The stack is a virtual router. Although the master establishes the connection to the VPN tunnel, the tunnel and the Hub at the other end of it "see" the stack as one router reachable via the stacked IP address. Hosts "see" the same thing, and, like other routers, connect to the shared stack IP address.

How it works:

- You associate slave Nodes with a master Node that can use their WAN modules
- All Nodes will use the Shared IP address as their default gateway

Benefits of stacking:

- Redundancy: If a master or slave Node stops working, then the slave Node with the highest serial number adopts the stack's gateway IP address and serves as a temporary master. Slave Nodes can also be converted into permanent masters.
- Increased capacity: WAN connections from multiple Nodes are associated with one master.

Upper limits:

- The maximum stack size for any given deployment is determined by:
  - the capacity of the routers in the stack, which need to be able to take over for one another
  - the bonding capacity of the Hub the stack is connected to.
- The newest Viprinet firmware, RuggedVPN, can accommodate a maximum of 16 channels in a VPN tunnel.

You will need:

- Multiple Viprinet Nodes
- Individual IP addresses for each Node in the stack (private if they don't need to be accessed directly through the internet, public if they do)
- A shared default gateway IP address for the stack (public or private)

Keep in mind:

- All of the Nodes' IP addresses and the *Shared IP address* must be part of the same subnet
- The most powerful Node in the stack should be the master because this Node determines the bonding capacity of the stack
- The unit with the highest serial number will take over as master should the master fail (this will be the most powerful model)
- Configuration changes (other than security-related ACL adjustments, see the *Stacking hints* section) should only be made on the master. It will automatically transmit them to the slaves. The only settings that vary from slave Node to slave Node are the module settings
- All configuration changes made on a temporary master (a backup Node) will go away when the real master comes back online

6.9.0 Setting up a new stack

There are seven steps to setting up a new stack. They are:

1. Reset all Nodes
2. Set up master

- Setup tool – Node mode:
  - Modules
  - Tunnel
  - Channels
- AdminDesk
  - QoS

3. Set up Slave
- Setup tool – Advanced mode:
  - IP address
  - AdminDesk
  - Modules
4. Install Stacking licenses
5. Adjust LAN settings
6. Set *Shared IP* address
7. Configure Stacking settings

6.9.0.0 Step 1: Reset your Nodes

It is best to create a stack out of newly configured routers so you avoid accidentally introducing settings that aren't relevant to their new functions.

You can reset most Nodes by pressing the routers' reset buttons for five seconds with a paperclip or a pencil until the Viprinet logo starts flashing.

To reset a 500 series Node:

8. Remove all SIM cards.
9. Connect the Node to your computer or a LAN via its LAN interface.
10. Open the setup tool.
11. Select this Node in the detected routers list and click *Next*.
12. Confirm your action by clicking *Yes, I want to reset the router*.
13. The Node will reset to factory defaults and restart.
14. After about two minutes, the Node will appear in the router list in the setup tool again and can be reconfigured.

6.9.0.1 Step 2: Configure the master Node

Consult section 4.0, the quickstart guide, for information on how to set up a Node, and 4.1.0 for information on configuring VDSL and other wired connections. Remember that the LAN IP address needs to be in the same subnet as the slaves and the Shared IP address. Enter the Shared IP address as the default gateway. If you have already configured a tunnel and channels for this stack on the Hub, make sure that you match those settings precisely.

6.9.0.2 Step 3: Configure slaves

In the Setup tool

Follow the first six steps you did to configure the master in the setup tool, but in the sixth step, click the "Do something else" radio button, and select *Minimal config* in the dropdown menu. You will only be configuring the routers IP address and AdminDesk login information in the setup tool. When setup is finished, the router will reboot.

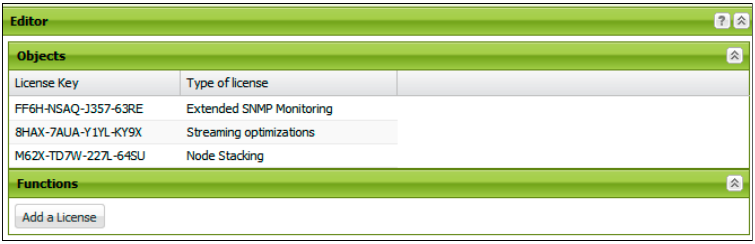
In the AdminDesk

Follow the same AdminDesk directions given in Chapter 4 for the master. As noted there, the computer you use to run the Setup Tool must be in the same network segment as the router or directly connected to it.

6.9.0.3 Step 4: Install Stacking licenses on masters and slaves

This procedure is the same for masters and slaves.

1. After the router reboots, log into the AdminDesk and select *Product Features License Manager* in the menu tree.



Editor

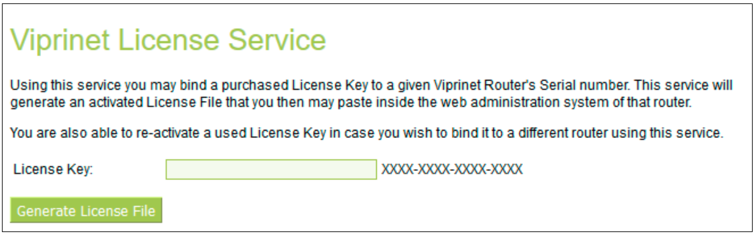
Objects

License Key	Type of license
FF6H-NSAQ-J357-63RE	Extended SNMP Monitoring
8HAX-7AUA-Y1YL-KY9X	Streaming optimizations
M62X-TD7W-227L-64SU	Node Stacking

Functions

Figure 6.11 The license menu screen

2. Direct your web browser to https://license.vipri.net.
3. Enter your license key, including the hyphens, in the *License key* field.



Viprinet License Service

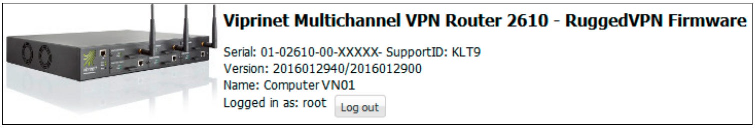
Using this service you may bind a purchased License Key to a given Viprinet Router's Serial number. This service will generate an activated License File that you then may paste inside the web administration system of that router.

You are also able to re-activate a used License Key in case you wish to bind it to a different router using this service.

License Key: XXXX-XXXX-XXXX-XXXX

Figure 6.12 Generating a license key

4. Click the *Generate License File* button
5. Enter the serial number of the Node you wish to install this license on. The serial number of the Node is listed in the *Vital Statistics* frame at the top of the AdminDesk page and on the router's back.



Viprinet Multichannel VPN Router 2610 - RuggedVPN Firmware

Serial: 01-02610-00-XXXXX- SupportID: KLT9
Version: 2016012940/2016012900
Name: Computer VN01
Logged in as: root

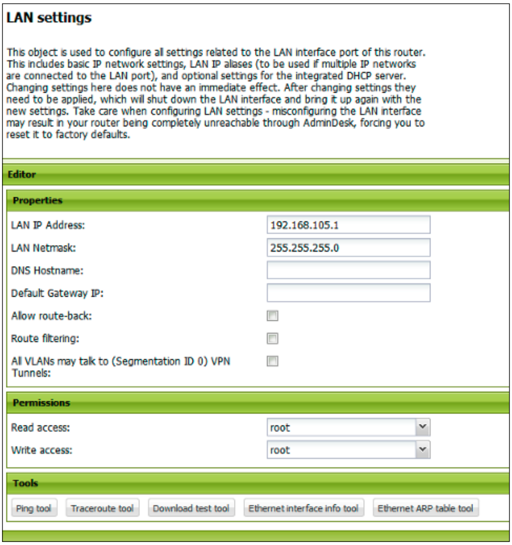
Figure 6.13 Vital Statistics frame

6. Click *Generate License File* again.
7. A webpage will load listing the license key just used and the serial number of your Node, as well as text starting "-----Begin License-----"and ending with "-----End License-----"; highlight and copy all of this text.
8. Log on to the AdminDesk for the Node you're adding stacking to. Expand *Product features license manager* in the menu tree.

9. Select the *Add a license* submenu.

10. Paste the text you copied from the licensing website into the *Change Value* field and click on *Save Changes*; after changes are saved, the *Change Value* field will clear itself.
11. Select *Logging and Maintenance* in the menu tree, and click *Reboot Router.* The router will reboot.

