



BROADBAND AGGREGATOR BA-4000

Broadband Aggregator BA-4000

BA-4000 User Manual

Release 1.00.15

February 2012

Legal information

Copyright

Copyright © 2010-2012, VP Networks, Inc. All rights reserved. No part of this documentation may be reproduced in any form or by any means without prior written authorization from VP Networks, Inc..

Disclaimer

Precautions have been taken to ensure accuracy of the information provided in this manual. Typographic or pictorial errors that are brought to our attention will be corrected in subsequent issues. VP Networks, Inc. reserves the right to revise this documentation and to make changes in content from time to time without obligation to provide notification of such changes. VP Networks, Inc. provides this documentation without warranty expressed, implied, statutory, or otherwise and specifically disclaims any warranty of merchantability or fitness for a particular purpose. VP Networks, Inc. may make improvements or changes in the product(s) described in this documentation at any time. Product specifications in this manual are provided for the convenience of our customers. They are all correct at the time of publication. VP Networks, Inc. reserves the right to make product changes from time to time, without prior notification, which may change certain specifications or functions described here. VP Networks, Inc. recommends you to check for changes or updates before using the equipment. The handling, installation and usage of the VP Networks products are applicable to specified environments and should be used in recommended conditions. The equipment does not or will not provide protection against abuse, misuse, improper installation or maintenance. It is important that installation, operation and maintenance are performed in accordance with instructions supplied in the manual. Electricity and electrical devices must always be treated with caution and respect.

Trademarks

All trademarks and service marks specified herein are owned by their respective companies.

Technical support

VP Networks, Inc.
350 Townsend Street, Suite 320
San Francisco, CA 94107
Email: support@valuepointnet.com

Feedback

VP Networks, Inc. strives to provide quality documentation that enhances the user's experience with our products. We are constantly improving our guides and have a genuine interest in ensuring that our guides are easy to use and enable users to quickly find information they need. We invite you to be part of this process; please email your comments regarding VP Networks, Inc. product documentation and web content to: info@valuepointnet.com

Table of Contents

About this document	1
Purpose.....	1
Release information	1
Intended audience	1
Document organization.....	1
Contact information	1
Introduction.....	3
BA-4000 Features	3
BA-4000 User Interface.....	5
Logging on to BA-4000 user interface	5
BA-4000 user interface layout.....	6
Working with BA-4000 user interface.....	7
Internet Settings	9
WAN Interfaces	9
WAN-3G interfaces	11
LAN Interfaces	13
Routing / Load Balancer	16
Static Routes	16
Policy Routing	17
IP Pass-through	18
Load Balancing	19
Failover Only	19
Load balance and Failover	20
Quality of Service (QoS)	21
Setting File Sharing rules.....	21
QoS Settings WAN/LAN.....	21
QoS Classes	22
QoS Classifier Settings	22
Open VPN Client	25
Firewall	28
MAC/IP/Port filter settings	28
Port Forwarding	30
Virtual Servers	31
Source Network Address Translation (SNAT).....	32
Network Mapping	34
System Security	35
Management.....	37
SNMP.....	37
Remote SysLog.....	37
Status.....	38
System Info	38
Network Status.....	38
Statistics	39
Bandwidth Graph.....	39
DHCP Clients	40
System Command	40
System Log	40

System Administration	41
System Management	41
Administration Settings	41
DDNS Settings	41
NTP Settings.....	42
Configuration Management.....	43
Upgrade Firmware.....	43
Warranty and License.....	43

List of tables

Table 1 Internet Settings: WAN: Static WAN parameters	9
Table 2 Internet Settings: WAN: PPPoE parameters.....	10
Table 3 Internet Settings: WAN-3G	11
Table 4 Internet Settings: WAN-3G: Advance Settings.....	12
Table 5 Internet Settings: WAN: Configure Link Properties	12
Table 6 Internet Settings: LAN.....	14
Table 7 Internet Settings: LAN: Configure DHCP.....	14
Table 8 Internet Settings: LAN: Add static lease	15
Table 9 Routing/Load Balancer: Static Routing.....	16
Table 10 Routing/Load Balancer: Policy Routing.....	17
Table 11 Routing/Load Balancer: IP Pass-through	18
Table 12 Routing/Load Balancer: Load Balance.....	20
Table 13 QoS: QoS Setup of WAN/LAN Interfaces	21
Table 14 QoS: QoS Classes	22
Table 15 QoS: QoS Rules for WAN and LAN interface.....	22
Table 16 Open VPN: Secure VPN Client.....	25
Table 17 Firewall: MAC/IP/Port filter settings: Basic Settings	28
Table 18 Firewall: MAC/IP/Port filter settings	28
Table 19 Firewall: Port Forwarding.....	30
Table 20 Firewall: Port Forwarding: Virtual Servers	31
Table 21 Firewall: SNAT	32
Table 22 Firewall: Network Mapping	34
Table 23 Firewall: System Security Settings.....	35
Table 24 Administrator: System Management: DDNS Settings	41
Table 25 Administrator: System Management: NTP Settings	42

About this document

This chapter provides information about:

“Purpose”

“Release information”

“Intended audience”

“Document organization”

“Contact information”

Purpose

This document is to introduce and describe the BA-4000 User Interface (UI) and provide details related to network configurations using BA-4000 UI.

Release information

This is Issue 1 of this document for BA-4000, Release 1.4.

Intended audience

This guide is intended for system and network administrators for working with the BA-4000 UI. It also provides instructions for administering, configuring and monitoring the networks and services using BA-4000. Knowledge of networking and technologies such as ADSL and Ethernet is assumed.

Document organization

Chapter 1 provides information about the scope of the BA-4000 User Interface Guide

Chapter 2 provides an overview of BA-4000 and a brief description of the features supported by BA-4000 in the current release.

Chapter 3 provides a description of BA-4000 User Interface and provides the procedures to log into the UI.

Chapter 4 provides detailed information for configuring all the functionalities and features supported by BA-4000.

Chapter 5 provides information about troubleshooting using the tools supported by BA-4000.

Chapter 6 provides information about System Administration supported by BA-4000.

Contact information

Send your comments or feedback on this document to info@valuepointnet.com

Introduction

The BA-4000 Broadband Aggregator increases your Internet bandwidth and lowers your cost by connecting multiple ISP connections into one LAN network. The LAN bandwidth is the combined total of the separate WAN connections, both upstream and downstream.

The BA-4000 supports up to 200 Mbps across 3 Ethernet WAN connections, with proportional load balancing from 5 to 95 percent per port. The 4000 has automatic failover in the event a WAN connection goes down. In addition, it has a 3G USB connection for further back up.

The BA-4000 has policy based routing and Quality of Service to support data, video, and voice across multiple connections. It allows you to bind IP addresses to specific WAN ports to support VPN connections.

Pricing for the BA-4000 will dramatically lower your infrastructure costs, making previously unreachable venues affordable and increasing your Return on Investment.

BA-4000 Features

Some of the features supported by BA-4000 are:

Robust Bandwidth Aggregator with Seamless failover and load balancing between multiple ISP connections

Integrated firewall capabilities like stateful packet inspection.

Quality of Service to provide appropriate priority to different applications/users/data flows relatively to guarantee acceptable performance levels

Secure OpenVPN tunnels (with authentication and encryption) to transport sensitive data across public networks.

Flow based management interface to classify traffic based on any combination of network, application, and content and user information to customize application delivery policies across the WAN.

BA-4000 User Interface

The BA-4000 User Interface acts as a user-friendly tool to configure multiple WANs for bandwidth aggregation with an integrated firewall for stateful packet inspection. BA-4000's reliable and secure feature-set enables efficient configuration of the customer network and network resources for reliable and resilient operation.

Logging on to BA-4000 user interface

BA-4000 User Interface (UI) can be accessed from a web-browser with appropriate licenses obtained from VP Networks, Inc.

This procedure provides instructions to log on to BA-4000 User Interface (UI).

