5.6.3.2 User Accounts

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English WAN Setup NAT LAN Wireless Parental Control Home Networking			Sto Choose Ar	rage UserAccount Configu dd, or Remove to configure U Isername HomeDir Ren Add Remove	ration ser Accounts.		
Print Server DLNA Storage Service Storage Device Info User Accounts							

Click the **Add** button to display the following.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English 🔻	Storage UserAccount Co	nfiguration					
WAN Setup	Username:						
NAT	Password:						
LAN	Confirm Password:						
Wireless	volumeName:						
Parental Control							
Home Networking							
Print Server							
DLNA				Save/Apply			
Storage Service							
Storage Device Info							
User Accounts							

After filling in the respective fields, click the **Save/Apply** button.

To remove an account, tick the box and Click the **Remove** button.

5	Storage UserAccount Configuration					
Choose Add, or Remove to configure User Accounts.						
	Username	rname HomeDir Remove				
	Test	Office/Test				
	Add Remove					

Chapter 6 Advanced Setup

You can reach this page by clicking on the following icon located at the top of the screen.



6.1 Security

For detailed descriptions, with examples, please consult Appendix A - Firewall.

6.1.1 IP Filtering

This screen sets filter rules that limit IP traffic (Outgoing/Incoming). Multiple filter rules can be set and each applies at least one limiting condition. For individual IP packets to pass the filter all conditions must be fulfilled.

NOTE: This function is not available when in bridge mode. Instead, MAC Filtering performs a similar function.

OUTGOING IP FILTER

By default, all outgoing IP traffic is allowed, but IP traffic can be blocked with filters.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Voice	Diagnostics	Management	Logout
English	Outgoing IP Filtering When the firewall is en Choose Add or Remove	g Setup abled on a WAN or LAN ii e to configure outgoing IP	nterface, all outgoing IP filters.	traffic is allowed. However,	some IP traffic can be BL	OCKED by setting up filters.		
IP Filtering Outgoing Incoming MAC Filtering		Filter Name I	P Version Protocol	SrcIP/ PrefixLength Sa	cPort DstIP/ PrefixL	ength DstPort Remove]	

To add a filter (to block some outgoing IP traffic), click the **Add** button. On the following screen, enter your filter criteria and then click **Save/Apply**.



COMT		Info Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Security IP Filtering Outgoing Incoming MAC Filtering Quality of Service Routing DNS DSL	Add IP Filter Outgoing The screen allows you to create a filt in this filter rule must be satisfied for Filter Name: IP Version: Protocol: Source IP address[/prefix length]: Source Port (port or port:port): Destination IP address[/prefix length Destination Port (port or port:port):	er rule to identify IP traffic by sp the rule to take effect. Click 'Sa IPv4	ecifying a new filter name ar ve/Apply' to save and activat ▼ ▼	id at least one condition the filter.	on below. All of the specifi	ied conditions
DNS Proxy Interface Grouping			Save/Apply			

Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label.
IP Version	Select from the drop down menu.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

INCOMING IP FILTER

By default, all incoming IP traffic is blocked, but IP traffic can be allowed with filters.

COM	REND	M		Q5	Consultant of the second	Ś		~
		Device Info	Basic Setup	Advanced Setup	Voice	Diagnostics	Management	Logout
English	Incoming IP Filtering 5	ietup	rface all incoming IP trai	fic is BLOCKED. However, core	ia IR traffic can be ACC	CEPTED by catting up filters		
Security IP Filtering	Choose Add or Remove to	configure incoming IP fil	ters.	Inc is beoekeb. However, son	le ir daine can be Acc	center by second up meas		
Outgoing Incoming MAC Filtering	L	Filter Name Interfac	es IP Version Proto	Add Remove	SrcPort DstIP/ Pr	efixLength DstPort R	emove	

To add a filter (to allow incoming IP traffic), click the **Add** button.

On the following screen, enter your filter criteria and then click **Save/Apply**.



COMT		e Info Basic Setu	p Advanced Setup	Diagnostics	Management	Logout
English 🔻	Add IP Filter Outgoing					
Security IP Filtering Outgoing Incoming MAC Filtering Quality of Service Routing DNS	The screen allows you to create a filt in this filter rule must be satisfied for Filter Name: IP Version: Protocol: Source IP address[/prefix length]: Source Port (port or port:port): Destination IP address[/prefix length] Destination Port (port or port:port):	er rule to identify IP traffic by the rule to take effect. Click 'S IPv4	pecifying a new filter name and wve/Apply' to save and activate	l at least one condition the filter.	below. All of the specified	I conditions
DNS Proxy	WAN Interfaces (Configured in R	outing mode and with firev	all enabled) and LAN Inter	aces		
Interface Grouping		cs displayed below to apply th	sture.			
IP Tunnel	Select All 🖉 br0/br0					
IPSec Certificate			Save/Apply			

Consult the table below for field descriptions.

Field	Description
Filter Name	The filter rule label.
IP Version	Select from the drop down menu.
Protocol	TCP, TCP/UDP, UDP, or ICMP.
Source IP address	Enter source IP address.
Source Port (port or port:port)	Enter source port number or range.
Destination IP address	Enter destination IP address.
Destination Port (port or port:port)	Enter destination port number or range.

At the bottom of this screen, select the WAN and LAN Interfaces to which the filter rule will apply. You may select all or just a subset. WAN interfaces in bridge mode or without firewall enabled are not available.



6.1.2 MAC Filtering

NOTE: This option is only available in bridge mode. Other modes use IP Filtering to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the VR-3063 can be set according to the following procedure.

COMT	REND Image: Device Info Image: Basic Setup Image: Basic Setup
English Security IP Filtering MAC Filtering	MAC Filtering Setup MAC Filtering is only effective on WAN services configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table. MAC Filtering Policy For Each Interface: WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.
Quality of Service Routing DNS DSL	Interface Policy Change atm0.1 FORWARD Image
Interface Grouping IP Tunnel IPSec Certificate	Choose Add or Remove to configure MAC filtering rules. Interface Protocol Destination MAC Source MAC Frame Direction Remove Add Remove

MAC Filtering is only effective on WAN services configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:

WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Choose **Add** or **Remove** to configure MAC filtering rules. The following screen will appear when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them must be met.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English 🔻	MAC Filtering Setup						
Security	Create a filter to identify th activate the filter.	ne MAC layer frames by	specifying at least one co	ondition below. If multiple cond	tions are specified, all o	f them take effect. Click 'Ap	ply' to save and
IP Filtering	Protocol Type:		•				
MAC Filtering	Destination MAC Address:						
Routing	Source MAC Address:						
DNS	Frame Direction:	LAN<=	>WAN ▼				
DSL	WAN Interfaces (Configure	ed in Bridge mode only)					
DNS Proxy	br 0 0 35/atm01	•					
Interface Grouping	<u>bi_b_b_</u> coldand.1						
IP Tunnel				Save/Apply			
Certificate							

Click **Save/Apply** to save and activate the filter rule.



Consult the table below for detailed field descriptions.

Field	Description
Protocol Type	PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected bridge interface



6.2 Quality of Service (QoS)

NOTE: QoS must be enabled in at least one PVC to display this option. (See Appendix F - Connection Setup for detailed PVC setup instructions).

To Enable QoS tick the checkbox $\ensuremath{\boxtimes}$ and select a Default DSCP Mark.

Click **Save/Apply** to activate QoS.

COMT		ice Info	Advanced Setup	Diagnostics	Management	Logout
English Security Quality of Service QoS Queue QoS Classification	Qo5 Queue Managemen If Enable Qo5 checkbox is sel particular classifier. Click 'App Note: If Enable Qos checkl	t Configuration ected, choose a default differentiat ly/Save' button to save it. box is not selected, all QoS will	ed services code point mark to I be disabled for all interfac	automatically mark in	coming traffic without refe	erence to a
QoS Port Shaping Routing DNS DSL DNS Proxy Interface Grouping IP Tunnel	Note: The default DSCP m	ark is used to mark all egress p lo Change(-1) •	Save/Apply	ny classification rul	es.	

QoS and DSCP Mark are defined as follows:

Quality of Service (QoS): This provides different priority to different users or data flows, or guarantees a certain level of performance to a data flow in accordance with requests from Queue Prioritization.

Default Differentiated Services Code Point (DSCP) Mark: This specifies the per hop behavior for a given flow of packets in the Internet Protocol (IP) header that do not match any other QoS rule.

6.2.1 QoS Queue

6.2.1.1 QoS Queue Configuration

Configure queues with different priorities to be used for QoS setup.

In ATM mode, a maximum of 16 queues can be configured. In PTM mode, a maximum of 8 queues can be configured. For each Ethernet interface, a maximum of 8 queues can be configured.

For each Ethernet WAN interface, a maximum of 8 queues can be configured.



Logout











English 🔻 Security

Quality of Service

QoS Queue Setup In ATM mode, maximum 16 queues can be configured. In PTM mode, maximum 8 queues can be configured. For each Ethernet interface, maximum 8 queues can be configured. To add a queue, click the Add button. To remove queues, check their remove-checkboxes, then click the Remove button. The Enable button will scan through every queue in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checkde will be disabled. The enable-checkbox us shows status of the queue after page reload.