6.9.0.4 Step 5: Set up the shared stack IP address with LAN aliases on masters and slaves



LAN settings

This object is used to configure all settings related to the LAN interface port of this router. This includes basic IP network settings, LAN IP aliases (to be used if multiple IP networks are connected to the LAN port), and optional settings for the integrated DHCP server. Changing settings here does not have an immediate effect. After changing settings they need to be applied, which will shut down the LAN interface and bring it up again with the new settings. Take care when configuring LAN settings - misconfiguring the LAN interface may result in your router being completely unreachable through AdminDesk, forcing you to reset it to factory defaults.

Editor

Properties

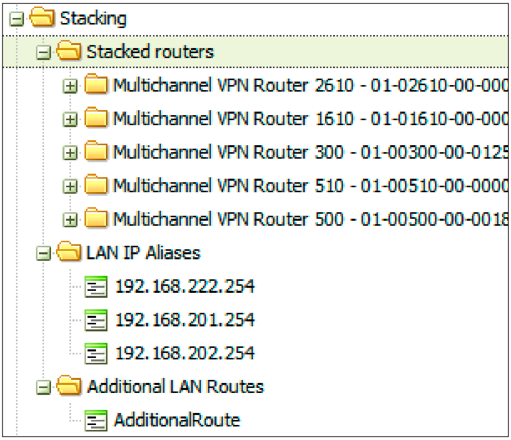
LAN IP Address:	192.168.105.1
LAN Netmask:	255.255.255.0
DNS Hostname:	
Default Gateway IP:	
Allow route-back:	□
Route filtering:	□
All VLANs may talk to (Segmentation ID 0) VPN Tunnels:	□

Permissions

Read access:	root
Write access:	root

Tools

Figure 6.14 LAN settings



Stacking
Stacked routers
Multichannel VPN Router 2610 - 01-02610-00-000
Multichannel VPN Router 1610 - 01-01610-00-000
Multichannel VPN Router 300 - 01-00300-00-0125
Multichannel VPN Router 510 - 01-00510-00-0000
Multichannel VPN Router 500 - 01-00500-00-0018
LAN IP Aliases
192.168.222.254
192.168.201.254
192.168.202.254
Additional LAN Routes
AdditionalRoute

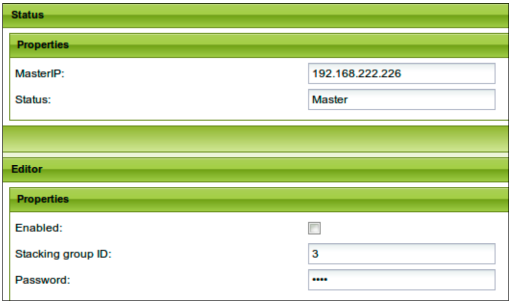
Figure 6.15 The Stacking menu and its submenus

The *Shared IP address* is the default gateway IP address for all Nodes in the stack. You will configure it in the main *LAN Settings* menu. If you haven't specified this setting in the Setup Tool, navigate to the LAN settings of each master and slave and enter the stack's shared IP address in the "Default gateway" field.

6.9.0.5 Step 6: Turn on Stacking for masters and slaves

These procedures are very similar for masters and slaves.

1. Select the *Stacking* item in the AdminDesk menu tree
2. Define a stacking group ID and password
3. Tick *Enabled*
4. Click *Apply* at the bottom right of the frame



Status

Properties

MasterIP: 192.168.222.226

Status: Master

Editor

Properties

Enabled: □

Stacking group ID: 3

Password: ••••

Figure 6.16 Setting the master IP address configuration

5. After your changes are applied, Nodes should show up under *Stacking – Stacked routers*

Slaves:

Slaves should show up in the *Stacked routers menu* as *Connected: True*.

Master:

In the AdminDesk menu tree, select the Stacking sub-item *Stacked routers*. Designate this Node as the master, then click *Apply*. This Node's serial number should automatically propagate to the *Current Master* field at the top of this menu.

All:

Restart stacking by clicking *Apply settings (and restart service)*

6.9.0.6 Changing the master

When you expand an existing stack with a model of Node more powerful than the others, you should make it the master. To do so:

- Go to the Stacked Nodes menu
- Select the appropriate Node as the new *Designated master* and click *Apply*.
- Applying this change will cause a short interruption in service for devices accessing the internet through the LAN this stack is connected to.

6.9.1 Stacking hints

- The safest way to remove a slave from the stack is to initiate a factory default reset
  - If you just turn off stacking, that slave Node will see an enabled tunnel and try to connect to it
  - Also DHCP could be enabled and, without the stack, active!
- The error “Stacking received corrupted broadcast notification” can be caused by an incorrect stacking password
- In a stack, a slave may be reached via it’s LAN interface by an intruder pretending to be on the LAN. ACL settings configured on the master are not automatically pushed to the slaves, unlike QoS settings. Therefore it is strongly recommended that you set up the ACLs on the slaves to protect them appropriately.
- Although a default gateway is not usually configured on Nodes, one must be set up on every stacked router and set to the shared LAN IP address. If this setting is not configured, or is configured incorrectly, traffic coming from slaves will not be correctly routed to the master that is administering all connections.

6.10 GEO tracking

The position of Nodes containing a GPS-capable LTE module can be tracked. Of the non-modular Nodes Viprinet offers, the 500 model does not have a GPS chip, but slot 4 in the 51X series is GPS-capable. To use this functionality, GPS has to be enabled in the *Position determination* menu for the relevant module. This data can be accessed by selecting the GEO Tracking item in the AdminDesk menu tree. To view the entire menu, consult section 2.5.1.5.0.0.

6.11 AccessPoint

This is a special menu, only relevant to 200, 500, and 5XX series Nodes that have integrated wifi access points that can provide 2.4 or 5 GHz (Dual Band) connectivity. To activate AccessPoint, navigate to its item in the menu tree, tick *Enabled* in the editor pane, and click *Apply*. Ensure that the radio channel, encryption, SSID, password, authentication mode, and authorized clients are configured appropriately for your network. This is also where you can view a list of currently connected clients.
To view the entire menu, consult section 2.5.1.5.0.0.

Chapter 7. Support

7.0 Troubleshooting

7.0.0 Ways to permanently lock yourself out of your router

If you lock yourself out of the AdminDesk, Support may be able to assist you, but in most cases you will have to reset and reconfigure the router.

7.0.0.0 Inappropriate port forwarding settings

When creating port forwarding entries for addresses associated with one of your routers, proceed very carefully. If you set *IP Protocol* to Ignore a port that the router uses locally (particularly 80 and 443, associated with the AdminDesk), this router will become unreachable! Forwarding to those ports will have the same effect.

7.0.0.1 Incautious ACL (Access Control List) changes

When you are setting deny rules, be very careful. If you overgeneralize, you could lock out access to every IP address.

7.0.0.2 Forgetting your "root" password

If you forget your "root" password, you will need to reset the router.

7.0.1 Ways to temporarily lock yourself out of your router

7.0.1.0 SSL fingerprint changes without flexible Access Control settings

If you regenerate or change the SSL certificate for the AdminDesk while you are connected to it via HTTPS, the HTTPS web interface will become unavailable until the new certificate is ready. This may take up to ten minutes. To be on the safe side, always make sure that you can reach the HTTP interface (see *ACL settings*) so you can access the AdminDesk via HTTP if you are locked out via HTTPS.
If you change the SSL certificate fingerprint for the AdminDesk, you will lose access to the SSL version of the Admin-Desk for at least ten minutes. Make sure that your ACLs allow access to the AdminDesk via HTTP while you are making this adjustment.

7.0.2 Resetting your router

If you reset your router all of your settings will be irretrievably lost. To use it again you will have to reconfigure it from the beginning, starting with the setup tool, as discussed in Chapter 4.

You can reset most Viprinet routers by pressing the reset button on their faceplate using a pencil or other pointed object for five seconds until the lights behind the Viprinet logo start flashing.

The 200 Node does not have a reset button; a reset is possible by unplugging the WAN module and use of the setup tool like described for 5xx series below.
500 and 51X series Nodes do not have reset buttons. To reset them:

- Remove all SIM cards
- Connect the Node to your computer or a LAN via its LAN interface
- Open the setup tool
- Select this Node in the detected routers list and click *Next.*
- Confirm your action by clicking *Yes, I want to reset the router*
  The Node will reset to factory defaults and restart
- After about two minutes, the Node will appear in the router list in the setup tool once more, and can be reconfigured.