To log on to BA-4000 User Interface

Complete the following procedure to log on to BA-4000 UI:

1. Switch on the BA-4000. Connect one end of the Ethernet cable on the LAN port of BA-4000 and the other end to a LAPTOP or desktop. Ensure the laptop / desktop IP is configured in the same LAN segment of BA-4000 segment which is 192.168.100.x
2. Set the laptop/desktop IP as 192.168.100.100; MASK 255.255.255.0;GW 192.168.100.1; DNS 192.168.100.1
3. Launch a web-browser, either Mozilla Firefox or Internet Explorer and navigate to the following URL:

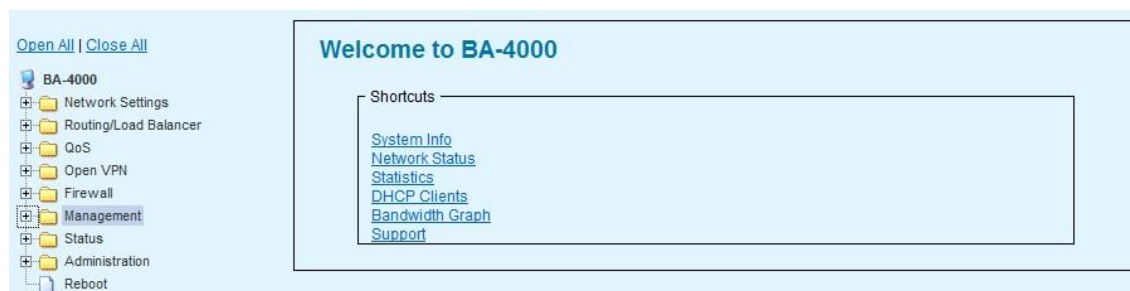
<http://192.168.100.1/>

192.168.100.1 is the default LAN IP address of BA-4000.

Result: The **Login** screen is displayed.

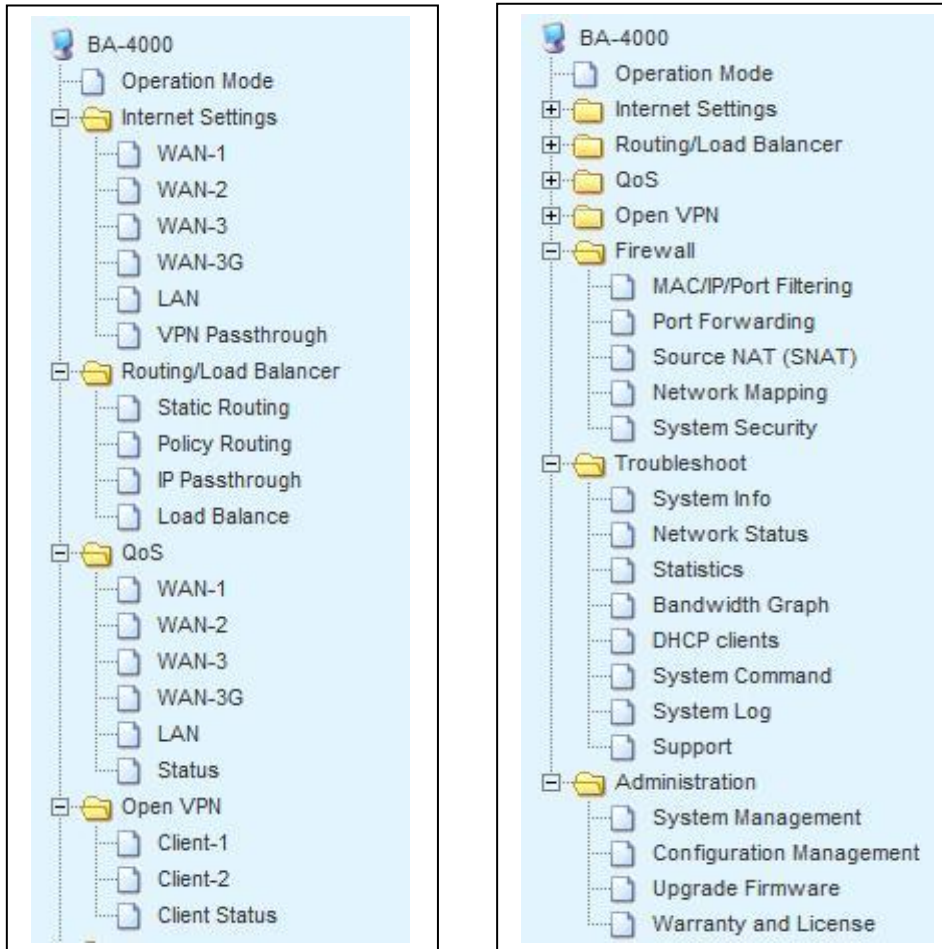
4. Enter the appropriate BA-4000 UI username and password.
5. Default Username: "root" and Password: "root"
6. Click "**OK**".

Result: The home page of BA-4000 will be displayed.



BA-4000 user interface layout

BA-4000 has a web-based, easy-to-navigate graphical user interface used to configure, administer, and secure the network. This section provides a description of the BA-4000 user interface layout.



BA-4000 UI can be classified into the following regions:

- Header – consists of the logo and shortcuts to perform certain operations on BA-4000 user interface
- Menu bar – consists of the main menu options used for navigation and configuration

Information related to BA-4000 software version, licenses, firmware version, and MAC address of the Ethernet interfaces can be viewed from the BA-4000 UI “status” tab.

Working with BA-4000 user interface

BA-4000 configuration menus are Internet Settings, Routing/Load Balancing, QoS, OpenVPN, Firewall, Troubleshooting and Administration from the BA-4000 user interface. Configuring these features and functionalities requires user input in terms of values for certain attributes. Some fields/attributes are auto-populated by the system while the others must be configured by the user. The fields/attributes that are mandatory for a particular configuration need to be filled in by the user.

Careful configuration of the network using the features supported by BA-4000 enables high performance, secure and reliable networks with remote management and monitoring.

Internet Settings

All interfaces supported by the system can be configured from the BA-4000 User Interface. BA-4000 supports WAN, WAN-3G and LAN.

WAN Interfaces

BA-4000 supports two types of WAN interfaces. The number of WAN interfaces supported by the system is indicated on the UI. The WAN interfaces and the associated parameters can be configured from BA-4000 UI. The WAN interfaces supported can be of the following types:

Static WAN configuration: In this configuration, the ISP allocates a static global IP address for the WAN connectivity.

PPPoE configuration: In this configuration, the ISP provides the global IP address automatically using PPPoE protocol for WAN connectivity.

DHCP configuration: The ISP provides the global IP address automatically. No configuration required on the BA-4000. Just chose “DHCP” and click Apply.

Note: If you are using an external modem for a PPPoE connection, ensure that the modem is configured in the bridged mode.

The BA-4000 supports configuration of WAN link properties. These parameters are used to define the firewall and link failure detection methods for the interface. These properties are used by the load balancer and firewall. BA-4000 also supports IP aliasing, a process of adding more than one IP address to a network interface.

Table 1 Internet Settings: WAN: Static WAN parameters

Field	Description
Interface IP	IP address of the Static WAN interface on BA-4000 used to connect to the remote network. This IP address is usually given by the ISP.
Subnet Mask	Subnet Mask corresponding to the Interface IP; this field is populated by the system by default. However you can modify the subnet mask. This is usually given by the ISP.
Gateway	IP address of the remote router which interfaces with the network. This IP address is usually given by the ISP.
Alias Interface IP	IP address of the alias (to the WAN interface) being added. BA-4000 supports max of 20 Alias IP on the WAN interface. Default: “Disabled”
MAC Clone	Configures MAC address for the Wan Ethernet interface. This overrides the factory-set MAC address on that interface. This is useful for MAC-locked Internet connections like cable modems and DSL. If this field is left empty, the factory-programmed MAC address will be used. Format: 12:34:56:78:90:12

Wide Area Network (WAN-1) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type:	STATIC (fixed IP) ▼
Static Mode	
IP Address	192.168.66.199
Subnet Mask	255.255.255.0
Default Gateway	192.168.66.10
Additional IP Addresses (IP Alias)	Disable ▼
MAC Clone	
State	Disable ▼

Table 2 Internet Settings: WAN: PPPoE parameters

Field	Description
Provider Name	Name of the ISP.
User Name	User name provided by the ISP for authentication purposes.
Password	Password provided by the ISP for authentication purposes.
Confirm Password	Password provided by the ISP for authentication purposes; must match the value of the Password field.
PPPoE MTU	Maximum Transmission Unit of the PPPoE interface; this field is populated by the system. Default: 1492
Operation Mode	Keep Alive (Used to always connect with the ISP connection)
Modem Access IP Address	IP address of the BA-4000 interface connected to the external modem. This IP address must be in the same subnet as the modem IP address.
Modem Access Subnet Mask	Subnet Mask corresponding to the Interface IP
MAC Clone	Configures MAC address for the Wan Ethernet interface. This overrides the factory-set MAC address on that interface. This is useful for MAC-locked Internet connections like cable modems and DSL. If this field is left empty, the factory-programmed MAC address will be used. Format: 12:34:56:78:90:12

Wide Area Network (WAN-1) Settings	
You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.	
WAN Connection Type:	PPPoE (ADSL) ▼
PPPoE Mode	
User Name	test1
Password	••••••
Verify Password	••••••
PPPOE MTU	1492
Operation Mode	Keep Alive ▼
Modem Access	IP Address <input type="text"/> Subnet Mask <input type="text"/>
MAC Clone	
State	Disable ▼

WAN-3G interfaces

BA-4000 supports configuration of 3G USB modem interfaces in the standard PPP configuration. WAN-3G interfaces are used to connect to the internet through dialup modems. The modems supported by BA-4000 are external USB analog modems, external USB wireless devices. However, PCI WIN modems are not supported. BA-4000 also supports configuration of the WAN-3G link properties used to define the firewall and link failure detection methods for the interface. These properties are used by the load balancer and firewall.