QoS Queue	Note: Ethe	rnet LA	N queue cor	nfigura	ition only takes eff	ect when a	ll the queu	es of the interf	ace have been	configured.	age reioda	
Wlan Queue	Name	Key	Interface	Qid	Prec/Alg/Wght	DSL	PTM	Shaping	Min Bit	Burst	Enable	Remove
QoS Classification				•		Latency	Priority	Rate(bps)	Rate(bps)	Size(bytes)		
Routing	LAIN Q8	1	etni	•	1/5P						•	
DNS	LAN Q7	2	eth1	7	2/SP						•	
DNS Proxy	LAN Q6	3	eth1	6	3/SP						•	
Interface Grouping IP Tunnel	LAN Q5	4	eth1	5	4/SP							
IPSec	LAN Q4	5	eth1	4	5/SP							
Certificate Power Management	LAN Q3	6	eth1	3	6/SP							
Multicast	LAN Q2	7	eth1	2	7/SP							
Wireless	LAN Q1	8	eth1	1	8/SP							
	LAN Q8	9	eth2	8	1/SP							
	LAN Q7	10	eth2	7	2/5P							
	LAN Q6	11	eth2	6	3/SP							
	LAN Q5	12	eth2	5	4/SP							
	LAN Q4	13	eth2	4	5/SP						•	
	LAN Q3	14	eth2	3	6/SP							
	LAN Q2	15	eth2	2	7/SP							
	LAN Q1	16	eth2	1	8/SP							
	LAN Q8	17	eth3	8	1/SP							
	LAN Q7	18	eth3	7	2/SP						•	
	LAN Q6	19	eth3	6	3/5P							
	LAN Q5	20	eth3	5	4/SP						•	
	LAN Q4	21	eth3	4	5/SP						•	
	LAN Q3	22	eth3	3	6/SP							
	LAN Q2	23	eth3	2	7/SP							
	LAN Q1	24	eth3	1	8/SP							
	LAN Q8	25	eth4	8	1/SP							
	LAN Q7	26	eth4	7	2/5P							
	LAN Q6	27	eth4	6	3/SP						•	
	LAN Q5	28	eth4	5	4/SP							
	LAN Q4	29	eth4	4	5/SP							
	LAN Q3	30	eth4	3	6/SP							
	LAN Q2	31	eth4	2	7/SP							
	LAN Q1	32	eth4	1	8/SP							
	Default Queue	97	atm0	1	8/WRR/1	Path0					•	
	Add Er	able	Remove									

To remove queues, check their remove-checkboxes (for user created queues), then click the **Remove** button.

The Enable button will scan through every queue in the table. Queues with the enable-checkbox checked will be enabled. Queues with the enable-checkbox un-checked will be disabled.



The enable-checkbox also shows status of the queue after page reload. Note that if WMM function is disabled in the Wireless Page, queues related to wireless will not take effect. This function follows the Differentiated Services rule of IP QoS.

Enable and assign an interface and precedence on the next screen. Click **Save/Apply** on this screen to activate it.

To add a queue, click the **Add** button to display the following screen.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English •	QoS Queue Setup This screen allows you	ı to configure a QoS qı	ueue and add it to a se	lected layer2 interface.			
Security	Name:						
Quality of Service	Enable:	Enab	le 🔻				
Queue Configuration Wlan Queue	Interface:		T				
QoS Classification QoS Port Shaping				Save/Apply			

Name: Identifier for this Queue entry.

Enable: Enable/Disable the Queue entry.

Interface: Assign the entry to a specific network interface (QoS enabled).

After selecting an Interface the following will be displayed.

COMT		ce Info	Advanced Setup	Diagnostics	Management	Logout
English 🔻	QoS Queue Setup This screen allows you to config	igure a QoS queue and add it to a s	elected layer2 interface.			
Security Quality of Service QoS Queue Queue Configuration Wlan Queue QoS Classification QoS Port Shaping Routing DNS DSL DNS Proxy	Name: Enable: Interface: Queue Precedence - The precedence list shows the - Note that precedence level with - precedence level with WRR/W in precedence level with WRR/W Scheduler Algorithm Weighted Round Robin Weighted Fair Queuing	Enable atm0 (lowe e scheduler algorithm configured at th SP scheduler may have only one VFQ scheduler may have multiple q	er value, higher priority) each precedence level, queue, ueues,			
Interface Grouping IP Tunnel IPSec	Queue Weight: DSL Latency:	1 [1-63] Path0 V				
Certificate			Save/Apply			

The precedence list shows the scheduler algorithm for each precedence level. Queues of equal precedence will be scheduled based on the algorithm. Queues of unequal precedence will be scheduled based on SP.

Click Save/Apply to apply and save the settings.

Scheduler Algorithm: Choose a method for QoS Queue Scheduling.Queue Weight: Represents the priority quantity allocated to this Queue.DSL Latency: The DSL latency set for this queue.

6.2.1.2 Wlan Queue

Displays the list of available wireless queues for WMM and wireless data transmit priority.

COMTR	END	Devi	ce Info	Ba	sic Setup A	dvanced	Setup	Diagnostics	Management	Logout
English 🔻	QoS Wlan Queue Set	tup								
Security	Note: If WMM function	is disab	led in Wireles	s Page,	queues related to v	vireless will r	not take effe	ts.		
Quality of Service	Name	Rey	Interface	Qiu	Prec/Aig/wgiit	CildDie				
Queue Configuration	WMM Voice Priority	33	wian0_0	8	1/5P	Enabled				
Wlan Queue	WMM Voice Priority	34	wlan0_0	7	2/SP	Enabled				
QoS Classification	WMM Video Priority	35	wlan0_0	6	3/SP	Enabled				
QoS Port Shaping	WMM Video Priority	36	wlan0_0	5	4/SP	Enabled				
Routing	WMM Best Effort	37	wlan0_0	4	5/SP	Enabled				
DNS	WMM Background	38	wlan0_0	3	6/SP	Enabled				
DNS Proxy	WMM Background	39	wlan0_0	2	7/SP	Enabled				
Interface Grouping	WMM Best Effort	40	wlan0_0	1	8/SP	Enabled				
IP Tunnel	WMM Voice Priority	65	wlan1_0	8	1/SP	Enabled				
IPSec	White Voice Priority	65	when 1 . 0	7	2/50	Cashlad				
Certificate	WIMM VOICE PRIORICY	00	Wian1_0		2/5P	Enabled				
Power Management Multicast	WMM Video Priority	67	wlan1_0	6	3/SP	Enabled				
Wireless	WMM Video Priority	68	wlan1_0	5	4/SP	Enabled				
	WMM Best Effort	69	wlan1_0	4	5/SP	Enabled				
	WMM Background	70	wlan1_0	3	6/SP	Enabled				
	WMM Background	71	wlan1_0	2	7/SP	Enabled				
	WMM Best Effort	72	wlan1_0	1	8/SP	Enabled				

6.2.2 QoS Classification

The network traffic classes are listed in the following table.

COMT	R	F		D		Device	Info	Basic Set	tup Adv	ance	d Setu	p D	Diagno	S stics	Ma	nager	ment	Lo	g out	
English Security Quality of Service OoS Queue	QoS Classification Setup maximum 32 rules can be configured. To add a rule, click the Add button. To remove rules, check their remove-checkboxes, then click the Remove button. The Enable button will scan through every rule in the table. Rules with enable-checkbox un-checked will be disabled. The enable-checkbox also shows status of the rule after page reload. If you classle WMM function in Wreles Rape, classificator ented to wireless will not take effects																			
Queue Configuration								CLASSIFIC	ATION CRITER	A					CL	ASSIFIC	ATION F	ESULTS		
Wlan Queue	C	lass	Order	Class	Ether	SrcMAC/	DstMAC/	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP	802.1P	Queue	DSCP Mark	802.1P Mark	Rate	Enable Ren	nove
QoS Classification QoS Port Shaping		ame		and	TANG	Plask	Piosk	FrenkLeligti	Add	Enab	le Ren	iove	CHECK	Gneck	ney	PIOT	inark.	Leunickobs		

Click **Add** to configure a network traffic class rule and **Enable** to activate it. To delete an entry from the list, click **Remove**.

This screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one logical condition. All the conditions specified in the rule must be satisfied for it to take effect.