7.0.3 Troubleshooting hints

7.0.3.0 Speed tests

It is preferable to use a CLI utility or one of Viprinet's built in utilities rather than a speed test website.
This is because:

- Speed test websites tend to get confused by autotuning unless you are downloading a larger file, which allows them to see the full adaptation curve
- If you are doing a speed test for mobile data, carriers track whether you are going to speed test websites and temporarily improve your service, resulting in misleading values.

When you are running a download test, view the router you are testing in the Monitor to assess its realtime performance.

7.0.3.1 The "Did you remember?" checklist

- Did you hit the *Apply* button? After you edit them and before you hit *Apply*, entry fields turn gray to indicate that a change has been made and not yet confirmed.
- If a link that you just configured is down, are the module, channel, and tunnel *Enabled*?
- Is the SSL fingerprint for the tunnel incorrect?
- Has a default gateway been entered that isn't needed?
- Are QoS and other settings in sync on the Hub and the Node?
- If you have just modified QoS, turn on *Log new connections* then check the syslog to see if your settings have been applied successfully
- Central Hubs in redundancy clusters and masters in Node stacks see different stability values than spares and slaves.
-

7.0.3.2 Quick and dirty fixes

- To make sure a Hub and a Node are in sync, copy the Hub QoS onto the Node and restart the tunnel.
- If the log window is empty, exit the AdminDesk and log back in again
- When all else fails, reconnect the tunnel; this function can be found in the Channel and Module menus

7.0.4 Forgotten IP addresses, temporary access drops, and VPN client problems

7.0.4.0 Forgotten IP addresses

If you forget the IP address of your router, open the setup tool and find the router in the list of active routers that the software finds when it scans your network.

7.0.4.1 Access drops

Creating a traffic routing rule may kick you from the AdminDesk. If you restart the LAN interface or make a change that affects the connection between your PC and the LAN IP address of the router, you will need to log back on.

Also, if you bookmark your router's AdminDesk in your browser after logging in, you must make sure that only the IP address and port forward for the router are included in the bookmark URL. If /exec is included you will not be able to access the router with this bookmark.

7.0.4.2 VPN Client

7.0.4.2.0 Client will not start

The message "Connecting to service" displays for an extended period, followed by "Service is not installed or could not be started successfully. Please make sure the Viprinet VPN Client Service is installed and enabled, then try again", after which the software closes.

Cause: The administrator password for your computer is necessary to run the Client.

- Each time you start the VPN Client, a prompt for the administrator password should appear unless you or your IT Support department have gone to the trouble of setting up the VPN Client to start along with Windows on system boot, in which case credentials are automatically supplied
- If for some reason the administrator password is not requested by the VPN Client software when it opens, the service will not be able to start.

Solution: Associate administrative rights with the program

- Open the directory your VPN Client software is in; most likely this will be /Program Files/Viprinet/VPN Client. Right-click on the executable. Select Start as Administrator in the menu that appears. You should then be prompted to enter your administrator password. If the Client window does not appear, check your system tray (not your start menu!) at the bottom of your screen for its icon. This does not make the program a startup item, but does make sure it prompts you for your administrator password when it is opened.

7.0.4.2.1 Client will not connect

The routing configuration in the client resets to match the settings on the Hub for the account being used every time you launch the client. If these settings are wrong or won't work with your setup, you may need to adjust these each time you launch until the settings on the Hub are correct.

7.0.5 Common configuration mistakes

- Incorrectly entered data (passwords; channel, tunnel; IP address; netmask)
- Settings left at defaults
- No firewall
- No virus protection software
- Consumer-level appliances
  - Make sure your hardware and software are rated for your level of traffic and intensity of use
- Wrong IP address type assigned to Node or Hub
  - Make sure public IP addresses are assigned to components that need to access or be accessed from the public internet
- Network plan mistakes
  - Example: Using an IP address segment for VPN clients that is duplicated elsewhere in your network. Although IP address pools properly set up on a Hub with segmentation enabled can conflict with one another without causing any problems, they should not conflict with ranges elsewhere in your network.
- Routing issues
  - NAT entry missing (only applicable if you are using private IP addresses)
  - routing entry missing or incorrect
- Improper use of bonding
  - Only one provider or medium; use multiple to benefit from bonding
  - Overuse of shared media
- Use of IPSec or additional VPN tunnels; this may work, but QoS settings will not be correctly applied
- Incorrect autotuning
- No autotuning
- Unrealistic or incorrect latency and bandwidth values specified
- Inconsistently applied QoS rules
- Need and don’t have an additional route to reach a different segment (e.g. another LAN)
- Auto PIN detect working improperly; switch it off
  - This may happen with private SIMs used by groups like police and other government workers, as well as those bought from resellers

7.0.6 Quality problems

7.0.6.0 Unsatisfactory transfer rates

7.0.6.0.0 Cause: Packet loss at the VPN tunnel

This problem causes re-transmissions in the VPN tunnel

- manifests as latency peaks (intermittent slowdowns of the connection)
- even 1% packet loss may lead to significant throughput drops
- autotuning will reduce performance in this situation, as it reduces the amount of bandwidth used

Diagnosis

- Use Viprinet Monitor and Viprinet Signal Monitor to track timing of packet loss
- Using mtr, traceroute, ping, and Wireshark, determine the source of packet loss, and address it as necessary:
  - the Hub
  - the LAN interface
  - the service provider

Solution

- Adjustments in the Hub or LAN interface or contact the service provider as applicable

7.0.6.0.1 Cause: Latency in the WAN too high

High latencies limit throughput due to rising bandwidth delay product
Frequent cause: Node to Hub link is experiencing high latencies due to

- overbooking
- packet loss
- improper autotuning
- inaccurate routing

Diagnosis

- Two simultaneous downloads are faster than one single download
- Use traceroute to check the connection between the Node modules and the Hub, watch for
  - packet loss
  - latency jitter
  - observe current latency in the Viprinet Monitor
  - latency values appearing both when data is being sent and when it is not
  - doubling latency peaks
- For comparison, start a download from a Linux or Windows 7 PC with TCP window scaling enabled

Solutions

- Find source and location of packet loss and set up wire screening if needed
- If the latency increase is caused by connection saturation, manually correct latency autotuning and maximum bandwidth settings if necessary to lower latencies
- Deactivate channels using traffic-heavy WAN lines until after you've done wire screening
- Reduce maximum bonding latency in the QoS class(es) affected using the high latency line
- Use *Bonding TCP optimizer* instead of *Bonding* in the QoS classes affected; latency per TCP connection will rise slightly in this class
- Insensitive to latency jitter in WAN
- Sensitive to packet loss at LAN
- DO NOT use with WLAN

7.0.6.0.2 Cause: Overrating capabilities of shared media

Some media–e.g. all wireless media and cable–are only available shared, and thus limited by the coefficient of overbooking (quality depends on how many users are on the network and how much bandwidth they are using)

- Advertised bandwidth specs of mobile media cannot be reached even in the laboratory
- Mobile media is also limited by the capacity of the provider's dedicated lines

Diagnosis
Important things to remember when using shared media:

- Bonding multiple cable lines may not result in increased bandwidth
  - for upstream speeds, bonding multiple cable accounts works quite well as they are not as overbooked.
- Bonding multiple SIM card modules serviced by the same provider will not result in increased bandwidth
- Availability is unpredictable
- Line parameters determined by Node speed tests not as accurate with shared media
- With 3G, latencies tend to be higher

Solutions

- Combine as many different media and providers as possible
- Set a lower optimal latency value in your autotuning settings
- Use directional antennas to reach different 3G cells

7.0.6.0.3 Cause: Poor Hub connection

Packet loss at the Hub not only affects performance but can confuse bandwidth autotuning.

Diagnosis
Despite a strong LAN connection, throughput may be low

- Download a large test file from the internet with a laptop connected to a switchport next to the Hub
- Observe data rate and stability of transfer rate; oscillations indicate packet loss
- Use traceroute to check the Hub's connectivity to all lines employed

Sources

- Weak datacenter connection
  - Incorrect traffic management at datacenter or facility at your main office
  - Properly equipped datacenters/onsite facilities should provide transfer rates around 100 Mbit/s without high latency

Solution

- Address Hub setup problem

7.0.6.0.4 Cause: Use of IPSec or additional VPN tunnels

Building a tunnel within a tunnel adversely affects service quality, as it obscures TCP-IP traffic that Viprinet's optimization tools need to analyze, prevents application of QoS templates, and increases processor load.