Note: The external modems must support the modem AT command set.

Table 3 Internet Settings: WAN-3G

Field	Description
Description	Description of the dial-up interface being configured.
Interface Type	If PPP is chosen, Enables the WAN-3G interface in the PPP configuration. Values: Disable / PPP Default: Disable
User Name	User name provided by the ISP for authentication purposes.
Password	Password provided by the ISP for authentication purposes.
Number to dial	Number to dial, provided by the ISP.
3G Device	Port to which the modem is connected. Values: USB0-USB6, ACM0-ACM2, AutoDetect Default: "AutoDetect"

Table 4 Internet Settings: WAN-3G: Advance Settings

Field	Description
APN	Access Point Name provide by the ISP
PIN	PIN of the simcard used in the USB modem
Modem init String1	AT command string to turn on the transmitter on the wireless modem.
Modem init String2	AT command string to turn on the transmitter on the wireless modem.

Wide Area Network (3G-USB-MODEM) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

Modem Connection Type:		PPP
3G Settings		
User Name	valuepoint	
Password	*****	
Dial Number	*99#	
3G Device	USB0	
Advanced Settings	<input checked="" type="checkbox"/>	
APN	version3g	
PIN		
Modem Init String 1		
Modem Init String 2		

Table 5 Internet Settings: WAN: Configure Link Properties

Field	Description
Network Type	<p>Values: Public / Captive</p> <p>Default: Public (Most of the cases the choice is Public interface only) Captive network is chosen for connectivity like VSAT, Leased Line or MPLS and this connectivity is used between multiple branches of the same organization</p>
Link Priority	<p>Priority assigned to the configured interface/link. The higher the number, higher the priority. The priority for each link is (This Link/Total Priority). Setting two links to 10 and 1 yields about 10 to 1 load balancing. Setting 10 and 10 is the same as 1 and 1. Range: 1-9</p> <p>Default: 1</p>
MTU	<p>Configures the maximum transmission unit of the interface. Range: 68 – 1518</p> <p>Default: 1500</p>
Default Firewall Policy	<p>Used to enable or disable the firewall for the selected interface. Values: Drop incoming connections / Accept incoming connections</p> <p>Default: Drop incoming connections</p>

NAT	NAT maps all of the private IP addresses on a LAN network to the single IP address supplied by the ISP. Values: Enable / Disable Default: Enable
Proxy ARP	Checkbox to enable Proxy ARP, a technique in which the host (BA-4000), answers ARP requests intended for another machine behind the public network. Proxy ARP can help machines on a subnet reach remote subnets without the need to configure routing or a default gateway.
VPN Traffic	Used to configure whether to allow VPN traffic via this WAN interface or not. Values: Allow Always / Do not Allow / Allow when link is down Default: "Allow Always"
Link Detection Method	Select the method to monitor the interface. Values: 1. Ping Gateway IP (Gateway IP of the ISP) 2. ARP Gateway IP (Gateway IP of the ISP; Use if the ISP's gateway does not respond to ICMP echo messages) 3. Ping Remote IP (IP address of the remote host) 4. Link/Cable Detect 5. None, Always UP

Link Properties	
Network Type	Public Network ▼
Link Priority	1 ▼
MTU	1500
Default Firewall Policy	Drop Incoming Connections ▼
NAT	Enable ▼
Proxy ARP	Disable ▼
VPN Traffic	Allow Always ▼
Link Failure Detection Method	Ping Gateway IP ▼
<div> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </div>	

LAN Interfaces

The LAN interfaces can be configured in the Static LAN mode. BA-4000 supports the configuration of LAN link properties with an option to define the link failure detection method for the LAN interface. It also supports the configuration of Static leases that are used to assign static or fixed IP Addresses to the DHCP clients; primarily used for servers, printers etc.

The following table provides the details regarding the parameters associated with the LAN interface:

Table 6 Internet Settings: LAN

Field	Description
Interface IP	IP address of the Static LAN connection for the concerned port; usually this IP address is associated with the private network. Example 192.168.100.1
Subnet Mask	Subnet Mask corresponding to the Interface IP address
Proxy ARP	Checkbox to enable Proxy ARP, a technique in which the host (BA-4000), answers ARP requests intended for another machine behind the public network. Proxy ARP can help machines on a subnet reach remote subnets without the need to configure routing or a default gateway.
MAC Address	MAC address of the LAN Port of BA 4000 will be automatically configured
NAT	NAT maps all of the private IP addresses on a LAN network to the single IP address supplied by the ISP. Default: Disable
DHCP Type	Checkbox to enable DHCP server for this interface. When enabled, the DHCP parameters must be configured as stated in the following section.

Table 7 Internet Settings: LAN: Configure DHCP

Field	Description
Start IP Address	Start of the IP address in the Address pool for DHCP clients.
End IP Address	End of the IP address in the Address pool for DHCP clients.
Subnet Mask	Subnet Mask corresponding to the Interface IP address
Gateway	Default Gateway corresponding to the Interface IP address
DNS server	BA-4000 has Built-in and Custom options in the DNS server settings. If the option custom is chosen, the Primary and Secondary DNS need to be provided. Default: Built-in
Lease time (Hours)	Time in hours that is assigned to a lease, after which indicates the lease expires. Range: 1 – 99 Default: 24

Table 8 Internet Settings: LAN: Add static lease

Field	Description
MAC address	MAC/Physical address of the Ethernet Interface.
IP Address	IP address to be assigned to the host. It must be in the same subnet as the Interface IP and must be outside the pool range specified in the DHCP configuration.

Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters.

LAN Setup	
IP Address	192.168.100.1
Subnet Mask	255.255.255.0
Proxy ARP	Disable ▼
MAC Address	00:00:00:44:44:44
NAT	Disable ▼
DHCP Type	Server ▼
Start IP Address	192.168.100.100
End IP Address	192.168.100.200
Subnet Mask	255.255.255.0
Default Gateway	192.168.100.1
DNS Servers	Built-in ▼
Lease Time	86400
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Static Leases		
No	MAC	IP
1	00:01:02:03:04:05	1.2.3.4
2	00:1f:16:09:ed:04	192.168.100.77
3		
4		
5		
6		
7		
8		
9		
10		

Routing / Load Balancer

Static Routes

You can manually configure fixed routes in the network by configuring static routes. These routes are not adaptive; in case of a failure or change in the network, these routes must be reconfigured manually. A maximum of 200 static routes can be configured from BA-4000 UI.

Table 9 Routing/Load Balancer: Static Routing

Field	Description
Destination	Remote IP address or remote IP subnet.
Type	Mask Provided by the ISP. Values: Host / Net Host: Incase if type is selected as "Host" the subnet mask is automatically assigned as 255.255.255.255 Net: Incase if type is selected as "Net" the subnet mask parameter need to be entered.
Gateway	IP address of the gateway
Metric	Number of hop counts to reach the destination. Range: 0-127 Default: 0
Interface	Destination port to which the traffic must be routed. If the value "Auto Detect" is selected, then the system automatically selects the interface. Values: Auto Detect, WAN1, WAN2, WAN3, WAN-3G, LAN, VPN1, VPN2, Custom Default: Auto Detect
Gateway	IP address of the gateway.
Float	This field is visible when the interface type is chosen as WAN1, WAN2 or WAN3. Enabling this checkbox deletes the static route and stores the route information when the link goes down. The route is restored once the link is up. This is Mainly used to check the status of the remote network. Selecting the option "Auto Detect" for the Interface field disables the "Float" option.
Ex 1: Adding a host route : D- 192.168.100.5 SM: 255.255.255.255, GW: 192.168.5.1	
Ex 2: Adding a subnet route: D- 192.168.100.5 SM: 255.255.255.0, GW: 192.168.10.1	

Static Routing

You may add or remove Internet routing rules here.

Add a static route

Destination	<input type="text"/>
Type	Host ▾
Gateway	<input type="text"/>
Metric	0 <input type="text"/>
Interface	Auto Detect ▾
Comment	<input type="text"/>

Current Static Routes

No.	Destination	Netmask	Gateway	Metric	Interface	Float	Comment
1 <input type="checkbox"/>	192.168.100.5	255.255.255.255	192.168.5.1	0	detect	no	webserver
2 <input type="checkbox"/>	192.168.100.5	255.255.255.0	192.168.10.1	0	WAN-1	yes	webserver

Configured Static Routes will be displayed in the table below the settings tab. If any rule to be deleted, select the rule by clicking the check box in the “No.” row and press “Delete Selected”.