Add Network Traffic Class Rule	
This screen creates a traffic class rule to classify the ingress traffic into a priority Click 'Apply/Save' to save and activate the rule.	queue and optionally mark the DSCP or Ethernet priority of the packet.
Traffic Class Name:	
Rule Order:	Last 🔻
Rule Status:	Enable 🔻
Specify Classification Criteria (A blank criterion indicates it is not used for cla	assification.)
Ingress Interface:	LAN 👻
Ether Type:	•
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	
Specify Classification Results (A blank value indicates no operation.)	
Specify Egress Interface (Required):	
Specify Egress Queue (Required):	~
 Packets classified into a queue that exit through an interface for which the que is not specified to exist, will instead egress to the default queue on the interface. 	ue
Mark Differentiated Service Code Point (DSCP):	
Mark 802.1p priority:	•
 Class non-vlan packets egress to a non-vlan interface will be tagged with VID Class vlan packets egress to a non-vlan interface will have the packet p-bits re Class non-vlan packets egress to a vlan interface will be tagged with the interface Class vlan packets egress to a vlan interface will be additionally tagged with the 	o and the class rule p-bits. -marked by the class rule p-bits. No additional vlan tag is added. sce VID and the class rule p-bits. a packet VID, and the class rule p-bits.
Set Rate Limit:	[Kbits/s]
	Apply/Save

Click **Apply/Save** to save and activate the rule.

Field	Description
Traffic Class Name	Enter a name for the traffic class.
Rule Order	Last is the only option.
Rule Status	Disable or enable the rule.
Classification Criteria	
Ingress Interface	Select an interface: (i.e. LAN, WAN, local, ETH1, ETH2, ETH3, wl0)
Ether Type	Set the Ethernet type (e.g. IP, ARP, IPv6).
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in the Destination MAC Address.
Classification Results	
Specify Egress Interface	Choose the egress interface from the available list.
Specify Egress Queue	Choose the egress queue from the list of available for the specified egress interface.
Mark Differentiated Service Code Point	The selected Code Point gives the corresponding priority to packets that satisfy the rule.
Mark 802.1p Priority	Select between 0-7. - Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits. - Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added. - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits. - Class vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits. - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.
Set Rate Limit	The data transmission rate limit in kbps.



6.2.3 QoS Port Shaping

QoS port shaping supports traffic shaping of the Ethernet interface. Input the shaping rate and burst size to enforce QoS rule on each interface. If "Shaping Rate" is set to "-1", it means no shaping and "Burst Size" will be ignored.

COMTI	REN	D	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English •	QoS Port Sh	aping S	etup					
Security	QoS port shap If `Shaping Ra	oing supp ite' is set	oorts traffic shaping of Ethe to `-1', it means no shapin	ernet interface. Ig and 'Burst Size' w	ill be ignored.			
Quality of Service					_			
QoS Queue	Interface	Туре	Shaping Rate (Kbps)	Burst Size (byte	es)			
Queue Configuration	ETH1	LAN	-1	0				
Wlan Queue								
QoS Classification	ETH2	LAN	-1	0				
QoS Port Shaping	ETH3	LAN	-1	0				
DNS	ETH4	LAN	-1	0				
DSL								
DNS Proxy	Save/Apply							

Click **Save/Apply** to apply and save the settings.

6.3 Routing

The following routing functions are accessed from this menu: **Default Gateway, Static Route, Policy Routing** and **RIP**.

NOTE: In bridge mode, the **RIP** menu option is hidden while the other menu options are shown but ineffective.

6.3.1 Default Gateway

The default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

COMT	REND		Racic Setup		S	Management	
		Device Into	busic Setup	Advanced Setup	Diagnostics	Hanagement	Logout
English v	Routing Default Gatewa	ау					
Security Quality of Service	Default gateway interface list being the highest and the las	t can have multiple WA It one the lowest priorit	N interfaces served as ty if the WAN interface	system default gateways but is connected. Priority order (t only one will be used can be changed by rer	l according to the priority noving all and adding the	with the first m back in again.
Routing Default Gateway	Selected Default Gateway Interfaces	1	Available Route Interfaces	d WAN			
Static Route Policy Routing				*			
DNS		->					
DNS Proxy		<-					
Interface Grouping IP Tunnel	-			-			
IPSec Certificate	WAN Interface selected NO	O CONFIGURED	INTERFACE •				
Power Management				Save/Apply			

Click **Save/Apply** to apply and save the settings.



6.3.2 Static Route

This option allows for the configuration of static routes by destination IP. Click **Add** to create a static route or click **Remove** to delete a static route.

COMT	REND Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English •	Routing Static Route Add Enter the destination network address, subnet m	ask, gateway AND/OR av	vailable WAN interface then (click "Apply/Save" to a	add the entry to the routir	ng table.
Security Quality of Service Routing Default Gateway Static Route Policy Routing RIP DNS	IP Version: Destination IP address/prefix length: Interface: Gateway IP Address: (optional: metric number should be greater than Metric:	or equal to zero)	▼ ▼ Save/Apply			

After clicking **Add** the following will display.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English 🔻	Routing Static Route Ad	d address, subnet mas	sk, gateway AND/OR av	ailable WAN interface then o	click "Apply/Save" to a	dd the entry to the routin	g table.
Security Quality of Service Routing Default Gateway Static Route Policy Routing RIP	IP Version: Destination IP address/prefix l Interface: Gateway IP Address: (optional: metric number shou Metric:	length: Ild be greater than of	equal to zero)	• • •			
DNS				Save/Apply			

- **IP Version:** Select the IP version to be IPv4 or IPv6.
- **Destination IP address/prefix length:** Enter the destination IP address.
- **Interface:** Select the proper interface for the rule.
- Gateway IP Address: The next-hop IP address.
- Metric: The metric value of routing.

After completing the settings, click **Save/Apply** to add the entry to the routing table.

6.3.3 Policy Routing

This option allows for the configuration of static routes by policy. Click **Add** to create a routing policy or **Remove** to delete one.



On the following screen, complete the form and click **Save/Apply** to create a policy.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English •	Policy Routing Settup Enter the policy name, polic Note: If selected "IPOE" as N	ies, and WAN interface WAN interface, default	e then click "Apply/Save gateway must be conf	e" to add the entry to the po igured.	licy routing table.		
Quality of Service Routing Default Gateway	Policy Name:		¥				
Static Route Policy Routing RIP	Source IP:						
DNS DSL DNS Proxy	Default Gateway IP:			Save/Apply			

Field	Description
Policy Name	Name of the route policy
Physical LAN Port	Specify the port to use this route policy
Source IP	IP Address to be routed
Use Interface	Interface that traffic will be directed to
Default Gateway IP	IP Address of the default gateway



6.3.4 RIP

To activate RIP, configure the RIP version/operation mode and select the **Enabled** checkbox \square for at least one WAN interface before clicking **Save/Apply**.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English V Security Quality of Service Routing Default Gateway	Routing RIP NOTE: If selected interface To activate RIP for the WAN I uncheck the 'Enabled' checkbo	e has NAT enabled, of nterface, select the de xx. Click the 'Apply/Sav	only Passive mode is sired RIP version and o ve' button to star/stop	allowed. operation and place a check RIP and save the configurati	in the 'Enabled' check on.	box. To stop RIP on the W	/AN Interface,
Static Route Policy Routing RIP DNS DSL	Send default route	n Enable					



6.4 DNS

6.4.1 DNS Server

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. **DNS Server Interfaces** can have multiple WAN interfaces served as system DNS servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

COMT	REND	M		Ö	C S		\$		
		Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout		
English 🔻	DNS Server Configuratio	'n							
Security Quality of Service Routing	Select DNS Server Interface static IPoE protocol is confi DNS Server Interfaces can highest and the last one the	e from available WAN int gured, Static DNS server have multiple WAN inter e lowest priority if the W	terfaces OR enter stati r IP addresses must be faces served as syster /AN interface is connec	E DNS server IP addresses for e entered. In dns servers but only one w ted. Priority order can be ch	or the system. In ATM ill be used according anged by removing al	mode, if only a single PV to the priority with the firs I and adding them back in	C with IPoA or st being the n again.		
DNS DNS Server	Select DNS Server Selected DNS Server Interfa	Interface from availa	able WAN interfaces Available WAN Ir	terfaces					
Dynamic DNS DSL	^			^					
DNS Proxy Interface Grouping IP Tunnel		->							
IPSec Certificate	-			-					
Power Management Multicast	Use the following set of th	Static DNS IP address	5:						
Wireless	Secondary DNS server:								
	Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses. Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface								
	Obtain IPv6 DNS info from a WAN interface: WAN Interface selected: NO CONFIGURED INTERFACE								
	 Use the following Sta Primary IPv6 DNS server: 	tic IPv6 DNS address:							
	Secondary IPv6 DNS server	: ::							
			S	ave/Apply					

Click **Save/Apply** to save the new configuration.



6.4.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the VR-3063 to be more easily accessed from various locations on the Internet.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Security	Dynamic DNS Choose Add or Remo	ve to configure Dynam	ic DNS.				
Quality of Service Routing DNS DNS Server Dynamic DNS			Hostname	Username Service In Add Remove	terface Remove		

To add a dynamic DNS service, click **Add**. The following screen will display.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Security Quality of Service Routing DNS DNS DNS	Dynamic DNS This page allows you to add a D-DNS provider Hostname Interface	Dynamic DNS addres	s from DynDNS.org, Ta S.org ▼	20, or no-ip.com.			
DNS Server Dynamic DNS DSL DNS Proxy Interface Grouping	DynDNS Settings Username Password			Save/Apply			

Click **Save/Apply** to save your settings.