IPSec

- Is intended for dedicated lines and will not work well with volatile connection types
- Cannot be autotuned
- Cannot be optimized
- Viprinet's VPN tunnel is equally secure, easier to administer, and provides better performance

Solution: Remove additional tunnels

7.0.6.0.5 Cause: Use of additional protocol without WAN optimization

Protocols not designed for use on a WAN, such as Windows file shares (SMB/CIFS) often only send data in 64 KB chunks, and higher bandwidth and latency values will not increase their transfer rate.

Solution

- Create a dedicated QoS for affected traffic with a low maximum bonding latency
- Purchase a WAN optimizer which is adapted to this protocol and insert it in the network after the Hub(s) but before the Node(s)

7.0.6.0.6 Cause: Virus or trojan infection in LAN

Diagnosis

- Check log files at bottom of AdminDesk window for “Number of active flows has risen to” reports
- More than 1000 links to one host are often the result of infection

Solution

- Network structures susceptible to virus attacks should be secured by a suitable gateway and firewall

7.0.6.0.7 Cause: Configuration settings incorrect for external modem

Diagnosis

- Auto configuration is enabled in the Expected internet link capacity menu for a gigabit ethernet module connected to an external modem. The module will detect values that are incorrect.

Solution

- Set realistic values for your connection manually.

7.0.6.0.8 Cause: Inaccurate configuration

Common types

- Autotuning deactivated
- Unrealistic or incorrect latency and bandwidth values specified
- Inconsistently applied QoS rules
  - Data streams in the same class compete with one another; avoid sorting data streams with very different requirements into the same QoS class
  - Example: Interactive traffic, such as SSH connections, has been paired with high bandwidth video downloads in your settings. You discover that SSH connections have suddenly become very slow, as their latency has increased

Solution: correct settings

7.0.6.0.9 Cause: Other network components

Solution: Firewall and other appliances need to be rated for the appropriate capacity

7.0.6.1 Module will not connect

7.0.6.1.0 Cause: Automatic disconnects due to inappropriate MTU settings

Ethernet module menus include the property *MTU* (maximum transmission unit), which refers to packet size. If a timed channel (one whose cost depends on how many seconds, minutes, or hours it is used for) is delivered through this module and it always disconnects on connect, it may be a sign that the MTU value has been set too high.

Solution: Enter a lower MTU to resolve this problem. See section 2.5.1.5.0.0 for more information.

7.0.6.1.1 Cause: Antenna position or type

Solution: Position

- Antenna must be pointed at the correct tower
- Antennas must be pointed away from each other at 45 degree angles
- No two sets of antennas should be sitting next to each other.

Solution: Type

- 3G/UMTS and 4G/LTE connections will not work without antennas
- Do not use knuckle antennas mounted on the module for these kinds of connections; you must use a separate base

7.0.6.1.2 Auto APN detect working improperly

This may happen with private SIMs used by groups like police and other government workers, as well as those bought from resellers.

Solution: Turn off *APN Auto Configuration* and use data provided from the mobile carrier.

7.0.7 Stacking issues

7.0.7.0 "Stacking received corrupted broadcast notification"

Solution: Correct stacking password. If this does not help, contact Support.

7.0.7.1 Channel names

In most setups, channel names only have to differ within the same tunnel and the same names (e.g. Slot 1, Slot 2) can be used multiple times within the same deployment. However, if these channels are combined into one tunnel with stacking, they must be renamed.

Solution: Rename channels.

7.0.7.2 Incorrect IP address for slave

When a slave in a stack is mistakenly routed through its own IP address instead of the gateway IP address associated with the master, routing information is not pushed to it.

Solution: Correct slave IP address and default gateway.

7.0.8 Tunnel problems

7.0.8.0 Problem: Tunnel cannot be established

Possible causes:

- Tunnel channels are named inconsistently at Hub and Node
- An incorrect tunnel password has been entered
- The Hub's WAN IP address cannot be reached from the internet
- A private IP address was assigned instead of a public IP address
- The ACL of any provider or network component is blocking TCP port 443, which is needed to establish Viprinet tunnels
- None of your bonded connections are active, or none of them can access the internet
- Node is set to connect to default (blank) IP address instead of the actual public gateway IP address
- If you have more than one gateway beyond the Node for your LAN, you have to set up routing rules that indicate to which IP address traffic should be directed
- The SSL certificate fingerprint on the Hub has been changed

Diagnosis

- Check the Node's log for error messages
- Check the Hub's log for error messages
- Check to see if it the Hub is receiving tunnel connections
- Ping the Hub's WAN interface from the Node; ask Support if you do not know how

Solution

Check each item in the checklist above. Adjust the relevant values.

7.0.8.1 No throughput existing tunnel

Frequent causes:

- NAT entry missing
- Routing entry missing
- Routing entry incorrect
- Hub is not connected to the ISP gateway it should be using

Diagnosis

- Use traceroute to check the connection from the host in the LAN to the internet destination; if you do not know how to do this, contact Support
- Can the Node be reached / reach the internet?
- Ping the ISP gateway
- Ping the Hub's LAN IP address
- Ping the Hub's gateway IP address
- Check network plan and routing concept
- Check Node and Hub configuration for common mistakes

7.0.8.2 No connection existing tunnel

Cause: Too many connections

- New connections cannot be set up: the maximum number of possible connections per host has been attained.

Symptoms

- When using a proxy, additional connections will be refused by this host. If this host is blocked, the number of connections will drop and further traffic will be permitted.

Diagnosis

- Check the log file on the Node for the message: "Number of active flows has risen to 25000"; this indicates hosts being used to send spam or torrenting files
- If no proxy or firewall is being used, the log file alert will read: "Source host IP [ADDRESS] reached maximum traffic flow limit, dropping connection" for outgoing traffic or "Destination host [IP ADDRESS] reached maximum traffic flow limit, dropping connection" for incoming traffic; [IP ADDRESS] will be the address of the affected host

Solutions

- Scan the host machine with your virus-protection software to determine if it has been infected or compromised, and look for any other evidence of a virus or trojan horse infection
- Should you need to employ more than 5000 connections per host, contact Viprinet Support

7.0.8.3 Tunnel drops out or reboots for no reason

Frequent causes

- Simultaneous reconnect of all connected lines. Could happen with DSL lines if no "Reconnect at time of day" is configured.
- All connections in the Viprinet deployment are the same type of medium, provided by the same ISP, or both
- Node has been overwhelmed with connections
  - Possible Source 1: DoS attack
  - Possible Source 2: Virus infection circulating in the LAN
- Compatibility conflict between networking hardware being used
- Firewall problems
- Rare: overheating components, damaged LAN cable, electricity fluctuations

Diagnosis

- Check log file on the Node and Hub for
  - reports of line outages
  - reconnects
  - "Number of active flows has risen to" reports; this may indicate DoS attacks or virus infections
- Check the *Router Health* page in the AdminDesk

7.1 Additional support resources

7.1.0 Self-service options

1) This FAQ answers general questions about Viprinet and its technologies, many of which are also covered in this manual: http://www.viprinet.com/faq

2) You can download the files which were included on your setup CD as well as additional support and information resources at: http://www.viprinet.com/downloads

3) Firmware release notes are available at: http://www.viprinet.com/firmware

4) For more background information on basic networking concepts, consult:

Tanenbaum, Andrew S., Wetherall, David J.
Computer Networks. 5th ed.
New Jersey: Prentice Hall, 2010. ISBN-13: 9780132126953
http://computernetworks5e.org/blogs/

Appendices

A0. Glossary

3G An abbreviation that encompasses all third-generation wireless telephone technologies, including UMTS, CDMA2000, HSPA+, EVDO, and others.

4G An abbreviation for fourth-generation wireless telecom technologies, including LTE, WiMAX, and others. 4G hardware is downward compatible with 3G connections.

ACL (Access Control List) A list of rules that determine what traffic is permitted to access specific services on the router. ACLs are stateless, which means each traffic request is handled independently.

AdminDesk (Viprinet) A browser-based administration tool that is part of the firmware of each Viprinet Node and Hub. You can can access it via your browser, using your router's IP address as the URL.

ADSL Asymmetric DSL, a consumer-grade service.

ADSL2+ Annex A The most commonly implemented version of the ADSL + standard, which sends data over POTS (plain old telephone service) lines rather than high speed digital lines. ADSL+ offers more downstream bandwidth than the original ADSL standard.