Policy Routing

Policy-based routing feature enables the network administrator to exercise policy-based routing principles to implement packet forwarding and routing. These custom-defined policies supersede the traditional routing protocol constraints. This finds effect where administrative issues dictate the need to route traffic through specific paths. The routing policies can be defined if Load Balance and Policy Routing of WAN load balancing is configured.

Table 10 Routing/Load Balancer: Policy Routing

Field	Description
Source Interface	Interface at which the packet is being received. Values: Loopback / LAN
Source IP	IP address of the source of the packet. Format: Single IP address or Single Subnet. Example: 192.168.5.1 or 192.168.5.0/24
Destination IP	IP address where the packet needs to be routed to. Format: Single IP address or Single Subnet. Example: 192.168.5.1 or 192.168.5.0/24
Priority	Values: High / Medium/Default Default: High
Provider	Interface through which the packets are to be routed. Values: WAN1, WAN2, WAN3 and WAN-3G Default: WAN1
Comment	Text box provided to name the rule
Insert Location	Indicates the Priority of the routing decision

Values: After Last Rule / Before First Rule

Default: After Last Rule

Policy Routing

You may add or remove policy routing rules here.

Add a policy route

Source Interface	Any
Source	
Destination	
Priority	High
Provider	WAN-1
Comment	
Insert Location	After Last Rule

Current Policy Routing Rules

No.	Source Iface	Source	Destination	Priority	Provider	Comment
1 <input type="checkbox"/>	LAN-1	192.168.5.1	122.166.116.12	high	WAN-1	nani

Configured Policy Routes will be displayed in the table below the settings tab. If any rule to be deleted, select the rule by clicking the check box in the “No.” row and press “Delete Selected”.

IP Pass-through

IP Pass-through feature is used to pass-through the available IP address of the selected pool to the devices behind the LAN port of the BA-4000. For example if Wi-Fi Controller NC-3650 need to be configured with a Public IP for remote access and subscriber VPN, and the controller is behind the BA-4000 LAN, then those IPs will be configured in IP Pass-through tab.

Table 11 Routing/Load Balancer: IP Pass-through

Field	Description
Outside Interface	<p>The interface from which the IP need to be passed through.</p> <p>Values: WAN-1/WAN-2/WAN-3</p> <p>Default: WAN-1</p>
Outside IP Address/Range	<p>The range of IP address needs to be pass-through BA-4000.</p> <p>For example: 70.33.21.40 - 50</p>
Inside Interface	<p>The interface to which the pass-through is required. In BA-4000 there is only one LAN interface, hence the Inside Interface is always LAN only.</p>
Bypass Firewall	<p>By clicking the check box, all the ports for the selected IPs are pass-through, no firewall applicable for the IPs. If this feature is not enabled and customer want to pass-through only specific ports for the IPs then the required rule to be added in "Firewall Settings"</p>

Comment

Text box provided to name the rule

IP Passthrogh

You may add or remove IP Passthrough rules here.

Add IP Passthrough Rule

Outside Interface	WAN-1 ▼
Outside IP Address/Range	70.133.189.67 - 77
Inside Interface	LAN ▼
Bypass Firewall	<input checked="" type="checkbox"/>
Comment	Controller IPs

Current IP Passthrough Rules

No.	Outside Iface	Outside IP	Inside Iface	Bypass FW	Comment
1 <input type="checkbox"/>	WAN-1	70.133.189.67 - 77	LAN-1	yes	Controller IPs

Configured IP Pass-through will be displayed in the table below the settings tab. If any rule to be deleted, select the rule by clicking the check box in the “No.” row and press “Delete Selected”.

Load Balancing

Load balancing is a technique of distributing the IP traffic across multiple clusters. This enhances scalability and availability of services such as web, terminal services and virtual private networking. It ensures high availability by detecting link failures and automatically redistributing traffic to the surviving links. Load balancing can be used to provide resilience or redundant backup in case of failure of one part of WAN access. For example, a company with an ADSL line might have a secondary ADSL line, or any other kind of internet feed. Internet traffic may be evenly distributed across both connections, giving more total net bandwidth, or traffic policies may determine the routing of certain traffic through specific connections. This is known as link load balancing. Where one connection fails, all traffic can automatically be routed via the other connection. This is known as failover.

BA-4000 supports the following WAN load balancing techniques:

Failover Only

This is the default configuration. If there are multiple WAN interfaces configured, the WAN interface with higher link weight takes higher priority and functions as the primary interface. For details regarding link weight configuration, refer to, “To configure WAN link properties”. In case of primary interface failure, the secondary interface takes over. In this mode port forwarding to internal servers will not be automatically switched to the working interface.

Load balance and Failover

In this configuration, if there are multiple ISPs configured, the ISP configured with higher priority takes a proportional amount for traffic. Additional traffic is apportioned to the other links per connection. In order to maintain integrity of secure connections, each unique source IP to destination IP connection will be assigned to a single WAN port. This configuration can be enabled if the web server is configured in the LAN and multiple ISPs are configured in the network. In this configuration, routing policies can be still defined to route specific connection requests through the other configured links.

Table 12 Routing/Load Balancer: Load Balance

Field	Description
Method for public network	Load balancing configuration Values: Failover only / Load Balance & Failover Default: Failover only
Check Interval (seconds)	Frequency at which the status of the interface is monitored. Default: 15 Secs

Load Balance

You may setup the load balancing and link detection properties here.

Load Balance Properties	
Method for Public Network	Failover Only ▼
Link State Check Interval (seconds)	15
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Quality of Service (QoS)

Quality of Service (QoS) refers to resource reservation control mechanisms. It is the ability to provide appropriate priority to different applications/users/data flows relatively to guarantee acceptable performance levels. This plays a very important role in upholding performance levels of essential applications in times of network resource congestion. With the QoS support achieved performance levels (data rate and delay, and dynamically controlled scheduling priorities) are monitored and the reserved capacity is released when necessary.

BA-4000 supports the configuration of QoS on the WAN1, WAN2, WAN3, WAN-3G and LAN interfaces. . To use QoS, first enable QoS on the respective interfaces globally and select Save. Once enabled, the link bandwidth configuration and QoS class definitions can be defined. QoS on the WAN interfaces control outgoing traffic flow from your network to the internet (ISP). QoS on the LAN interface controls incoming traffic flow from the internet (ISP) to your network.

Setting File Sharing rules

Instead of configuring detailed QoS rules, you can enable some default file sharing control rules, you must enable Quality of Service on each WAN interface and the LAN port.

For each active port: WAN (1-3) and LAN

1. Click on QoS, select enable and save
2. Click on Qos, select Set File Sharing Rules. This will reset the port.
3. Click on Qos, select enable and set the correct bandwidth (port upload speed for WAN and aggregate download speed for LAN) and save
4. Click on Qos, select Apply QoS Config

When enabled, this feature will greatly slow file sharing traffic and preserve that bandwidth for legitimate applications. This can be combined with bandwidth and session limits on the ValuePoint Gateway Controller 3560. Enabling the file sharing rules will clear out any existing QoS entries for that port.

QoS Settings WAN/LAN

Table 13 QoS: QoS Setup of WAN/LAN Interfaces

Field	Description
Enable	Checkbox used to enable or disable QoS configuration.
Upload Bandwidth (kbps)	Enter the maximum bandwidth resource in kbps allocated for upload on the configured link. Values: 64K - 80M and User defined in Bits/sec. Default: User defined
Reserved Bandwidth (kbps)	The minimum bandwidth that is reserved for the link even when the traffic load increases.
Based on the available resources in the network and how much need to be provided to QoS, define the service either through the default choices or select "user defined". Once QoS is configured press "SAVE" to get the CLASS / SERVICE based QoS configurations tabs	

Quality of Service Settings - WAN-1

You may setup rules to provide Quality of Service guarantees for specific applications.

QoS Setup	
Quality of Service	Enable <input type="checkbox"/>
Upload Bandwidth:	User defined <input type="text" value="1024k"/> Bits/sec

Group	Attribute
Class1	Disabled <input type="button" value="Modify"/>
Class2	Disabled <input type="button" value="Modify"/>
Class3	Disabled <input type="button" value="modify"/>
Class4	Disabled <input type="button" value="modify"/>
Class5	Disabled <input type="button" value="Modify"/>
Default	Rate:5%, Ceil:100%, Prio: 1 <input type="button" value="Modify"/>

No	Name	Group	Info.
<input type="button" value="Add"/>	<input type="button" value="Delete"/>		
<input type="button" value="Apply QoS Config"/> <input type="button" value="Reset All"/>			

QoS Classes

Table 14 QoS: QoS Classes

Field	Description
BA-4000 supports up to 5 classes and a Default class with 5% as reserved bandwidth and 95% as idle bandwidth. Default the Class is disabled. To configure the Class based QoS, click on "Modify" button. It will pop up a window for the Class configurations.	
Group Name	Identifier for the QoS class being created.
Enable	Checkbox to enable/configure the QoS class.
Rate	The minimum bandwidth that is reserved for the QoS class even when the traffic load increases.
ceil	The maximum bandwidth that is reserved for the QoS class even when it is idle.
Priority	The priority of the QoS class; lower the number, higher the priority.