Consult the table below for field descriptions.

Field	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name of the dynamic DNS server
Interface	Select the interface from the list
Username	Enter the username of the dynamic DNS server
Password	Enter the password of the dynamic DNS server



6.5 DSL

The DSL Settings screen allows for the selection of DSL modulation modes. For optimum performance, the modes selected should match those of your ISP.

COMT	REND 🌆		Ö	E		S
	Device In	fo Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English 🔻	DSL Settings					
Security	Select the modulation below.		Select the	profile below.		
Quality of Service Routing	G.Dmt Enabled		🖉 Sa En	abled		
DNS	 G.lite Enabled 		🕑 Sb En	abled		
DSL	 T1.413 Enabled 		🕑 8c En	abled		
DNS Proxy	AD5L2 Enabled		🕑 Sd En	abled		
IP Tunnel	AnnexL Enabled		🕑 12a E	nabled		
IPSec	ADSL2+ Enabled		12b E	nabled		
Certificate	AnnexM Enabled		🕑 17a E	nabled		
Power Management	VDSL2 Enabled					
Wireless			🕑 356 E	nabled		
			U50			
			🖉 Enabl	ed		
	Select the phone line pair below.					
	Inner pair					
	 Outer pair 					
	Capability					
	 Bitswap Enable 					
	SRA Enable					
	G.997.1 EOC xTU-R Serial Number					
	Equipment Serial Number					
	Equipment MAC Address					
			Save/Apply			

DSL Mode	Data Transmission Rate -	- Mbps (Megabits per second)
G.Dmt	Downstream: 12 Mbps	Upstream: 1.3 Mbps
G.lite	Downstream: 4 Mbps	Upstream: 0.5 Mbps
T1.413	Downstream: 8 Mbps	Upstream: 1.0 Mbps
ADSL2	Downstream: 12 Mbps	Upstream: 1.0 Mbps
AnnexL	Supports longer loops but w	ith reduced transmission rates
ADSL2+	Downstream: 24 Mbps	Upstream: 1.0 Mbps
AnnexM	Downstream: 24 Mbps	Upstream: 3.5 Mbps
VDSL2	Downstream: 100 Mbps	Upstream: 60 Mbps

VDSL Profile	Maximum Downstream Throughput- Mbps (Megabits per second)
8a	Downstream 50
8b	Downstream 50
8c	Downstream: 50
8d	Downstream: 50
12a	Downstream: 68

12b	Downstream: 68
17a	Downstream: 100
35b	Downstream: 300
Options	Description
US0	Band between 20 and 138 kHz for long loops to upstream
Phoneline pair	Select inner pair/outer pair if the DSL line uses alternated pair for data connection
Bitswap Enable	Enables adaptive handshaking functionality
SRA Enable	Enables Seamless Rate Adaptation (SRA)

6.6 DNS Proxy

DNS proxy receives DNS queries and forwards DNS queries to the Internet. After the CPE gets answers from the DNS server, it replies to the LAN clients. Configure DNS proxy with the default setting, when the PC gets an IP via DHCP, the domain name, Home, will be added to PC's DNS Suffix Search List, and the PC can access route with "Comtrend.Setup.Home".

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English	DNS Proxy Configu Enable DNS Prox	uration					
Quality of Service Routing DNS DSL	Host name of the Bro Domain name of the	oadband Router: Cor LAN network: Hor	ntrend.Setup ne				
DNS Proxy				Save/Apply			

See below for further details.

The Host Name and Domain Name are combined to form a unique label that is mapped to the router IP address. This can be used to access the WUI with a local name rather than by using the router IP address. The figure below shows an example of this. In the browser address bar (circled in red) the prefix "http://" is added to the local name "Comtrend.Setup.Home" [Host.Domain] for WUI access.

New Tab	× New Tab	×
$\leftarrow \rightarrow G$	익 www.Comtrend.Setup.Home	



6.7 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button removes mapping groups, returning the ungrouped interfaces to the Default group. Only the default group has an IP interface.

COMT	REI	ND	Device In	fo Basic Setup	Advanced S	S etup	Diagnostics	Management	Logout
English 🔻	Interface grou	ping Confi	guration						
Security Quality of Service Routing	Interface Groupi mapping groups Default group. O	ng supports with approp inly the defa	multiple ports to P priate LAN and WAI ault group has IP in	VC and bridging groups. I N interfaces using the Add terface	ach group will perforn button. The Remove l	n as an inde button will r	ependent network. T emove the grouping	o support this feature, yo and add the ungrouped	u must create interfaces to the
DNS	Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs				
DNS Droxy				ComtrendAFE7_2.4GHz]			
Interface Grouping				ComtrendAFE7_5GHz]			
IP Tunnel	Default			ETH1]			
IPSec	Delaut			ETH2]			
Certificate				ETH3]			
Power Management				ETH4]			
Multicast Wireless	Add Remov	/e				-			

To add an Interface Group, click the **Add** button. The following screen will appear. It lists the available and grouped interfaces. Follow the instructions shown onscreen.



COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Security Quality of Service Routing DNS DSL DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Wireless	Interface grouping Configu To create a new interface grou 1. Enter the Group name and the 2. If you like to automatically a DHCP client request with the sg 3. Select interfaces from the aw that these clients may obtain p 4. Click Apply/Save button to re IMPORTANT If a vendor ID an appropriate IP address. Group Name: Grouped WAN Interfaces Grouped LAN Interfaces Grouped LAN Interfaces Automatically Add Clients W the following DHCP Vendor	ration p: he group name must dd LAN clients to a v cliaidabe interface list a ublic IP addresses nake the changes effi is configured for a	t be unique and select WAN Interface in the n HCP option 60) will be ective immediately a specific client devi Available WAN Available WAN	either 2. (dynamic) or 3. (str ew group add the DHCP ven a denied an IP address from bed interface list using the an ce, please REBOOT the cli Interfaces able LAN Interfaces 11 12 13 14 14 14 10_2 10_3 14 10_2 10_3 11_1	atic) below: dor ID string. By conf the local DHCP server row buttons to create ient device attache	iguring a DHCP vendor ID .' the required mapping of t d to the modem to allo	string any the ports. Note w it to obtain
				Save/Apply			

Automatically Add Clients With Following DHCP Vendor IDs:

Add support to automatically map LAN interfaces to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when Interface Grouping is enabled.

For example, imagine there are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE while the other PVCs are for IP set-top box (video). The LAN interfaces are ETH1(eth1.0), ETH2(eth2.0), ETH3(eth3.0), and ETH4(eth4.0).

The Interface Grouping configuration will be:

- 1. Default: ETH1, ETH2, ETH3, and ETH4.
- 2. Video: nas_0_36, nas_0_37, and nas_0_38. The DHCP vendor ID is "Video".

If the onboard DHCP server is running on "Default" and the remote DHCP server is running on PVC 0/36 (i.e. for set-top box use only). LAN side clients can get IP addresses from the CPE's DHCP server and access the Internet via PPPoE (0/33).

If a set-top box is connected to ETH1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

1. Default: ETH2, ETH3, and ETH4

2. Video: nas_0_36, nas_0_37, nas_0_38, and ETH1.



6.8 IP Tunnel

6.8.1 IPv6inIPv4

Configure 6in4 tunneling to encapsulate IPv6 traffic over explicitly-configured IPv4 links.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English v	IP Tunneling 6in4	Tunnel Configuratio	n				
Security		Name WAN LA	N Dynamic IPv4	Mask Length 6rd Prefix	Border Relay Add	ress Remove	
Quality of Service				Add Remove			
Routing				Add Keniove			
DNS							
DSL							
DNS Proxy							
Interface Grouping							
IP Tunnel							
IPv6inIPv4							
IPv4inIPv6							

Click the **Add** button to display the following.

COMT	REND Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Security Quality of Service Routing DNS DSL DNS Proxy Interface Grouping ID Tunool	IP Tunneling 6in4 Tunnel Configura Currently, only 6rd configuration is support Tunnel Name Mechanism: Associated WAN Interface: Associated LAN Interface:	tion ad. (3RD _AN/br0 ▼	T		
IPv6inIPv4 IPv4inIPv6 IPSec	6rd Prefix with Prefix Length: Border Relay IPv4 Address:		Save/Apply			

Click **Save/Apply** to apply and save the settings.

Options	Description
Tunnel Name	Input a name for the tunnel
Mechanism	Mechanism used by the tunnel deployment
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for point-to-multipoint tunneling / manual for point-to-point tunneling
IPv4 Mask Length	The subnet mask length used for the IPv4 interface
6rd Prefix with Prefix Length	Prefix and prefix length used for the IPv6 interface
Border Relay IPv4 Address	Input the IPv4 address of the other device



6.8.2 IPv4inIPv6

Configure 4in6 tunneling to encapsulate IPv4 traffic over an IPv6-only environment.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Security Quality of Service Routing DNS DSL DNS Proxy Interface Grouping IP Tunnel IPv6inIPv4 IPv4inIPv6	IP Tunneling 4in6 T	funnel Configuration	Name W	AN LAN Dynamic AFTR	Remove		

Click the **Add** button to display the following.