ADSL2+ Annex B Unlike the other annexes to the ADSL+ specification, this one is intended for use with digital ISDN connections.

AES Advanced Encryption Standard. A specification for the protection of electronic data that was accepted by NIST in the United States to replace DES (Digital Encryption Standard) in 2001. It is capable of protecting multiple network layers.

APN Access point name. The name of a gateway that allows communication between mobile networks and the open internet.

ARP table Address Resolution Protocol Table. Used to match MAC and IP addresses on LANs.

autotuning A method of making automated adjustments to the network congestion avoidance parameters of TCP connections.

backbone A high-capacity network that connects multiple smaller networks to one another, whether within an organization or from region to region. Backbone routers route the connections that are part of a backbone.

backup score A measure of transfer rates used to configure when backup channels or Nodes will become active to take the place of disconnected or malfunctioning ones.

bandwidth A measure of a connection's transmission capacity, expressed as bit per second (kilobits, megabits, etc).

bandwidth delay produc The maximum amount of data a network circuit can handle at any one time. Equal to the connection capacity expressed as bit per second (kbps, in most Viprinet settings).

bonding Combining multiple connections or connection types to access better reliability or bandwidth than would be available with one connection alone. Another term sometimes used is teaming.

bonding capacity A measure of a router or tunnel's processing capacity, expressed as bit per second.

cable (DOCSIS) An international telecommunications standard that utilizes the cable television infrastructure just as DSL uses telephone lines. Its formal name is Data Over Cable Service Interface Specification.

CDMA (Code Division Multiple Access) A radio technology that allows multiple terminals, hosts, or stations to transmit over a shared medium. The IS-95 and 2000 CDMA standards (2G and 3G respectively) have primarily been used for mobile phones in North America, although the 450 standard is beginning to be used in areas where existing technologies are too resource-intensive to deploy.

cell The location of a transceiver (transmitter-receiver) in a cellular radio network, usually a cell tower. Every network includes multiple cells, each of which provides coverage within a certain range. Adjacent cells use disparate frequencies to prevent interference.

channel In the context of this manual, channel refers to an internet connection between one

	hot-plug module and the Hub that connects it to the public internet. The VPN tunnel over which data is transmitted from the Node to the Hub is composed of bonded channels.
CIDR	(Classless Inter-Domain Routing) A method for allocating IP addresses. Classful routing allocates addresses in 8-bit groups; this type of routing can allocate addresses of any group size. CIDR notation compactly indicates the number of bits in the netmask associated with an IP address, as in this example: 192.168.100.0/22.
command line tools (See Appendix 1)	Utilities without a GUI, which the user gives commands to and receives output from in a terminal window or a CLI (command-line interface).
commit interval	In this context, the number of seconds between updates to the traffic accounting log; see Section 2.5.1.5.2, page 62.
DC-HSPA+	Dual-carrier Evolved High Speed Packet Access. It is an enhancement of UMTS that allows the user to connect to multiple transceivers (cells) at once.
destination	The host to which a packet is being sent.
DHCP server	A server that assigns internet protocol parameters, including addresses, using dynamic host configuration protocols.
DNS	Domain Name System. Translates domain names into IP addresses, and vice versa.
DoS attack	Denial of service attack. An attempt to make a machine inaccessible, usually by flooding it with connection requests.
downstream	Refers to incoming data and connections. Downloads come downstream.
DSL	Digital Subscriber Line. A type of broadband internet delivered over telephone lines.
DSLAM	Digital subscriber line access multiplexer. Connects DSL customer lines to their ISP's backbone.
EDGE	Enhanced Data rates for GSM Evolution. An extension of GSM intended to provide improved transmission speeds.
encrypted binary file	A computer file that contains data which has been protected with encryption.
ethernet frame	A digital transmission unit that encapsulates an ethernet packet's payload, providing source, destination, and protocol information as well as a Frame-Check-Sequence (FCS)
ethernet interface	A physical socket on a device that allows the user to connect it to a wired ethernet network. Most Viprinet devices have a LAN and a WAN ethernet interface.
EV-DO	(Evolution Data Only) A mobile internet standard that is an upgrade of CDMA2000.
Gateway	A router that connects different LANs (subnets).
GUI	Graphical User Interface.
GPS	Global Positioning System.
GPRS	General Packet Radio Service. Amobile internet service, typically priced by volume.
host	A device, such as a network card, that is capable of having an IP address.
hot plug module	A network card specialized for insertion in Viprinet's Nodes; a wide variety are available for a range of connection types. These can be removed or inserted in the Node while it is running.
hotspare	A spare Hub in a redundancy cluster that is available to become active instantly if it is needed to replace a malfunctioning or disconnected device in the same cluster.
HSPA+	See DC-HSPA+. Non dual-carrier.
Hub	A Viprinet VPN Concentrator that routes VPN connections from multiple Nodes, as well as reassembles and decodes split and encrypted packets
ICMP	Internet Control Access Protocol. Used to relay pings from diagnostic utilities and other sources to check the status of Nodes or Hubs. ICMP is used by utilities like traceroute to detect the location of network faults.
interpolation	The instantiation of new data points based on existing ones. For example, it is used for resizing images when the user zooms in, as they may do when viewing signal waveforms in the Viprinet Monitor.

interface
A physical network adapter fitted with a controller chip, connector, and drivers that allow it to be accessed with the user's OS, or the means by which a user interacts with a program or system, as in the term "command line interface".

IP address
A label indicating the location of a host in a network. Can be private or public, static or dynamically assigned.

IP, dynamically assigned or static
Dynamically assigned IP addresses are assigned each time the host connects to the ISP; static IP addresses do not change.

IP address block, range, pool
A series of consecutive IP addresses.

IP address header
Indicates protocol version, source, destination, and other information about the packet it is appended to.

IPSec
A VPN protocol for authenticating and encrypting individual packets. It is redundant in Viprinet deployments and should not be used as it can cause connectivity problems.

ISP
Internet Service Provider.

kbps
Kilobit per second.

LAN
Local Area Network.

LAN IP alias
An additional IP address assigned to a LAN interface.

LAN interface
See ethernet interface.

latency
Delay in processing network data. The time that passes between the time of a packet's transmission and the reception of a response.

layer 2 network
A switched network.

leased line
An exclusive (rather than shared) symmetric telecom line provided by an ISP to two or more locations in a client organization. The quality of the connection and associated support is defined in a contract called an SLA (Service Level Agreement).

link stability
Describes the availability of a network connection. Network access that does not drop out often is stable. Unreliable network access is not stable.

logging
Keeping a record of a Node, Hub, or connection's state.

LTE
Long Term Evolution. A fourth-generation mobile wireless standard.

MIB
Management Information Base. A database used to keep track of hosts in a network so they can be managed with SNMP.

modem
A device that modulates signals so they can be more easily transmitted and received. It may, for example, translate digital data into electrical signals for transmission over telephone lines.

Monitor (Viprinet)
A utility that allows network administrators to assess the status of all connections associated with one Node in a Viprinet deployment in realtime.

MPLS
Multiprotocol Label Switching. A method used to send data through the shortest path possible to its destination.

ms
Milliseconds.

NAT, NAT entry
Network address translation. Used to substitute public addresses for those of hosts with private IP addresses to allow them to access the internet. A NAT entry is a record of what translated and original IP addresses correspond to each other.

netmask
Mask used to divide a network into subnets, such as LANs. See Section 1.3 for a more in-depth explanation.

network plan, network topology
The structure of a network.

network segment
Either a physical (cabling) or a logical (IP address range) subdivision of a network.

Node
In a Viprinet context, a router that enables LANs to connect to a Hub with a variety of media and providers.