Once all the configurations are done, please press "Modify" the save the settings.

Class1	
Group Name	<input type="text" value="Class1"/>
Enable	<input checked="" type="checkbox"/>
Rate:	<input type="text" value="10"/> % of upload bandwidth
Ceil:	<input type="text" value="100"/> % of upload bandwidth
Priority	<input type="text" value="1"/>

QoS Classifier Settings

Table 15 QoS: QoS Rules for WAN and LAN interface

Field	Description
-------	-------------

To add the QoS Rules click on the "Add" button after the class settings, it will pop up a window for QoS Classifier settings.

Name	A unique user-defined name given to the QoS Rule name
Group	Please select the QoS class group you need to assign (Values: Class 1 - Class 5)
MAC Address	Physical address of the source. Ex: 00:1b:91:ff:9f:9e
Destination IP	IP Address of the destination. Any of the following formats are supported: 192.168.100.0/24 (subnet) or 192.168.100.2
Source IP	IP Address of the source. Any of the following formats are supported: 192.168.100.0/24 (subnet) or 192.168.100.2
Packet Length	Packet length in bytes. Rule will be applied to packets with a minimum length specified in this field and up to a maximum length specified in the Maximum Packet Length field.
Protocol	Select the protocol to be used. Values: TCP, UDP, ICMP
Destination Port	Specify the destination port for TCP or UDP. This value can be specified as a range, a fixed number or ranges. To include all ports in the supported range, enter ALL. Range: 0-65535
Source Port	Optional field used to identify the source port if the protocol chosen is TCP or UDP. This value can be specified as a range or a fixed number port number. Range: 0-65535
TOS Filter	The type of Service specification to ensure the quality of service on the traffic generated under this class. Values: Minimize-Delay, Maximize-Throughput, Maximize-Reliability, Minimize-cost, Normal-Service and Disable. Default: Disable

Once all the configurations are done in QoS classes and QoS Rules, press "Apply QoS Config" to enable the QoS.

Classifier Settings	
Name	Valuepoint
Group	Class1 ▼
Mac address	54:42:49:57:34:59
Dest IP Address	122.166.116.12
Source IP Address	192.168.100.100
Packet Length	128 - 1024 (ex: 0-128 for small packets)
Protocol	TCP ▼
Dest. Port Range	1000 - 1500
Src Port Range	1200 - 2400
TOS Filter:	Minimize-Delay ▼
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	

Open VPN Client

BA-4000 supports 2 OpenVPN clients. These are used to create site-site VPN tunnels and are compatible with OpenVPN Server. The clients are designed in such way that BA-4000 can be connected to two different VPN Servers through 2 clients using different ports. For example it can be managed over VPN by connecting it to a NOC server and second client is used to connect to the Head Office / Data Center to interwork with Applications Servers. The clients are designed to auto failover to the working WAN link on the VPN Gateway.

Table 16 Open VPN: Secure VPN Client

Field	Description
Service	Check-box used to enable or disable secure VPN client configuration.
Client Description	Description for each client. Can be left blank. Used for ease of administration.
Client Name	Mandatory field to enter the name of the client. This field can take alphanumeric characters. Special characters such as – and _ are supported. However, the server name must start with an alphabet in the lower case only and can end with an alphabet or a number. This field must have a minimum of four characters.
Password	Enter the password obtained from the downloaded certificate for the client while configuring the Secure VPN server and associated clients
Verify Password	Re-enter the password for confirmation
Server Name / IP (1)	IP address or name of the broadband connection of the server where the secure VPN is configured.
Server Port (1)	Secure VPN server port number. Default : UDP/1194
Server Name / IP (2)	IP address or name of the broadband connection to the server where the secure VPN is configured. This service takes over in case of a failure of IP1.
Server Port (2)	Secure VPN server port number. Default : UDP/1195
MTU	The maximum packet size (not including the IP header) of tunnel data in UDP tunnel transport mode. Default: 1500
Protocol	Select the protocol to be used to connect to the Secure VPN server. Default: UDP Values: TCP, UDP
Authentication Algorithm	Select the algorithm to authenticate the packets. The default being SHA1 which uses a data string, a secure hash algorithm, and a key, to produce a digital signature. Default: SHA1 Values: SHA1, none
Cipher Type	Select the algorithm to be used to encrypt the packets. The

	<p>blowfish algorithm is recommended in cases where the keys do not change frequently.</p> <p>Default: Blowfish-128-CBC</p> <p>Values: Blowfish-128-CBC, AES-128-CBC, AES-256-CBC, 3DES-192-CBC, and none.</p>
Enable LZO compression	<p>Enables packet level data compression. Reduces packet sizes by 5-15%, at the cost of latency.</p> <p>Default: none</p>
Default Firewall Policy	<p>Used to enable or disable the firewall for the selected interface</p> <p>Values: Drop incoming connections / Accept incoming connections / Accept only Management Port</p> <p>Default: Drop incoming connections</p>
NAT	<p>NAT maps all of the private IP addresses on a LAN network to the single IP address supplied by the ISP.</p> <p>Values: Enable / Disable</p> <p>Default: Enable</p>
Upload VPN Keys	<p>This is to be enabled to load the Secure VPN certificates to be loaded to interwork with the VPN Server. The client key will have two certificates and two keys which need to be uploaded to the client box.</p> <ol style="list-style-type: none"> 1. Certificate Authority: This certificate is to indicate the VPN Server settings and its configurations. 2. Certificate: This certificate related to client box 3. PKey: Private key related to client box 4. TLSKey: Is the key related to the VPN Server. <p>As per the present configurations the certificates and Keys need to be copied to the BA-4000 appliance.</p>

For example:

Assume the customer obtained a Secure VPN client from their Head Office and the Key name is "valuepoint_br1.zip" and the VPN Server name is "valuepoint-hq". The password for the client is "Qr24sTv" By unzipping the client key will get the following files.

1. valuepoint-hq_ca.crt
2. valuepoint-br1.crt
3. valuepoint-br1.pkey
4. ta.key
5. info.cfg

Open VPN Client-1	
Service	Enable ▾
Client Description	Valuepoint Branch1
Client Name	valuepoint-br1
Password	••••••
Verify Password	••••••
Server Name / IP (1)	122.166.116.12
Server Port (1)	1194
Server Name / IP (2)	
Server Port (2)	
MTU	1500
Protocol	UDP ▾
Authentication Algorithm	SHA1 ▾
Cipher Type	BLOWFISH-128-CBC ▾
Enable LZO Compression	ENABLE ▾
Default Firewall Policy	Accept Incoming Connections ▾
NAT	DISABLE ▾
Upload VPN Keys	<input checked="" type="checkbox"/>

Upload VPN Keys will open with four fields to upload the certificates and keys

Certificate Authority	Open the "valuepoint-hq_ca.crt" file, copy the certificate "Begin Certificate" to "End Certificate" and paste it in the box.
Certificate	Open the "valuepoint-br1.crt" file, copy the certificate "Begin Certificate" to "End Certificate" and paste it in the box.
Key	Open the "valuepoint-br1.pkey" file, copy the certificate "Begin Certificate" to "End Certificate" and paste it in the box.
TLS Key	Open the "ta.key" file, copy the certificate "Begin Certificate" to "End Certificate" and paste it in the box.

After apply the settings, the BA-4000 automatically opens up the VPN Status to show the status

Firewall

The Firewall is a system that is used to define rules that govern the routing of connection requests to and from the customer/your network. By using a firewall system between your intranet and the internet you can allow a defined set of services to pass through the different network zones while keeping other services out. Such rules can be defined and enforced by the BA-4000.

MAC/IP/Port filter settings

MAC/IP/Port Filter settings used to accept/drop the connection requests. The connection requests that match the defined criteria and the parameter selected is "accept", then the packet will be routed accordingly or if the selected parameter is "drop" will be discarded.

Table 17 Firewall: MAC/IP/Port filter settings: Basic Settings

- Basic Settings is used to enable the MAC/IP/Port filter setting rules and set the default policy for the packets which do not match with any rules.