COMT		e Info Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Security Quality of Service Routing DNS DSL DNS Proxy Interface Grouping IP Tunnel IPv6inIPv4 IPv6inIPv6	IP Tunneling 4in6 Tunnel Co Currently, only DS-Lite configuratio Tunnel Name Mechanism: Associated WAN Interface: Associated LAN Interface: Manual C Automatic AFTR:	nfiguration in is supported. DS-L LAN/	te v v or0 v Save/Apply			

Click **Save/Apply** to apply and save the settings.

Options	Description
Tunnel Name	Input a name for the tunnel
Mechanism	Mechanism used by the tunnel deployment
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for point-to-multipoint tunneling / manual for point-to-point tunneling
AFTR	Address of Address Family Translation Router



6.9 IP Sec

You can add, edit or remove IPSec tunnel mode connections from this page.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English • Security	IPSec Tunnel Mode (Add, remove or enable)	Connections /disable IPSec tunnel c	onnections.				
Quality of Service Routing DNS DSI		Connection N	lame Remote Gate	Local Addresses Add Remove	Remote Addresses	Remove	
DNS Proxy Interface Grouping IP Tunnel							
IPv6inIPv6 IPv4inIPv6 IPSec							

Click **Add New Connection** to add a new IPSec termination rule.

COMTREND Device Info Basic Setup Advanced Setup Diagnostics Management Logout English 🔻 IPSec Settings IPSec Connection Name new connection Security Quality of Service IPv4 ▼ IP Version: Routing DNS Tunnel Mode ESP • DSL **DNS Proxy** Local Gateway Interface: Select interface • Interface Grouping IP Tunnel 0.0.0.0 Remote IPSec Gateway Address IPv6inIPv4 Tunnel access from local IP addresses Subnet ٠ IPv4inIPv6 IPSec IP Address for VPN Certificate 255.255.255.0 Mask or Prefix Length Power Management Tunnel access from remote IP addresses Subnet Multicast Wireless IP Address for VPN Mask or Prefix Length 255.255.255.0 Key Exchange Method Auto(IKE) • Pre-Shared Key • Authentication Method Pre-Shared Key key Perfect Forward Secrecy Disable • Show Advanced Settings Advanced IKE Settings Save/Apply

The following screen will display.

IPSec Connection Name	User-defined label
IP Version	Select the corresponding IPv4 / IPv6 version for the IPSEC connection
Tunnel Mode	Select tunnel protocol, AH (Authentication Header) or ESP (Encapsulating Security Payload) for this tunnel.
Local Gateway Interface	Select from the list of wan interface to be used as gateway for the IPSEC connection
Remote IPSec Gateway Address	The location of the Remote IPSec Gateway. IP address or domain name can be used.
Tunnel access from local IP addresses	Specify the acceptable host IP on the local side. Choose Single or Subnet .
IP Address/Subnet Mask for VPN	If you chose Single , please enter the host IP address for VPN. If you chose Subnet , please enter the subnet information for VPN.
Tunnel access from remote IP addresses	Specify the acceptable host IP on the remote side. Choose Single or Subnet .
IP Address/Subnet Mask for VPN	If you chose Single , please enter the host IP address for VPN. If you chose Subnet , please enter the subnet information for VPN.
Key Exchange Method	Select from Auto(IKE) or Manual

For the Auto(IKE) key exchange method, select Pre-shared key or Certificate (X.509) authentication. For Pre-shared key authentication you must enter a key, while for Certificate (X.509) authentication you must select a certificate from the list.

See the tables below for a summary of all available options.

Auto(IKE) Key Exchange Method	
Pre-Shared Key / Certificate (X.509)	Input Pre-shared key / Choose Certificate
Perfect Forward Secrecy	Enable or Disable
Advanced IKE Settings	Select Show Advanced Settings to reveal the advanced settings options shown below.

Advanced IKE Settings	Hide Advanced Settings
Phase 1	
Mode	Main 🔹
Encryption Algorithm	3DES 🔻
Integrity Algorithm	MD5 🔻
Select Diffie-Hellman Group for Key Exchange	1024bit 🔻
Key Life Time	3600 Seconds
Phase 2	
Encryption Algorithm	3DES 🔹
Integrity Algorithm	MD5 🔻
Select Diffie-Hellman Group for Key Exchange	1024bit 🔻
Key Life Time	3600 Seconds
	Save/Apply
L Advanced IKE Settings	Select Hide Advanced Settings to hide the
Advanced IKE Settings	advanced settings options shown above.
Phase 1 / Phase 2	Choose settings for each phase, the available
	options are separated with a "/" character.
Mode	Main / Aggressive
Encryption Algorithm	DES / 3DES / AES 128,192,256
Integrity Algorithm	MD5 / SHA1
Select Diffie-Hellman Group	768 – 8192 bit
Key Life Time	Enter your own or use the default (1 hour)

The Manual key exchange method options are summarized in the table below.

Manual Key Exchange Method	
Key Exchange Method	Manual 🔻
Perfect Forward Secrecy	Disable •
Advanced IKE Settings	Show Advanced Settings
Encryption Algorithm	3DES •
Encryption Key	
	Hex value: DES - 16 digit, 3DES - 48, AES 32, 48, 64 digit
Authentication Algorithm	MD5 🔻
Authentication Key	
	Hex value: MD5 - 32 digit, SHA1 - 40 digit
SPI	101
	Hex value: 100-FFFFFFF
	Save/Apply

Encryption Algorithm	DES / 3DES / AES (aes-cbc)
Encryption Key	DES: 16 digit Hex, 3DES: 48 digit Hex
Authentication Algorithm	MD5 / SHA1
Authentication Key	MD5: 32 digit Hex, SHA1: 40 digit Hex
SPI (default is 101)	Enter a Hex value from 100-FFFFFFFF

6.10 Certificate

A certificate is a public key, attached with its owner's information (company name, server name, personal real name, contact e-mail, postal address, etc) and digital signatures. There will be one or more digital signatures attached to the certificate, indicating that these entities have verified that this certificate is valid.

6.10.1 Local

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English •	Local Certificates Add, View or Remove	certificates from this p	age. Local certificates	are used by peers to verify y	your identity.		
Security	Maximum 4 certificate	es can be stored.					
Quality of Service							
DNS			Name 1	In Use Subject Type	Action		
DSI			Create Certif	icate Request	Certificate		
DNS Proxy							
Interface Grouping							
IP Tunnel							
IPSec							
Certificate							
Local							
Trusted CA							

CREATE CERTIFICATE REQUEST

Click Create Certificate Request to generate a certificate-signing request.

The certificate-signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate-signing request. Your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. Enter the required information and click **Apply** to generate a private key and a certificate-signing request.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Security Quality of Service Routing DNS DSL DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Local Trusted CA	Create new certifica To generate a certifica Country Code for the o Certificate Name: Common Name: Organization Name: State/Province Name: Country/Region Name	ate request te signing request you certificate.	S (United States)	non Name, Organization Nan	ne, State/Province Nar	me, and the 2-letter	



The following table is provided for your reference.

Field	Description
Certificate Name	A user-defined name for the certificate.
Common Name	Usually, the fully qualified domain name for the machine.
Organization Name	The exact legal name of your organization. Do not abbreviate.
State/Province Name	The state or province where your organization is located. It cannot be abbreviated.
Country/Region Name	The two-letter ISO abbreviation for your country.

IMPORT CERTIFICATE

Click **Import Certificate** to paste the certificate content and the private key provided by your vendor/ISP/ITSP into the corresponding boxes shown below.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English V Security Quality of Service Routing DNS DSL	Import certificat Enter certificate na Certificate Name:	e me, paste certificate cont BEGIN CERT <insert certifi<br="">END CERTIF</insert>	ent and private key. IFICATE cate here> ICATE				
DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Local Trusted CA Power Management Multicaet	Certificate:	BEGIN RSA <insert private<br="">END RSA PR</insert>	PRIVATE KEY key here> IVATE KEY				//
Wireless	Private Key:			Apply			A

Enter a certificate name and click the **Apply** button to import the certificate and its private key.



6.10.2 Trusted CA

CA is an abbreviation for Certificate Authority, which is a part of the X.509 system. It is itself a certificate, attached with the owner information of this certificate authority; but its purpose is not encryption/decryption. Its purpose is to sign and issue certificates, in order to prove that these certificates are valid.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Security Quality of Service Routing DNS DSL DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Local	Trusted CA (Certificat Add, View or Remove ce Maximum 4 certificates	te Authority) Certific artificates from this pag can be stored.	cates Le. CA certificates are u Name	Subject Type Action Import Certificate	certificates.		

Click **Import Certificate** to paste the certificate content of your trusted CA. The CA certificate content will be provided by your vendor/ISP/ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Security Quality of Service Routing DNS DSL DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Local Trusted CA Power Management	Import CA certificate Enter certificate name : Certificate Name:	e and paste certificate conte BEGIN CERTI <insert certific<br="">END CERTIFI</insert>	nt. FICATE ate here> CATE				
Multicast Wireless				Apply			

Enter a certificate name and click **Apply** to import the CA certificate.