NTP
Network time protocol.

overbooking	Selling more of a resource than is actually available. When ISPs do this, customer connectivity suffers.
packet -	A unit of data transmitted through a packet-switched network.
packet loss	The phenomenon of packets failing to reach their destination. Has multiple potential causes.
printer	Lorem ipsum dolor sit amet. Wait. Printers are out of hell: Klaatu Verata Nektu!
private IP address	One that, by convention, is not accessible to the public internet.
protocol, communications	A system of rules for data exchange within or between computing devices.
providers	Internet service vendors.
proxy	An intermediary between servers.
public IP address	One of a limited number of unique IP addresses that can be used on hosts that directly communicate with the open internet without using NAT. IPv4 addresses have been exhausted. IPv6 offers an extended address space as well as facilitates the creation of easier-to-use routing tables.
QoS	Quality of Service. Used to assign latency, allocated bandwidth, and other priority and connectivity settings to individual channels.
queue	The ordering of packets in the transmission buffer of a Node or Hub.
random early detection algorithm	A tool that monitors network queue size and discards or marks and delays packets to maintain queue size. Hosts transmitting the most are more likely to have their packets dropped. Does not work well with protocols sensitive to dropped packets, like VoIP.
redundancy cluster	A active-passive configuration of multiple operating Viprinet Hubs and spare systems.
root	The superuser account included by default on most computing systems.
router	A device that forwards data packets between networks. All Viprinet Hubs and Nodes are routers.
routing	How packets are passed through a network.
satellite access	Internet connectivity provided through communications satellites, usually to remote locations.
SDSL	A digital subscriber line with symmetric upstream and downstream connectivity; these are more expensive than asymmetric connections, which are usually consumer grade.
setup tool	The first utility you use to configure your Viprinet Node or Hub.
shared media	A connection that serves multiple users at the same time. Connection quality is affected by high demand. This includes cable broadband and all wireless connections.
Signal Monitor (Viprinet)	A utility that allows network administrators to evaluate signal strength for wireless connections.
SIM card	Subscriber Identity Module. A chip that stores subscriber information for a mobile plan.
slaved Node	A slave system which is offering its available WAN connections to the stacking master.
SNMP	Simple Network Management Protocol; for managing hosts on IP networks.
source	The host that is sending a given stream of packets.
speed test	A test of connection quality. Speed tests can be run manually using the Download test tool in the module slot and LAN settings menus on the AdminDesk.
SSH	Secure Shell. A cryptographic protocol for secure network transmissions.
SSL	Secure Sockets Layer. An encryption protocol for connections between servers and clients, often used on e-commerce sites.
stacking	Connecting backup slave Nodes to a master Node. This is the Node equivalent of a Hub redundancy cluster.
stalled	Data no longer being transmitted or received
subnet	hosts are subdivided into subnets by adding a routing prefix to their IP addresses. All hosts in the same network have the same routing prefix.
subnet mask	The netmask for a LAN.

switch, network A device that physically connects devices on a network and passes packets between them. Viprinet Hubs are not switches. They are routers.

switchport One port on a switch. Switch ports filter and forward packets between network segments.

tail drop a very simple networking algorithm. When a network queue is full, packets are dropped until there is room in the queue.

TCP Transmission Communication Protocol. Part of the suite used to transmit data through computer networks, including the internet. It divides data to be transmitted over networks via IP (internet protocol) into packets.

TCP window; window scaling Data being transmitted is chunked into TCP windows; the window size is how big or small that chunk is.

TCP/IP The internet protocol suite that is used on all networks. IP means internet protocol.

torrenting Downloading (usually large) files from several peers simultaneously. Multiple outgoing connections to the peers and a payload of significant size make this kind of operation very bandwidth-hungry.

ToS Type of Service; used in the IP header of a IP packet to classify the priority of the transported data.

traceroute A diagnostic tool for finding out the path packets are taking through a network and assessing sources of delay.

traffic The movement of packets through a network.

UDP User Datagram Protocol. A stateless protocol that does not require packet acknowledgments (ACKs). Allows hosts to establish a link without setting up a transmission path beforehand. Applications include domain name system and network time protocol communications, streaming media, and VoIP.

UMTS Universal Mobile Telecommunications System. A 3G standard based on GSM.

upstream Refers to outgoing data or connections. Uploads go upstream.

VDSL Very high bitrate Digital Subscriber Line. Asymmetric medium often used to deliver television and telephone as well as internet service ("triple-play"). Uses telephone lines, but is faster than ADSL.

VoIP Voice Over IP; internet telephony.

VLAN Virtual LAN. A Layer 2 seperation, to create multiple distinct broadcast domains that are mutually isolated.

VPN client Virtual Private Network Client. Allows users to connect to a Viprinet Hub (in this context). Also refers to any software that allows a remote user to function as part of a corporate intranet, for example.

VPN tunnel Virtual Private Network Tunnel. In this context, these connect VPN clients and Nodes to Hubs. It is composed of the Node's bonded channels. See channel.

WAN Wide area network. A network distributed over multiple LANs or geographic regions.

WAN interface See ethernet interface. Connects a Hub to a wide area network; this could be either the public internet or other portions of an organizational network.

WiMAX A high-powered wireless broadband communications standard intended to provide an alternative to wired connections.

wire screening interference elimination or line diagnostics.

A1. Relevant command-line tools for network troubleshooting

There are a number of Unix command-line tools that are necessary or useful to diagnose the sources of connectivity problems. Tools accessible from Viprinet's AdminDesk allow you to access some of these without using a command-line interface; see the table below. There are several versions of some utilities, and this is not an exhaustive list, but it should serve as an entry point for users new to network administration. You can invoke the built-in manual (or "man page") for every piece of software here by entering man at the command line while running it, but as man pages aren't always helpful, reference links are provided here when possible.

Name	Purpose	Reference
iperf	Used to generate TCP and UDP data streams to measure the throughput of a network connection; useful for diagnosing cases of high latency	Documentation: http://software.es.net/iperf/invoking.html
netcat	A very versatile program, common uses include port scanning and port listening; useful for diagnosing connectivity and latency problems	Manual, last original author version (1996): http://nc110.sourceforge.net/ GNU version manual (2004): http://netcat.sourceforge.net/
mtr	Combines the functionality of ping and traceroute; useful for diagnosing causes of high latency	Documentation: http://www.bitwizard.nl/mtr/
ping	Used to test how much time packets take to reach one host from another; useful for diagnosing cases of high latency or apparent loss of connectivity	The program was written in 1983, and the best resource for it is its man page or a general internet search.
tcpdump	Used to read the contents of network packets	Documentation: http://www.tcpdump.org/#documentation
traceroute	Used to display the route and delay of packets in transit; useful in diagnosing the causes of high latency	The program was written in 1987, and the best resource for it is its man page or a general internet search.
Wireshark	A versatile tool, used to examine a variety of different kinds of network data in many protocols	Documentation and resources: https://www.wireshark.org/docs/

Table A1.0 Command-line Tools

A2. A list of ports commonly used for Viprinet deployments

When setting up your network, you'll need to make sure that these ports are open. If there is some reason that it is not feasible to open them, please contact Support. If you are having connectivity problems, you may want to make sure that your firewall or other tools are not interfering with traffic through these ports.

Port number	Port type	Where	Used for
443	TCP	WAN at Hub	Incoming connections; Mandatory for Viprinet deployment to function
443	TCP	LAN	AdminDesk access
80	TCP	LAN	AdminDesk access
22	TCP	LAN	SSH CLI
161	UDP	LAN	SNMP
20022	TCP	LAN and WAN	Maintenance access
67	UDP	LAN	DHCP (private)
68	UDP	LAN	DHCP (private)
53	TCP and UDP	LAN	DNS (private)
123	UDP	LAN	Access to external time servers to set routers' internal clocks
514	UDP	LAN	System log messages

Table A2.0 Port listing

A3. CIDR notation

Classless Inter Domain Routing is used

- to assign IP addresses without using address classes
- to keep track in an easy to read way of how many bits of an IP address identify the network and cannot be incremented to add a host

Things to know

- a suffix is added, e.g. /24 to show how many bits of the address identify the network
  - In this example, ranges from 192.168.1.0 to 192.168.1.255 are available.
- all zeroes can be left out; e.g. 10/8 for 10.0.0.0/8

Example:

CIDR: 192.168.2.7/24

- Address: 192.168.2.7
- Netmask: 255.255.255.0
- Binary: 11111111.11111111.11111111.00000000
- Available IP address range: 192.168.2.0 to 192.168.2.255
- Number of hosts that can reside on this network: 254, using numbers between 1 and 254
- Network address: 192.168.2.0
- Broadcast address: 192.168.2.255