Field	Description
MAC/IP/Port filter settings	Values: Enable / Disable Default: Enable
Default Policy -- Packets that don't match any rules would be	Values: Accepted / Dropped Default: Accepted

Table 18 Firewall: MAC/IP/Port filter settings

Field	Description
Source IP Address	This field is used to specify the source IP addresses with the source of the connection request. You can specify any number of Source IP addresses. The values can include specific IP addresses and/or a subnet. Example specifying IP Addresses: 192.168.10.1, 192.168.10.0/24
Source MAC Address	This field is used to specify the source MAC addresses of the connection request. You can specify one source MAC addresses per rule. . Example specifying MAC Addresses: aa:bb:cc:dd:ee:ff
Destination IP Address	Used to specify the IP address of the destination for the connection request termination if this rule is applied. The values can include specific IP addresses and/or a subnet. In

	case if 3 IPs need to be forwarded then there will be 3 rules need to be created with one IP each. Example specifying IP Addresses: 192.168.100.1 or 192.168.100.0/24
Protocol	Select the Protocol to be used. Values: TCP, UDP, ICMP, TCP&UDP
Source Ports / Range	This field is used to identify the source port, if the protocol chosen is TCP or UDP. This can take any integral value from 0 to 65535. You can specify any number of ports. The values must be comma separated. The values can include specific port numbers and/or a range of port numbers.
Destination Ports / Range	This field is mandatory if you choose TCP or UDP protocols and is used to specify the original destination port number associated with the connection request. This field is not applicable to the ICMP and IGMP. This can take any value from 0 to 65535. You can specify any number of ports. The values must be comma separated. The values can include specific port numbers and/or a range of port numbers.
Action	Values: Drop/Accept Default: Drop

MAC/IP/Port Filter Settings	
Comment	Valuepoint
Source IP Address	192.168.100.100
Source MAC address	54:42:49:57:34:59
Dest IP Address	122.166.116.12
Protocol	TCP
Src Port(s) / Range	110 , 25 , ,
Dest Port(s) / Range	4343 , , ,
Action	Accept
Insert Location	After Last Rule

(The maximum rule count is 100.)

Apply Reset

MAC/IP/Port Filter configured settings will be displayed in the below table. If any rule to be deleted, select the rule in the provided check box in the “No” row and press “Delete Selected”.

Current MAC/IP/Port filtering rules in system:								
No.	Source MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port	Source Port	Action	Comment
1 <input type="checkbox"/>	54:42:49:57:34:59	122.166.116.12	192.168.100.100	TCP	4343	110 25	Accept	Valuepoint
Others would be accepted								-

Delete Selected Reset

Port Forwarding

A network port on one node is forwarded to another. This allows remote clients (clients on the internet) to connect to a specific client within a private LAN. For example, if you are managing an Access Point on Gateway Controller 3560 port 60001, create a port forwarding rule for port 60001 to the LAN IP of the Controller 3560.

Table 19 Firewall: Port Forwarding

Field			Description
Port Forwarding			Values: Enable, Disable Default: Disable
IP Address			Used to specify the IP address of the destination for the connection. The values can include specific IP addresses and/or a subnet. Incase if 3 IPs need to be forwarded then there will be 3 rules need to be created with one IP each. Example specifying IP Addresses: 192.168.100.1 or 192.168.100.0/24
Port Range			This field is used to identify the forwarded port. This can take any integral value from 0 to 65535. You can specify any number of ports. The value is entered as a range of port numbers. If you only want a single port like 443 to be open for access the Port Range is specified as 443-443
Protocol			Select the Protocol to be used. Values: TCP, UDP, TCP&UDP
Original address	Destination	IP	This field is optional to specify the destination IP address of the connection request.
Original Source IP address			This field is optional and is used to specify the source IP addresses with the source of the connection request. You can specify any number of IP addresses. The values can include specific IP addresses and/or a subnet. Example specifying IP Addresses: 192.168.10.1, 192.168.10.0/24

Port Forwarding	
Port Forwarding	Enable ▾
IP Address	122.166.116.12
Port Range	1194 - 1194
Protocol	UDP ▾
Original Dest IP Address	192.168.100.5 (optional)
Original Source IP Address	(optional)
Comment	VPN Server

(The maximum rule count is 64.)

Port Forwarding rules configured will be displayed in the below table. If any rule to be deleted, select the rule in the provided check box in the “No” row and press “Delete Selected”.

Current Port Forwards						
No.	IP Address	Port Range	Protocol	Original Dest IP Address	Original Source IP Address	Comment
1 <input checked="" type="checkbox"/>	122.166.116.12	1194 - 1194	UDP	192.168.100.5	-	VPN Server
<input type="button" value="Delete Selected"/> <input type="button" value="Reset"/>						

Virtual Servers

Used for forwarding the packets coming in public port to the private port of the web server / Application Servers in the LAN segment. This features allow a different external (WAN) and internal (LAN) port to be used.

Table 20 Firewall: Port Forwarding: Virtual Servers

Field	Description
Virtual Server	Values: Enable, Disable Default: Disable
IP Address	Used to specify the IP address of the destination for the connection request termination if this rule is applied. The values can include specific IP addresses and/or a subnet. Incase if 3 IPs need to be forwarded then there will be 3 rules need to be created with one IP each. Example specifying IP Addresses: 192.168.100.1 or 192.168.100.0/24
Public Port	The WAN IP port number on which the corresponding packets are received. For example, Port 60001
Private Port	The LAN IP port number for which the local server is configured to accept the packets. For a web server this would be port 80.
Protocol	Select the Protocol to be used. Values: TCP, UDP, TCP&UDP
Original Destination IP address	This field is optional to specify the destination IP address of the connection request.
Original Source IP address	This field is optional and is used to specify the source IP addresses with the source of the connection request. You can specify any number of source IP addresses. The values can include specific IP addresses and/or a subnet. Example specifying IP Addresses: 192.168.10.1, 192.168.10.0/24

Virtual Server	
Virtual Server	Enable ▾
IP Address	122.166.116.12
Public Port	80
Private Port	1222
Protocol	TCP ▾
Original Dest IP Address	192.168.100.5 (optional)
Original Source IP Address	(optional)
Comment	ERP Server

(The maximum rule count is 64.)

Apply Reset

Virtual Server rules configured will be displayed in the below table. If any rule to be deleted, select the rule in the provided check box in the “No” row and press “Delete Selected”.

Current Virtual Servers							
No.	IP Address	Public Port	Private Port	Protocol	Original Dest IP Address	Original Source IP Address	Comment
1	122.166.116.12	80	1222	TCP	192.168.100.5	-	ERP Server
<input checked="" type="checkbox"/>							

Delete Selected Reset

Source Network Address Translation (SNAT)

The Network Address Translation (NAT) technology converts private IP addresses (such as in the 192.168.0.0 range) of the machine on the internal private network to one or more public IP addresses for the Internet. It changes the packet headers to the new address and keeps track of them via internal tables that it builds. When packets come back from the Internet, NAT uses the tables to perform the reverse conversion to the IP address of the client machine. NAT not only conserves public IP addresses, but it also enhances security by keeping internal addresses hidden from the outside world.

Network administrators create a NAT table that does the global-to-local and local-to-global IP address mapping. Dynamic NAT (DNAT) can map all of the private IP addresses on the LAN network to the single IP address supplied by the ISP. Static NAT (SNAT) can map a single private IP address to a single public address.

Table 21 Firewall: SNAT

Field	Description
Source IP / Subnet	<p>This field is used to specify rules related to source IP/subnet to be NAT-ed.</p> <p>Options include:</p> <p>To NAT all source IP addresses, leave this field blank.</p> <p>To specify select IP address or subnets, enter IP addresses or subnets</p> <p>Entering specific IP addresses/subnets in this enables the option to specify list of IP addresses to be excluded from NAT.</p>
Egress Interface	Mandatory field identifying the interface used to route the connection request (from the private network) to the outside network.

	Values: WAN-1, WAN-2, WAN-3, WAN-3G LAN, VPN-1 & VPN-2
Destination IP / Subnet	Enter IP addresses to be NAT-ed. If this field is left blank, all packets going through the outgoing interface, irrespective of the destination IP address is NAT-ed. If this field is not empty, the NAT rule is applied to all connection requests destined to the specified IP addresses.
SNAT IP Address	This field is used to specify the public IP address that needs to be assigned to the interface. If this field is blank, the router assigns the first available public IP address from the outgoing interface. This field is disabled if IP Source field is left blank indicating that all IP sources will be NAT-ed.
Comment	Text box provided to name the rule
Insert Location	Indicates the Priority of the routing decision Values: After Last Rule / Before First Rule Default: After Last Rule

SNAT Rules

You may add or delete SNAT rules here.

Add a SNAT rule	
Source IP/Subnet	192.168.100.0/24
Egress Interface	WAN-1 ▼
Destination IP/Subnet	
SNAT IP	122.166.116.12
Comment	Subnet NAT-ed
Insert Location	After Last Rule ▼

SNAT configured settings will be displayed in the below table. If any rule to be deleted, select the rule in the provided check box in the “No” row and press “Delete Selected”.