6.11 Power Management

This screen allows for control of hardware modules to evaluate power consumption. Use the buttons to select the desired option, click **Apply** and check the response.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English •	Power Management						
Security Quality of Service Routing DNS DSL DNS Proxy	This page allows control of click Apply and check the Host CPU Clock divider Enable Status:	of Hardware modules to status response when Idle Enabled	o evaluate power consu	mption. Use the control but	tons to select the desi	red option,	
Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Wireless	Wait instruction when PEnable Status: Ethernet Auto Power E PEnable Status:	Idle Enabled Down and Sleep Enabled					
			Save/Apply	Refresh			



6.12 Multicast

Input new IGMP or MLD protocol configuration fields if you want modify default values shown. Then click **Save/Apply**.

COMT	REND Device Info Basic Setup Advanced Setup Diagnostics Advanced Setup Logout
English Security Quality of Service Routing DNS DSL DNS Proxy Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Wireless	<form><form><form><form><form><form><form><form><form></form></form></form></form></form></form></form></form></form>
	Save/Apply

Multicast Precedence:

Select precedence of multicast packets.

Multicast Strict Grouping Enforcement:

Enable/Disable multicast strict grouping.

The following table is provided for your reference.



Field	Description
Default Version	Define IGMP using version with video server.
Query Interval	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). The default query interval is 125 seconds.
Query Response Interval	The query response interval is the maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.
Last Member Query Interval	The last member query interval is the amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages. The default last member query interval is 10 seconds.
Robustness Value	The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2.
Maximum Multicast Groups	Setting the maximum number of Multicast groups.
Maximum Multicast Data Sources (for IGMPv3)	Define the maximum multicast video stream number.
Maximum Multicast Data Sources (for mldv2)	Define the maximum multicast video stream number from IPv6 source.
Maximum Multicast Group Members	Setting the maximum number of groups that ports can accept.
Fast Leave Enable	When you enable IGMP fast-leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port.

IGMP Group Exception List / MLD Group Exception List

Field	Description
Group Address	This is the delimited list of ignored multicast addresses being queried when sending a Group-Specific or Group-and-Source-Specific Query.
Mask/Mask Bits	This is the delimited list of ignored multicast mask being queried when sending a Group-Specific or Group-and-Source-Specific Query.

Field	Description
Remove	Allows a user to remove a specific item in the exception list.

6.13 Wireless

6.13.1 Basic 2.4GHz

The Basic option allows you to configure basic features of the wireless LAN interface. Among other things, you can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.

COMT	REN	D M		0	¢	3	₹ġ		Ş
		Device Info	Basic	: Setup	Advanc	ed Setup	Diagnostics	Management	Logout
English v	Wireless Bas	iic							
Security Quality of Service	This page allows network from ac	you to configure basic feature tive scans, set the wireless ne	es of the wir twork name	eless LAN int (also known	erface. You as SSID) a	can enable or nd restrict the	disable the wireless L channel set based on	AN interface, hide the country requirements.	
Routing	Enable	Wireless							
DSL	Hide Ad	cess Point							
DNS Proxy Interface Grouping	SSID: Co	mtrendAFE7_2.4GHz							
IP Tunnel IPSec	Country:	U	S V						
Certificate	Bandwidth:	4	0 MHz 🔻]					
Multicast	Maximum Client	is: 64							
Wireless 2.4GHz	Wireless - Gue	st/Virtual Access Points:							
Basic	Enable	SSID	Hidden	Maximum Clients	BSSID				
Advanced		Guest2		64	N/A				
5GHz		Guest3		64	N/A				
	Save/Apply								

Click **Save/Apply** to configure the basic wireless options.

Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox \square that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To view and connect to available wireless networks in Windows, open Connect to a Network by clicking the network icon (



Option	Description
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
Channel	Drop-down menu that allows selection of a specific channel.
Country	Local regulations limit channel range: 11 Channels (US, Canada)
Bandwidth	To utilize maximum data throughput, select 40MHz in 2.4G band.
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes ☑ in the Enabled column. To hide a Guest SSID select its checkbox ☑ in the Hidden column.
	Advertise. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for Enable WMF , Max Clients and BSSID , consult the matching entries in this table.
	NOTE: Remote wireless hosts cannot scan Guest SSIDs.



6.13.2 Security 2.4GHz

The following screen appears when Wireless Security is selected. The options shown here allow you to configure security features of the wireless LAN interface.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English •	Wireless Security						
Security Quality of Service Routing	This page allows you to confi You may setup configuration Note: When both STA PIN ar WPS will be disabled	gure security features manually or through V d Authorized MAC are	of the wireless LAN i ViFi Protected Setup(empty, PBC is used.	nterface. WPS) If Hide Access Point enabled	d or Mac filter list is er	mpty with 'allow' chosen,	
DNS DSI	WPS Setup						
DNS Proxy	Enable WPS	Enable	T				
Interface Grouping							
IP Tunnel	Add Client (This feature i	is only available for WF	PA2-PSK mode or OPI	EN mode with WEP disabled)		
Certificate		Use 5	TA PIN	ee			
Power Management	Manual Setup AP						
Multicast Wireless	You can set the network auth wireless network and specify	nentication method, se the encryption strengt	lecting data encryptic h.	on, specify whether a netwo	rk key is required to a	authenticate to this	
2.4GHz	Select SSID:	Comtre	endAFE7_2.4GF	Iz ▼			
Basic Security	Network Authentication:	WPA2	-PSK	¥			
Advanced	WPA/WAPI passphrase:	•••••	Click	here to display			
5GHz	WPA/WAPI Encryption:	AES	▼				
	WEP Encryption:	Disable	ed 🔻				
		Save/A	pply				

Please see 6.13.3 for WPS setup instructions.

Click **Save/Apply** to implement new configuration settings.

WIRELESS SECURITY

Setup requires that the user configure these settings using the Web User Interface (see the table below).

Select SSID

Select the wireless network name from the drop-down menu. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that client will not be granted access.

Network Authentication

This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified.

Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.

Different authentication type pops up different settings requests.

Choosing **WPA2-PSK**, you must enter WPA/WAPI passphrase and Group Rekey Interval.

WEP Encryption

This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic.

When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

Encryption Strength

This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

6.13.3 WPS 2.4GHz

Wi-Fi Protected Setup (WPS) is an industry standard that simplifies wireless security setup for certified network devices. Every WPS certified device has both a PIN number and a push button, located on the device or accessed through device software. The VR-3063 has a 2.4G WiFi On/Off & WPS button on the device.

Devices with the WPS logo (shown here) support WPS. If the WPS logo is not present on your device it still may support WPS, in this case, check the device documentation for the phrase "Wi-Fi Protected Setup".



NOTE: WPS is available in Open, WPA2-PSK and Mixed WPA2/WPA-PSK network authentication modes. Other authentication modes do not use WPS so they must be configured manually.

To configure security settings with WPS, follow the procedures below.

I. Setup

Step 1: Enable WPS by selecting **Enabled** from the drop down list box shown.

WPS Setup	
Enable WPS	Enable •

IIa. PUSH-BUTTON CONFIGURATION

The WPS push-button configuration provides a semi-automated configuration method. The 2.4G WiFi On/Off & WPS button on the front panel of the router can be used for this purpose.

The WPS push-button configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your WLAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE: The wireless AP on the router searches for 2 minutes. If the router stops searching before you complete Step 4, return to Step 3.

Step 2: Press WPS button

Press and release the 2.4G WiFi On/Off & WPS button on the front panel of the router. The WPS LED will blink to show that the router has begun searching for the client.

Step 3: Go to your WPS wireless client and activate the push-button function. A typical WPS client screenshot is shown below as an example.

PIN	WPS Associate IE	Progress >> 25%
PBC	WPS Probe IE	PBC - Sending EAPOL-Start

Now go to Step 4 (part III. Check Connection) to check the WPS connection.



IIb. WPS – PIN CONFIGURATION

Using this method, security settings are configured with a personal identification number (PIN). The PIN can be found on the device itself or within the software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check the device documentation for specific instructions.

The WPS PIN configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your wireless LAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

- **Step 2:** Select the Use STA PIN radio button in the WPS Setup section of the Wireless Security screen, as shown in **A** below.
 - **A** Input the STA PIN* and click the **Add Enrollee** button.

Use STA PIN	Use AP PIN	Add Enrollee
12345678	Help	

* Personal Identification Number (PIN) has to be read from either a sticker or the display on the new wireless device.

Step 3: Activate the PIN function on the wireless client. The client must be configured as an Enrollee.

The figure below provides an example of a WPS client PIN function in-progress.



III. CHECK CONNECTION

Step 4: If the WPS setup method was successful, you will be able access the wireless AP from the client. The client software should show the status. The example below shows that the connection established successfully.



You can also double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the status of the new connection.



6.13.4 Advanced 2.4GHz

The Advanced screen allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click **Save/Apply** to set new advanced wireless options.