CIDR	Number of addresses	Netmask	Netmask in binary
/8	16777216	255.0.0.0	1111 1111.0000 0000.0000 0000.0000 0000
/9	128x65536	255.128.0.0	1111 1111.1000 0000.0000 0000.0000 0000
/10	64x65536	255.192.0.0	1111 1111.1100 0000.0000 0000.0000 0000
/11	32x65536	255.224.0.0	1111 1111.1110 0000.0000 0000.0000 0000
/12	16x65536	255.240.0.0	1111 1111.1111 0000.0000 0000.0000 0000
/13	8x65536	255.248.0.0	1111 1111.1111 1000.0000 0000.0000 0000
/14	4x65536	255.252.0.0	1111 1111.1111 1100.0000 0000.0000 0000
/15	2x65536	255.254.0.0	1111 1111.1111 1110.0000 0000.0000 0000
/16	65536	255.255.0.0	1111 1111.1111 1111.0000 0000.0000 0000
/17	128x256	255.255.128.0	1111 1111.1111 1111.1000 0000.0000 0000
/18	64x256	255.255.192.0	1111 1111.1111 1111.1100 0000.0000 0000
/19	32x256	255.255.224.0	1111 1111.1111 1111.1110 0000.0000 0000
/20	16x256	255.255.240.0	1111 1111.1111 1111.1111 0000.0000 0000
/21	8x256	255.255.248.0	1111 1111.1111 1111.1111 1000.0000 0000
/22	4x256	255.255.252.0	1111 1111.1111 1111.1111 1100.0000 0000
/23	2x256	255.255.254.0	1111 1111.1111 1111.1111 1110.0000 0000
/24	1x256	255.255.255.0	1111 1111.1111 1111.1111 1111.0000 0000
/25	128x1	255.255.255.128	1111 1111.1111 1111.1111 1111.1000 0000
/26	64x1	255.255.255.192	1111 1111.1111 1111.1111 1111.1100 0000
/27	32x1	255.255.255.224	1111 1111.1111 1111.1111 1111.1110 0000
/28	16x1	255.255.255.240	1111 1111.1111 1111.1111 1111.1111 0000
/29	8x1	255.255.255.248	1111 1111.1111 1111.1111 1111.1111 1000
/30	4x1	255.255.255.252	1111 1111.1111 1111.1111 1111.1111 1100
/31	2x1	255.255.255.254	1111 1111.1111 1111.1111 1111.1111 1110
/32	1x1	255.255.255.255	1111 1111.1111 1111.1111 1111.1111 1111

Table A3.0 CIDR

A4. Network address translation

NAT is used to substitute private IP addresses with public ones that allow them to access the internet. Ports are also translated. See the illustration. Nodes should not be configured to provide NAT services, as it will interfere with the basic functioning of the deployment. The Hub needs to be able to differentiate between hosts on the LAN in order to apply certain QoS settings. ISPs can also provide NAT services.

The process includes the following steps:

- a host on a LAN, say a laptop computer, is sending packets to a website
    - the host is using a private IP address within the LAN

- the host's packets are received by the Node that manages its network segment
- the Node sends the packets on to the Hub through the VPN tunnel
- the Hub substitutes a public IP address for the host's private IP address and puts an entry in its lookup table correlating the two IP addresses
- when packets travel back to the host, the process is reversed

A5. Pairing connection types and their uses

Viprinet can help you get the most out of the connections you pay for, but you will have the best results when you use connections whose bandwidth, speed, and latency are most appropriate for your purposes, although this may not always be possible. If you only have access to higher-latency lines, it will be difficult to use interactive applications. If you only have access to lower-bandwidth lines, bonding several of them in a mixture of shared and non-shared media can help you access the amount of bandwidth you need. If you need reliable service, then bonding several lower-reliability lines can give you access to much higher reliability. If cost is a problem, then bonding several lower-cost connections can allow you to save money. For more information, see the case studies on our website.

Application	Desired characteristics	Appropriate connection types
VoIP	Low latency	Any DSL
Videoconferencing	Low latency and high bandwidth	DSL, cable
Frequent transfer of large files, e.g. serving media	High bandwidth	DSL, cable
Continuous use of low-bandwidth services, e.g. POS (point-of-sale) systems, access to databases	Reliability	Use a mixture of providers and technologies
Client consumer use (e.g. planes, trains, busses, lodgings)	Reliability	3G and 4G, maybe satellite if affordable

Table A5.0 Applications and appropriate connection types

Type of connection	Cost	Average latency	Average bandwidth	Average reliability
Leased lines and MPLS	High	Low	High	High, SLAs usually in place
ADSL	Low	Low, ~20-60ms	~20 Mbps (medium) for downloads, lower for uploads	Medium
VDSL	Low	Low	~50 Mbps (high) for downloads, lower for uploads	Medium
SDSL	High	Low	~2 Mbps both ways	~98.5%; line outages of up to five days a year

Table A5.1 Wired media connection types, costs, and characteristics

Type of connection	Cost	Average latency	Average bandwidth	Average reliability
LTE/4G, HSPA+	Most medium; Satellite high	Medium	Full capacity is ~50 Mbps upstream and ~100 Mbps downstream Often throttled to ~7.2 Mbps both ways limited by distance to tower limited by circuit load	Low. Depends on provider coverage and landscape
UMTS/3G/CDMA/EV-DO, EDGE	Low	Medium	Varies by load and distance to tower	Low. Depends on provider coverage and landscape
WiMAX	Varies	~50 ms	Medium ~25 Mbps	30mi/40km range
Satellite	High	High, >600ms	Low ~1-4 Mbps upstream and ~4-10 Mbps downstream	Low. Depends on provider coverage and technology
Cable	Low	Medium	Medium ~20 Mbps for downloads, lower for uploads	Medium

Table A5.2 Wireless media connection types, costs, and characteristics

A6. License Activation

Viprinet offers five add-ons which expand on the base functionality of your Hub or Node's firmware, increasing the level of control you have over your network. Licenses are bound to the serial number of the router they have been installed on. They cannot be moved to another router.

Traffic accounting functionality requires a license and its settings can be modified in the AdminDesk but it is installed on a separate accounting server and not discussed in this manual. Contact your vendor for a traffic accounting license and the manual for that product.

Add-ons available as of this writing are:

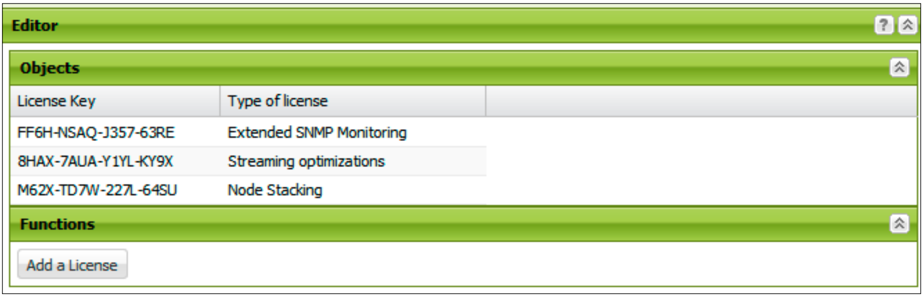
Add-on	Where to install	Where to read more about it
Hub Redundancy	Hub only	Section 6.4
Hub Tunnel Segmentation	Classic: Hub only RuggedVPN: must be installed on the Node if you wish to transport VLANs (layer2) over the tunnel (layer3)	Section 6.8
Node Stacking	Node only, each Node in the stack needs a license	Section 6.9

Add-on	Where to install	Where to read more about it
Streaming Optimization	Must be installed on Hub and all Nodes that connect to it	Section 6.0.1.1.0
Enhanced SNMP Monitoring	Install on the router you wish to monitor	Section 6.6
VPN Client (one needed for each user)	Hub only	Section 5.1

Table A6.0 Available add-ons

License keys for these add-ons can be purchased from your vendor. Each router will have to be activated individually.

To activate your licenses, follow these ten steps:



License Key	Type of license
FF6H-NSAQ-J357-63RE	Extended SNMP Monitoring
8HAX-7AUA-Y1YL-KY9X	Streaming optimizations
M62X-TD7W-227L-64SU	Node Stacking

Figure A6.0 Licenses added to a router

1) Direct your web browser to https://license.vipri.net.
2) Enter your license key in the *License key* field.
3) Click the *Generate License File* button.
4) Enter the serial number of the router you wish to install this license on. The serial number is listed in the *Vital Statistics* frame at the top of the AdminDesk page and on the router's back.
5) Click *Generate License File* again.
6) A webpage will load listing the license key just used and the serial number of your router, as well as text starting "-----Begin License-----"and ending with "-----End License-----"; highlight and copy all of this text.
7) Log on to the AdminDesk for the router where you wish to enable the add-on. Expand *Product features license manager* in the menu tree.
8) Select the *Add a license* sub-item.
9) Paste the text you copied from the licensing website into the *Change Value* field and click on *Save Changes*; after the changes are saved, the *Change Value* field will clear itself.
10) Select Logging and Maintenance in the menu tree, and click Reboot Router. The router will reboot.