Current SNAT Rules					
No.	Source	Egress Interface	Destination	SNAT IP	Comment
1 <input checked="" type="checkbox"/>	192.168.100.0/24	WAN-1	-	122.166.116.12	Subnet NAT-ed

Network Mapping

Network Mapping is most often used to resolve IP address conflicts. If two organizations, A and B, need to be linked and that both organizations have allocated the 192.168.1.0/24 sub network, then there is a need to connect the two networks so that all systems in network A can access the 192.168.1.0/24 network in B and vice versa without any re-addressing.

Table 22 Firewall: Network Mapping

Field	Description
Type	Mandatory field to specify source or destination IP address to be mapped. Select DNAT or SNAT to re-write (NAT) the destination IP address or source IP address respectively. Values: DNAT, SNAT Default: DNAT
Interface	Mandatory field to specify the interface. Values: WAN-1, WAN-2, WAN-3, WAN-3G LAN, VPN-1 & VPN-2
Original Network	Specify the Network address in the CIDR format; If the Type chosen is DNAT and traffic entering interface is addressed to this network (Original Network), then the destination address is re-written to the corresponding address in the New Network to field. If the Type chosen is SNAT, for traffic leaving the interface, the source address matching the Original Network, then the source address will be re-written to the corresponding address in the New Network to field.
New Network	Specify the Network address in the CIDR format; If the Type chosen is DNAT and traffic entering interface is addressed to this network (Original Network), then the destination address is re-written to the corresponding address in the New Network to field. If the Type chosen is SNAT, for traffic leaving the interface, the source address matching the Original Network, then the source address will be re-written to the corresponding address in the New Network to field.

Net Map Rules

You may add or delete Net Map rules here.

Add a Net Map rule

Type	DNAT ▼
Interface	WAN-1 ▼
Original Network	192.168.100.0/24
New Network	10.10.12.0/24
Comment	server segment
Insert Location	After Last Rule ▼

Add

Reset

Net Map Rules configured settings will be displayed in the below table. If any rule to be deleted, select the rule in the provided check box in the “No” row and press “Delete Selected”.

Current Net Map Rules					
No.	Type	Interface	Orig Network	New Network	Comment
1 <input checked="" type="checkbox"/>	dnat	WAN-1	192.168.100.0/24	10.10.12.0/24	server segment

System Security

BA-4000 supports the following predefined rules that can be enabled / disabled by the user

- Remote Management
- Block Ping from WAN
- Block Port Scan
- Block SYN Flood
- Stateful Packet Inspection (SPI)

Note: These rules are predefined and they can be activated using the “Enable/Disable” button associated with the respective rules.

Table 23 Firewall: System Security Settings

Field	Description
Remote Management (WAN)	Values: Deny/Allow. By enabling this rule to “Allow” the box can be remotely managed via the WAN interface IP. Default: Deny
Block ping from WAN	This is to block any ping request through the WAN IP. This is block by default. Default: Disable
Block Port Scan	This is to block port scan request through the WAN Interface. This is block by default. Default: Disable
Block SYN Flood	This is to block SYN Flood request through the WAN Interface. This is block by default. Default: Disable
Stateful Packet Inspection	This is enabled by default to inspect the packet which is coming into the network through WAN side based on the rules set.

System Security Settings

You may configure the system firewall to protect your network.

Remote management	
Remote management (via WAN)	Allow ▾

Block ping from WAN	
Block ping from WAN	Disable ▾

Block Port Scan	
Block port scan	Disable ▾

Block SYN Flood	
Block SYN Flood	Disable ▾

Stateful Packet Inspection (SPI)	
SPI Firewall	Enable ▾

Apply

Reset

5

Management

This section allows configuration of SNMP and SysLog monitoring of the BA-4000 system.

SNMP

You can enable SNMP monitoring for the BA-4000 in this section. The BA-4000 supports the RFC 1213 MIB2 objects. Please be sure the Read Only community strings matches your SNMP manager software, and enter the IP address of any remote management systems that are going to connect to the SNMP server on WAN ports.

Remote SysLog

The System Log records internal events, like port status, on the BA-4000. If you wish to transmit this log to a Syslog Server, enter the IP and Port here. You can view this log internally under the status menu.

Status

This section provides information about the BA-4000 system and helps provide logs and system commands to resolve any problem.

Status includes the following tasks:

- System Info
- Network Status
- Statistics
- Bandwidth Graph
- DHCP Clients
- System Command
- System Log
- Support

System Info

This section provides all relevant information of BA-4000. It's Software Version, System uptime, Operation Mode, System ID and license information.





BA-4000 System Information

System Info	
Software Version	BA4000_1.0.0rc1
Software Build Date	Mon Jun 27 13:10:36 UTC 2011
System Up Time	2:46
System Platform	MIPS
Operation Mode	Gateway Mode
System ID	A422-53FD-682B-6A95
License Status	OK

Network Status

This section provides status of the configured WAN and LAN interfaces for its mode of operation, IP address, Subnet mask, Gateway and status.

BA-4000 Network Status

Network Status							
Name	Mode	Type	IP Address	Subnet Mask	Gateway	Prio	State
WAN-1	STATIC	PUBLIC	192.168.5.200	255.255.255.0	192.168.5.1	1	DOWN
WAN-2	STATIC	CAPTIVE	192.168.66.1	255.255.255.0	192.168.66.10		DOWN
WAN-3	STATIC	PUBLIC	192.168.5.201	255.255.255.0	192.168.5.1	1	UP
WAN-3G	DISABLE	PUBLIC					DOWN
LAN	STATIC	LOCAL	192.168.100.1	255.255.255.0			UP
Default Gateway							
Default Gateway				192.168.5.1 dev eth2.2			
Ethernet Port Status							
Name	MAC Address			Cable State			
WAN-1	00:00:00:44:44:45						
WAN-2	00:00:02:02:02:22						
WAN-3	00:00:00:44:44:47						
LAN	00:00:00:44:44:44						

Statistics

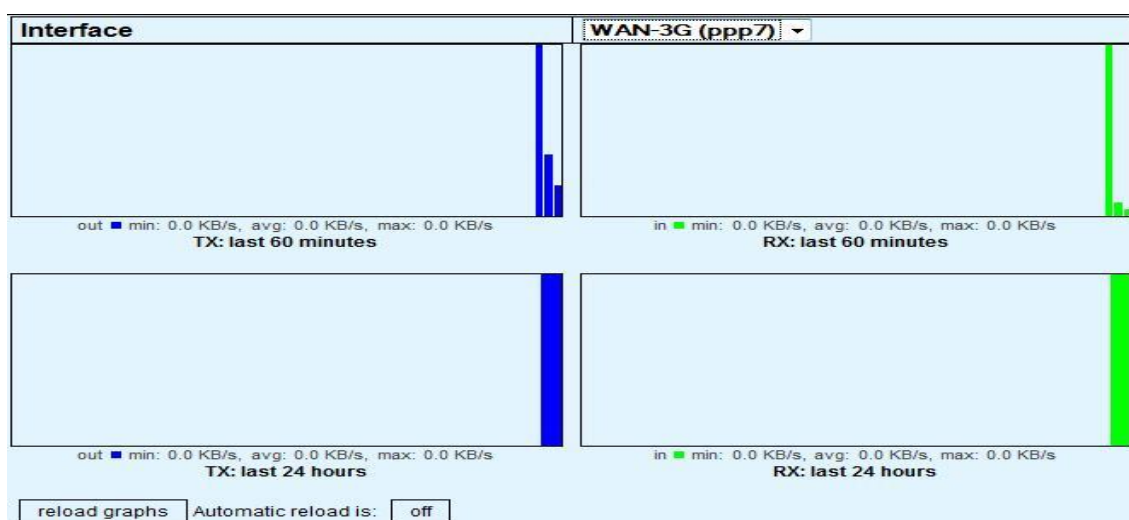
This section provides stats on Memory usage in BA-4000, consolidated usage of WAN/LAN interface (WAN Tx/Rx and LAN Tx/Rx bytes and packets) and stats of all the configured interfaces (both WAN & LAN)

Statistics	
Memory	
Memory total:	127032 kB
Memory left:	103636 kB
All interfaces	
Name	eth2.2 (WAN-1)
Rx Packet	0
Rx Byte	0
Tx Packet	4662
Tx Byte	214452
Name	wan2 (WAN-2)
Rx Packet	0
Rx Byte	0
Tx Packet	0
Tx Byte	0
Name	wan3 (WAN-3)
Rx Packet	276
Rx Byte	17928
Tx Packet	165
Tx Byte	8270

Bandwidth Graph

BA-4000 provides two types of Bandwidth Graphs for both Tx and Rx. Two graphs are displayed - one is for "last 60 mins" and the other is for "last 24 hours". The user can configure an auto reload of the graph or it can be done manually.