COMT	REND	Jr-	9	Ö	Ś		2
		Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English V	Wireless Advanced						
Security Quality of Service	This page allows you to configure to a particular speed, set the frag access point, set XPress mode an Click "Apply/Save" to configure th	e advanced features of gmentation threshold, s id set whether short or ne advanced wireless o	the wireless LAN interfa et the RTS threshold, s long preambles are use ptions.	ice. You can select a particular et the wakeup interval for clier ed.	r channel on which to op nts in power-save mode,	perate, force the transmissi set the beacon interval for	on rate r the
DNS DSL	Band: Fragmentation Threshold: RTS Threshold:	2.4GHz v 2346 2347					
DNS Proxy Interface Grouping IP Tunnel	DTIM Interval: Beacon Interval: Enable Smart Antenna Selection:	1 100 Enable ▼	-				
IPSec Certificate	Transmit Power:	100% ▼	S	ave/Apply			
Power Management Multicast Wireless							
2.4GHz Basic							
Security Advanced 5GHz							

Field	Description
Band	Set to 2.4 GHz for compatibility with IEEE 802.11x standards. The new amendment allows IEEE 802.11n units to fall back to slower speeds so that legacy IEEE 802.11x devices can coexist in the same network. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11a has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.

Field	Description
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Enable Smart Antenna Selection	The smart antenna feature can be enabled to allow the wireless chip to detect client position and automatically select wireless antenna to provide maximum performance at a different angle.
Transmit Power	Set the power output (by percentage) as desired.

6.13.5 Basic 5GHz

The Basic option allows you to configure basic features of the wireless LAN interface. Among other things, you can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.

COMT	REI	ND	Device Info	Basi	ic Setup	Adva	nced Setup	Diagnostics	Management	Logout
English V Security Quality of Service Routing DNS DSL DNS Proor	Wireless - This page a the networ requiremer E E H	Basic allows you to conf k from active scar its. nable Wireless ide Access Point	igure basic features is, set the wireless n	of the wir etwork na	eless LAN ini ame (also kn	erface. Yo own as SS	u can enable or d ID) and restrict th	isable the wireless LA e channel set based o	N interface, hide on country	
Interface Grouping IP Tunnel IPSec Certificate Power Management Multicast Wireless 2.4GHz	SSID: Channel: Country: Bandwidth Maximum Wireless -	ComtrendAFE7 :: Clients: • Guest/Virtual J	Access Points:	0 ▼ ▼ MHz ▼]					
5GHz Basic Security Advanced	Enable	st wl1_Guest1 wl1_Guest2 wl1_Guest3	5ID	Hidden	Maximum Clients 64 64 64 64	BSSID N/A N/A N/A				

Click **Save/Apply** to configure the basic wireless options.

Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox \square that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To view and connect to available wireless networks in Windows, open Connect to a Network by clicking the network icon (all or b) in the notification area. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.

Option	Description
SSID	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct
[1-32 characters]	SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
Channel	Drop-down menu that allows selection of a specific channel.
Country	Local regulations limit channel range: US/Canada = 1-11.
Bandwidth	To utilize maximum data throughput, select 80MHz in 5G band.
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes \square in the Enabled column. To hide a Guest SSID select its checkbox \square in the Hidden column.
	Do the same for Isolate Clients and Disable WMM Advertise . For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for Enable WMF , Max Clients and BSSID , consult the matching entries in this table.
	NOTE: Remote wireless hosts cannot scan Guest SSIDs.



6.13.6 Security 5GHz

The following screen appears when Wireless Security is selected. The options shown here allow you to configure security features of the wireless LAN interface.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English V	Wireless Security	uro conurity footuroo o	of the wireless I AN in	terface.			
Security Quality of Service Routing	You may setup configuration n You may setup configuration n Note: When both STA PIN and chosen, WPS will be disabled	ure security reatures o nanually or through Wi Authorized MAC are e	iFi Protected Setup(W empty, PBC is used. If	ierrace. IPS) Hide Access Point enabled	or Mac filter list is em	pty with 'allow'	
DNS DSL DNS Proxy	WPS Setup Enable WPS	Enable	V				
Interface Grouping IP Tunnel IPSec Certificate	Add Client (This feature is	only available for WP/	A2-PSK mode or OPEI utton Add Enrolle	N mode with WEP disabled) e			
Power Management	Manual Setup AP						
Wireless	You can set the network author this wireless network and spec	ntication method, sele ify the encryption stre	ecting data encryption ength.	, specify whether a network	c key is required to au	thenticate to	
2.4GHz 5GHz	Select SSID:	Comtrer	ndAFE7_2.4GH	<u>z</u> v			
Basic Security	Network Authentication:	WPA2 -	PSK	•			
Advanced	WPA/WAPI passphrase: WPA/WAPI Encryption: WEP Encryption:	AES Disabler		<u>ere to display</u>			
		Save/App	bly				

Please see 6.13.7 for WPS setup instructions.

Click **Save/Apply** to implement new configuration settings.

WIRELESS SECURITY

Setup requires that the user configure these settings using the Web User Interface (see the table below).

Select SSID

Select the wireless network name from the drop-down menu. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that client will not be granted access.

Network Authentication

This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified.

Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.

Different authentication type pops up different settings requests.

Choosing **802.1X**, enter RADIUS Server IP address, RADIUS Port, RADIUS key and Current Network Key.

Also, enable WEP Encryption and select Encryption Strength.



Choosing **WPA2-PSK**, you must enter WPA/WAPI passphrase and Group Rekey Interval.

WEP Encryption

This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic.

When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

Encryption Strength

This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers. Each key contains a 24-bit header (an initiation vector) which enables parallel decoding of multiple streams of encrypted data.

6.13.7 WPS 5GHz

Wi-Fi Protected Setup (WPS) is an industry standard that simplifies wireless security setup for certified network devices. Every WPS certified device has both a PIN number and a push button, located on the device or accessed through device software. The VR-3063 has a WiFi On/Off & WPS button on the device.

Devices with the WPS logo (shown here) support WPS. If the WPS logo is not present on your device it still may support WPS, in this case, check the device documentation for the phrase "Wi-Fi Protected Setup".



NOTE: WPS is available in Open, WPA2-PSK and Mixed WPA2/WPA-PSK network authentication modes. Other authentication modes do not use WPS so they must be configured manually.

To configure security settings with WPS, follow the procedures below.

I. Setup

Step 1: Enable WPS by selecting **Enabled** from the drop down list box shown.

WPS Setup	
Enable WPS	Enable •

Ia. PUSH-BUTTON CONFIGURATION

The WPS push-button configuration provides a semi-automated configuration method. The WiFi On/Off & WPS button on the front panel of the router can be used for this purpose.

The WPS push-button configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your WLAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

NOTE: The wireless AP on the router searches for 2 minutes. If the router stops searching before you complete Step 4, return to Step 3.

Step 2: Press WPS button

Press and release the 2.4G WiFi On/Off & WPS button on the front panel of the router. The WPS LED will blink to show that the router has begun searching for the client.

Step 3: Go to your WPS wireless client and activate the push-button function. A typical WPS client screenshot is shown below as an example.

<u>P</u> IN	WPS Associate IE		Progress >> 25%
P <u>B</u> C	WPS Probe IE	PBC - Sending EAPOL	-Start

Now go to Step 4 (part III. Check Connection) to check the WPS connection.



IIb. WPS – PIN CONFIGURATION

Using this method, security settings are configured with a personal identification number (PIN). The PIN can be found on the device itself or within the software. The PIN may be generated randomly in the latter case. To obtain a PIN number for your client, check the device documentation for specific instructions.

The WPS PIN configuration is described in the procedure below. It is assumed that the Wireless function is Enabled and that the router is configured as the Wireless Access Point (AP) of your wireless LAN. In addition, the wireless client must also be configured correctly and turned on, with WPS function enabled.

- **Step 2:** Select the Use STA PIN radio button in the WPS Setup section of the Wireless Security screen, as shown in **A** below.
 - **A** Input the STA PIN* and click the **Add Enrollee** button.



* Personal Identification Number (PIN) has to be read from either a sticker or the display on the new wireless device.

Step 3: Activate the PIN function on the wireless client. The client must be configured as an Enrollee.

The figure below provides an example of a WPS client PIN function in-progress.

<u>P</u> IN	🗹 WPS Associate IE	Progress >> 30%
PBC	WPS Probe IE	PIN - Sending EAP-Rsp(ID)
	Auto	

III. CHECK CONNECTION

Step 4: If the WPS setup method was successful, you will be able access the wireless AP from the client. The client software should show the status. The example below shows that the connection established successfully.

PIN	WPS Associate IE	Progress >> 100%
PBC	WPS Probe IE	PBC - Get WPS profile successfully.
	Auto	

You can also double-click the Wireless Network Connection icon from the Network Connections window (or the system tray) to confirm the status of the new connection.