A7. Instructions for VPN Client users

To use the Viprinet VPN Client, you will need:

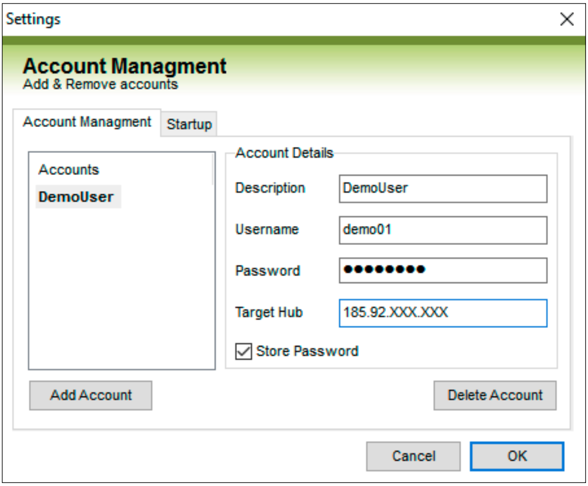
- The username and password for a VPN Client account, provided by your administrator
- The WAN IP address of the Hub you will be connecting to
- A computer running:
  - Windows XP, Vista, 7, or 8
  - or Mac OS X, versions 10.6 through 10.9 as of this writing.

(It is possible to run the Client under emulation using VMWare, Parallels, or VirtualBox, but this is not supported by Viprinet. It is not possible to run the Client using Wine or the emulator QEMU given the way they interface with the computer's OS.)

Troubleshooting

- If your client won't start and says it can't contact the webservice, remove and reinstall it.
- If you are going to be using a web browser and want that traffic to be sent through the VPN tunnel, special routing must be configured.
- If you log in as an administrator and still can't access your resources, make sure that the routing is set correctly. Each time the VPN Client starts, the routing is reset to match the configuration settings for this account on the Hub. Your administrator will follow the directions in section 5.1 to set up the client on the Hub end.

1) Follow the steps for installing the VPN Client described in section 3.2.
2) Click *Manage Accounts*, and enter the username and password given to you by your administrator.



Settings

Account Managment
Add & Remove accounts

Account Managment | Startup

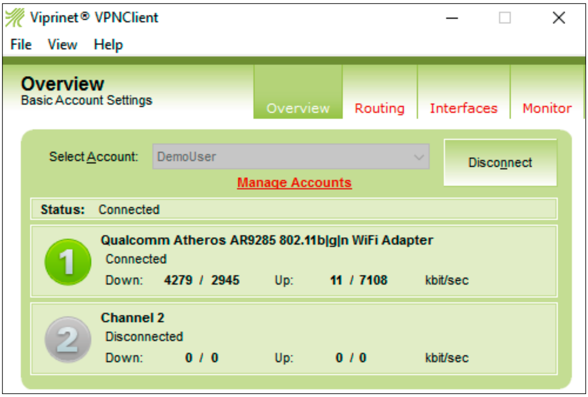
Accounts
DemoUser

Account Details

Description: DemoUser
Username: demo01
Password: ●●●●●●●●
Target Hub: 185.92.XXX.XXX
☑ Store Password

Figure A7.0 The account setup window

3) When your account is enabled, the device you are using to connect to the internet should have a green circle next to it in the *Overview* window as in figure A7.1.



Select Account: DemoUser

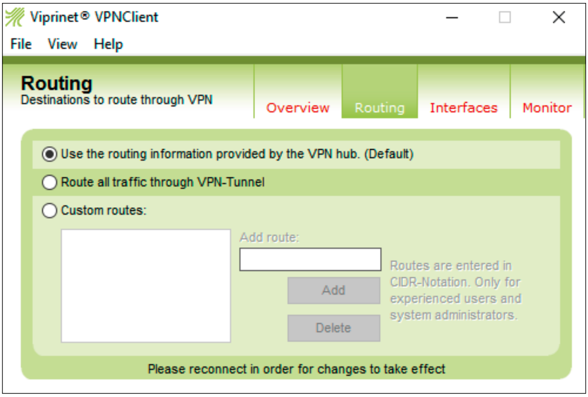
Status: Connected

Qualcomm Atheros AR9285 802.11b|g|n WiFi Adapter
Connected
Down: 4279 / 2945 Up: 11 / 7108 kbit/sec

Channel 2
Disconnected
Down: 0 / 0 Up: 0 / 0 kbit/sec

Figure A7.1 One active connection

4) Follow your administrator's instructions in regard to routing settings. In most cases, you should use the default.



● Use the routing information provided by the VPN hub. (Default)

○ Route all traffic through VPN-Tunnel

○ Custom routes:

Routes are entered in CIDR-Notation. Only for experienced users and system administrators.

Please reconnect in order for changes to take effect

Figure A7.2 Routing settings

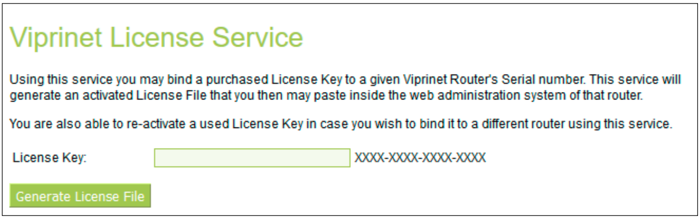
A8. Congestion control algorithms

There is a lot of information about different congestion control algorithms available on the internet. This quick overview provides a sense of the differences between these algorithms. Cubic is the default for Viprinet deployments and should be fine for most purposes.

BIC (Binary Increase Congestion control) – Best for large high-speed networks with long lines. Uses a binary search algorithm to determine the maximum sustainable transmission window size.
Reno – Detects congestion by tracking packet drops.
Cubic (current default) – A less aggressive descendant of BIC. Window size calculations are influenced by the period of time since the last congestion event and the amount of time between congestion events.
Highspeed - Uses ACK and packet loss to detect congestion. Received ACKs trigger increased window size; lost packets trigger decreased window size. Best for long high-bandwidth lines.
H-TCP – Similar to high speed, but less aggressive. However, non-lossy flows do tend to monopolize bandwidth.
Hybla – Best for terrestrial or satellite radio links with long RTTs.
Illinois – Uses packet loss and queuing delay to determine whether to decrease or increase transmission window size and at what rate to do so. As with many other algorithms in this list, it is best for long high-speed lines.
LP (low-priority) – Intended for low-priority traffic, this algorithm only allocates excess bandwidth rather than providing a “fair share” of bandwidth to all flows as other algorithms do.
Scalable – Decreases window size with each packet lost.
Vegas – Detects incipient congestion based on RTT (round-trip time) values.
Veno – A more precise version of Reno; only modifies the sender-side of that algorithm.
Westwood – A sender-side only modification of New Reno specialized to improve transmission rates
over long, unreliable, high-bandwidth, dynamic lines. Uses ACK stream to analyze available bandwidth so transmission window size can be modified as it becomes available.
YeAH (Yet Another Highspeed TCP) – Also well-suited for long high-bandwidth lines, this algorithm is intended to balance demands for window rescaling with router buffer limitations by responding to latency fluctuations. Because it de-prioritizes packet loss as a parameter, it is appropriate for lossy links.

A9. Generating license keys

To generate your license key(s):



Viprinet License Service

Using this service you may bind a purchased License Key to a given Viprinet Router's Serial number. This service will generate an activated License File that you then may paste inside the web administration system of that router.

You are also able to re-activate a used License Key in case you wish to bind it to a different router using this service.

Figure A12. License key page

1) Purchase a license from your vendor
2) Direct your web browser to https://license.vipri.net.
3) Enter your license key, including the hyphens, in the License key field.

4) Click the *Generate License File* button

5) Enter the serial number of the Node or Hub you wish to install this license on. The serial number is listed in the V*ital Statistics* frame at the top of the AdminDesk page and on the router's back.

6) Click *Generate License File* again.

7) A webpage will load listing the license key just used and the serial number of your router as well as text starting "-----Begin License-----"and ending with "-----End License-----"; highlight and copy all of this text.

8) Login to the AdminDesk. If you are installing a VPN Client license, follow the instructions in section 5.1 for setting up VPN Client accounts. Otherwise, navigate to *Product features License Manager* in the menu tree. Click *Add a license*. Paste the license key into the pop-up window that appears. Click *Submit* in the popup, then *Apply* in the menu after it closes.

viprinet®