Note: The graphs are available only for the configured interface. For example if only WAN1 and LAN are configured, the bandwidth graphs are available only for WAN1 and LAN.



DHCP Clients

If the DHCP server is enabled on the BA-4000, this section shows all the clients connected to the LAN interface of BA-4000.

DHCP Client List			
Monitor DHCP clients here.			
DHCP Clients			
Hostname	MAC Address	IP Address	Expires in
Nani-VAI	54:42:49:57:34:59	192.168.100.100	23:59:39

System Command

BA-4000 supports sets of commands which can be used for debug. Just type any word on the field provided and press "enter", a window opens up and shows all the supported system command in BA-4000. The supported commands are ifconfig, uptime, arp, logread, date, free, rebootnow, ping, netstat, route, iprule, lsusb, lsmodem, ipsec, qos.

System command

Command:

```

PING 122.166.116.12 (122.166.116.12): 56 data bytes
64 bytes from 122.166.116.12: seq=0 ttl=50 time=458.033 ms
64 bytes from 122.166.116.12: seq=1 ttl=50 time=187.782 ms
64 bytes from 122.166.116.12: seq=2 ttl=50 time=207.592 ms
64 bytes from 122.166.116.12: seq=3 ttl=50 time=207.428 ms
64 bytes from 122.166.116.12: seq=4 ttl=50 time=207.291 ms

--- 122.166.116.12 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 187.782/253.625/458.033 ms

```

System Log

Provides the logs of the services configured in the device and its status.

System Log

Syslog:

System Log

```

Jun 28 14:17:28 ba4000 user.notice admin: monitor_nld: Starting NLD monitor. checki=45
Jun 28 14:17:28 ba4000 user.info syslog: nld: starting. mode=0 scan_interval=15
Jun 28 14:17:28 ba4000 user.info syslog: nld: processing rescan signal
Jun 28 14:17:35 ba4000 daemon.info pppd[1853]: Connect time 14.4 minutes.
Jun 28 14:17:35 ba4000 daemon.info pppd[1853]: Sent 42419 bytes, received 43866 bytes.
Jun 28 14:17:35 ba4000 daemon.info pppd[1853]: Terminating on signal 15
Jun 28 14:17:35 ba4000 daemon.info pppd[1853]: Hangup (SIGHUP)
Jun 28 14:17:35 ba4000 daemon.notice pppd[1853]: Modem hangup
Jun 28 14:17:35 ba4000 daemon.notice pppd[1853]: Connection terminated.
Jun 28 14:17:36 ba4000 daemon.notice pppd[4815]: pppd 2.4.4 started by admin, uid 0
Jun 28 14:17:37 ba4000 local2.info chat[4821]: timeout set to 10 seconds
Jun 28 14:17:37 ba4000 local2.info chat[4821]: abort on (BUSY)
Jun 28 14:17:37 ba4000 local2.info chat[4821]: abort on (NO CARRIER)
Jun 28 14:17:37 ba4000 local2.info chat[4821]: abort on (VOICE)
Jun 28 14:17:37 ba4000 local2.info chat[4821]: abort on (NO DIALTONE)
Jun 28 14:17:37 ba4000 local2.info chat[4821]: abort on (NO DIAL TONE)
Jun 28 14:17:37 ba4000 local2.info chat[4821]: abort on (NO ANSWER)
Jun 28 14:17:37 ba4000 local2.info chat[4821]: abort on (DELAYED)
Jun 28 14:17:37 ba4000 local2.info chat[4821]: send (ATZ^M)
Jun 28 14:17:37 ba4000 local2.info chat[4821]: expect (OK)
Jun 28 14:17:37 ba4000 local2.info chat[4821]: ATZ^M^M
Jun 28 14:17:37 ba4000 local2.info chat[4821]: OK

```

System Administration

This section provides all the admin related operation of BA-4000 such as upgrade firmware, backup and restore of configuration, user authentication for logging into BA-4000 and their credentials.

System Management

Administration Settings

The username and password for logging into the box need to be configured in this tab.

Default username : *root*

Default password: *root*

Administrator Settings	
Account	<input type="text" value="root"/>
Password	<input type="password" value="...."/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

The user can modify the username and password as per their choice using these settings.

DDNS Settings

This is used to reach the box using DNS name instead of IP. This is useful for remote manageability of the box if the connectivity is either PPPoE or DHCP. BA-4000 DDNS are compatible with DynDNS.org / freedns.afraid.org / www.zoneedit.com / www.no-ip.com / CustomDNS / CustomDNS (HTTP)

Table 24 Administrator: System Management: DDNS Settings

Field	Description
DNS Provider	<p>Select the protocol used to notify a domain name sever to change the active DNS configuration of its configured hostnames, addresses or other information stored in the DNS. Selecting DynDNS enables the standard DynDNS protocol; selecting CustomDNS enables Customer DNS protocol for updating the BA-4000 DNS records.</p> <p>Values: None / DynDNS.org / freedns.afraid.org / www.zoneedit.com / www.no-ip.com / CustomDNS / CustomDNS (HTTP)</p> <p>Default: None</p>
Method	Select the method used to choose the IP address. Choose interface IP to auto detect interface IP, Use Web to detect IP address from a HTTP query.
Account	Enter the login ID to access the server; this is provided by the DNS service provider.
Password	Enter the password to access the server; this is provided by the DNS service provider.

DDNS Name	Enter the fully qualified domain name provided by the DNS Service provider.
DDNS Server Name	Incase if the DNS provider is chosen as customer DNS, fully qualified customer DNS name of the

DDNS Settings	
Dynamic DNS Provider	CustomDNS
Method	Use WAN-3 IP
Account	valuepoint
Password	••••••••
DDNS Name	br1.valuepoint.com
DDNS Server Name	members.valuepoint.com
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

NTP Settings

This is used to synchronize the calendar time on the BA-4000 with the chosen NTP Server.

Table 25 Administrator: System Management: NTP Settings

Field	Description
Current Time	Displays the current Day, Time and Date of BA-4000 appliance. This can be synced with the connected host in the LAN segment or with the NTP Server setting.
Time Zone	Chose and set the respective "Time Zone" of the location where the BA-4000 box is installed.
NTP Server	Enter the NTP you need to use for the BA-4000 to sync its time, date and day settings. Default : pool.ntp.org
NTP Synchronization (Mins)	NTP Sync timings in mins can be set in this tab. Default: 10 mins (means every 10min once the box tries to sync itself with the NTP server for its current time settings).

NTP Settings	
Current Time	Thu Dec 3 20:35:09 IST 19€ <input type="button" value="Sync with host"/>
Time Zone:	(GMT+05:30) India
NTP Server	pool.ntp.org ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw
NTP synchronization (Mins)	10
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Configuration Management

This section provides the BA-4000 configuration management. It has the following options for the users about the configurations

1. Export Settings
2. Import Settings
3. Load Factory Defaults

Export Settings	This is use to "Export" the current configured settings of the BA-4000 to a host computer. The backup file name will be "backup.dat"
Import Settings	If already backed up configurations need to be loaded on BA-4000, it will be done using this settings.
Load Factory Defaults	Used to bring BA-4000 to factory configured Settings

The screenshot displays a web-based configuration management interface with three distinct sections, each with a blue header bar:

- Export Settings:** Contains a text field labeled "Export Settings" and an "Export" button.
- Import Settings:** Contains a text field labeled "Choose Settings File", a "Browse..." button, and "Import" and "Cancel" buttons.
- Load Factory Defaults:** Contains a text field labeled "Load Factory Defaults" and a "Load Default" button.

Upgrade Firmware

Upgrade the BA-4000 firmware to obtain new functionality. It takes about 1 minute to upgrade the system. **DO NOT POWER OFF THE SYSTEM.** Caution! A corrupted image will render the system useless. Browse the location of the image file and press "Apply" to upgrade the new firmware on BA-4000. Before doing firmware image upgrade

- Ensure the BA-4000 is connected to a stable power source, incase during the upgrade if power fails the flash will get corrupted and system will be useless and will have to be sent to VP Networks customer support for repair.
- The existing configurations will be intact during the new firmware upgrade. BA-4000 is designed is such way the new version upgrade will not delete or reset the existing configurations.

The screenshot shows the "Upgrade Firmware" section of the interface. It features a blue header bar with the title "Upgrade Firmware". Below the header, there is a warning message in red text: "Upgrade the BA-4000 firmware to obtain new functionality. It takes about 1 minute to upgrade the system. DO NOT POWER OFF THE SYSTEM. Caution! A corrupted image will render the system useless." Below the warning, there is a form with a "Location:" label, a text input field, and a "Browse..." button. At the bottom left of the form is an "Apply" button.

Warranty and License

This section display the Warranty VP Networks provides to its customers and also any relevant licenses.