6.13.8 Advanced 5GHz

The Advanced screen allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click **Save/Apply** to set new advanced wireless options.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Security	Wireless Advanced This page allows you to configu force the transmission rate to a	ure advanced features particular speed, set	of the wireless LAN in the fragmentation th	nterface. You can select a p reshold, set the RTS thresho	articular channel on v old, set the wakeup in	which to operate, terval for clients	
Quality of Service Routing DNS DSL DNS Proxy Interface Grouping IP Tunnel IPSec Certificate	in power-save mole, set the be Click "Apply/Save" to configure Band: Fragmentation Threshold: RTS Threshold: DTIM Interval: Beacon Interval: Enable Smart Antenna Selection Transmit Power:	accon interval for the 2.4GHz 2346 2347 1 100 n: Enable 100% ▼	set Arre	ss mode and set whether s	nort or long preamble	s are used.	
Power Management Multicast Wireless 2.4GHz 5GHz Basic Security Advanced			Save/App	ły			

Field	Description
Band	5GHz band is used for high speed wireless network as defined in IEEE 802.11ac
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.



Field	Description
DTIM Interval	Delivery Traffic Indication Message (DTIM) is also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions in milliseconds. The default is 100 ms and the acceptable range is 1 – 65535. The beacon transmissions identify the presence of an access point. By default, network devices passively scan all RF channels listening for beacons coming from access points. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Enable Smart Antenna Selection	The smart antenna feature can be enabled to allow wireless chip to detect client position and automatically select wireless antenna to provide maximum performance at different angle.
Transmit Power	Set the power output (by percentage) as desired.



Chapter 7 Diagnostics

You can reach this page by clicking on the following icon located at the top of the screen.



7.1 Diagnostics – Individual Tests

The first Diagnostics screen is a dashboard that shows overall connection status.

COMT	REND				Ö	SE SE	3		×
		Device Info	Basic Setup	Adv	anced Setup	Diagno	stics	Management	Logout
English •		System				LA	N		
Diagnostics	Model	VR-3063u							
Ethernet OAM	Board ID	63138MV-1851AC2			لا		ل	لا	
Ping	Serial Number	0			ETH1	ETH2	ETH3	ETH4	
TraceRoute	Firmware Version	K011-416CTU- C02_R02.A2pvfbH043	3l.d26r		LAN IPv4 Address		192.168.1	.1	
	Bootloader (CFE) Version	1.0.38-118.8-2		L	LAN Subnet Mask		255.255.2	55.0	
	Up Time	48 mins:36 secs		_	LAN MAC Address		64:68:0c:	ff:af:e7	
				L	DHCP Server		Enabled		
	Wi	reless							
	2.4GHz	Interface					VVAIN		
	Driver Version	4.6.92.8.5.0							
	Primary SSID	ComtrendAFE7_2	2.4GHz						
	Status	Enabled					DOWN		_
	Channel	1		_ L	Default Gateway				
				Primary DNS Server		0.0.0.0	0.0.0.0		
		Secure		L	Secondary DNS Se	rver	0.0.0.0		
	Primary Encryption	WPA2-PSK AES							
	Primary Passphrase/Key	Show							
	5GHz I	nterface							
	Driver Version	4.6.92.8.5.0							
	Primary SSID	ComtrendAFE7_5	iGHz						
	Status	Enabled							
	Channel	36 Secure							
	Primary Encryption	WPA2-PSK AES							
	Primary Passphrase/Key	Show							

Click the Diagnostics Menu item on the left side of the screen to display the individual connections.



COMT		fo	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Diagnostics Ethernet OAM Ping TraceRoute	Diagnostics The individual tests are listed below. If a t fail status is consistent. If the test continu Test the connection to your local netw Test your ETHU Connection: Test your 2.4GHz Wireless Connection	st displays s to fail, cli rork FAIL FAIL PASS FAIL FAIL FAIL R: PASS PASS	a fail status, click Help Help Help Help Help Help Help Help	c'Rerun Diagnostic Tests' at bw the troubleshooting proc	the bottom of this pa edures.	ge to make sure the	

7.2 Ethernet OAM

The Ethernet OAM (Operations, Administration, Management) page provides settings to enable/disable 802.3ah, 802.1ag/Y1.731 OAM protocols.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Diagnostics Ethernet OAM Ping TraceRoute	Ethernet Link OAM (802 Enable Ethernet Service OAM (8 Enable (8) 802.1ag	.3ah) 802.1ag / Y.1731) © Y.1731	Save/A	pply	ittom of this pa	ge to make sure the	

To enable Ethernet Link OAM (802.3 ah), click Enabled to display the full configuration list. At least one option must be enabled for 802.1ah.

Ethernet Link OAM (802.3ah)							
Enabled							
WAN Interface:	•						
OAM ID:	1	(positive integer)					
Auto Event							
Variable Retrieval							
Link Events							
Remote Loopback							
Active Mode							



WAN Interface	Select layer 2 WAN interface for outgoing OAM packets
OAM ID	OAM Identification number
Auto Event	Supports OAM auto event
Variable Retrieval	Supports OAM variable retrieval
Link Events	Supports OAM link events
Remote Loopback	Supports OAM remove loopback
Active mode	Supports OAM active mode



To enable Ethernet Service OAM (802.1ag/Y1731), click Enabled to display the full configuration list.

Ether	Ethernet Service OAM (802.1ag / Y.1731)								
1	V Enabled 802.1ag Y.1731								
	WAN Interface:	•	~						
	MD Level:	0 🔻 [0-7	0 🗸 [0-7]						
	MD Name:	Broadcom	[e.g. B	roadcom]					
	MA ID:	BRCM	[e.g. B	RCM]					
	Local MEP ID:	1	[1-819	1]					
	Local MEP VLAN ID:	-1	[1-409	4] (-1 means no VLAN tag)					
	CCM Transmission								
	Remote MEP ID:	-1	[1-819	1] (-1 means no Remote ME	P)				
Loop	back and Linktrace T	est							
	Target MAC:		[e.g. 0	2:10:18:aa:bb:cc]					
	Linktrace TTL:	-1	[1-255]] (-1 means no max hop limi	it)				
Loo	pback Result:	N/A							
Link	ttrace Result:	N/A							
	Send Loopback Send Linktrace								
	Apply/Save								

Click **Apply/Save** to implement new configuration settings.

WAN Interface	Select from the list of WAN Interfaces to send OAM packets
MD Level	Maintenance Domain Level
MD Name	Maintenance Domain name
MA ID	Maintenance Association Identifier
Local MEP ID	Local Maintenance association End Point Identifier
Local MEP VLAN ID	VLAN IP used for Local Maintenance End point

Click CCM Transmission to enable CPE sending Continuity Check Message (CCM) continuously.

Remote MEP ID	Maintenance association End Point Identifier for the remote
	receiver

To perform Loopback/Linktrace OAM test, enter the Target MAC of the destination and click "Send Loopback" or "Send Linktrace" button.

Target MAC	MAC Address of the destination to send OAM loopback/linktrace packet
Linktrace TTL	Time to Live value for the loopback/linktrace packet



7.3 Ping

Input the IP address/hostname and click the **Ping** button to execute ping diagnostic test to send the ICMP request to the specified host.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Diagnostics Ethernet OAM Ping TraceRoute	Ping Send ICMP ECHO_REQUEST IP Address/Hostname: PING 192.168.1.1 (192.168 64 bytes from 192.168.1.1: 64 bytes from 192.168.1.1: 64 bytes from 192.168.1.1: 192.168.1.1 ping statist 4 packet transmitted, 4 pa round-trip min/avg/max = (packets to network h	234 ms 234 ms 376 ms 394 ms 380 ms ket loss	Ping			



7.4 Trace Route

Input the IP address/hostname and click the **TraceRoute** button to execute the trace route diagnostic test to send the ICMP packets to the specified host.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English T	TraceRoute						
Diagnostics	Send packets the host addres	ss specified and trace e	ach routing gateway t	he packets pass through.			
Ethernet OAM Ping	IP Address/Hostname:			TraceRoute			
TraceRoute	traceroute to 192.168.1.1 (19 1 192.168.1.1 (192.168.1.1)	92.168.1.1), 30 hops m 0.188 ms	ax, 38 byte packets				



Chapter 8 Management

You can reach this page by clicking on the following icon located at the top of the screen.



The Management menu has the following maintenance functions and processes:

8.1 Settings

This includes Backup Settings, Update Settings, and Restore Default screens.

8.1.1 Backup Settings

To save the current configuration to a file on your PC, click **Backup Settings**. You will be prompted for backup file location. This file can later be used to recover settings on the **Update Settings** screen, as described below.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English 🔻	Backup Settings						
Settings	Backup Broadband Route	r configurations. You	may save your router	configurations to a file on y	our PC.		
Backup							
Update Restore Default			Back	up Settings			
System Log							
SNMP Agent							
TR-069 Client							
Internet Time							
Access Control							
Update Software							
Reboot							



8.1.2 Update Settings

This option recovers configuration files previously saved using **Backup Settings**. Press **Browse...** to search for the file, or enter the file name (including folder path) in the **File Name** box, and then click **Update Settings** to recover settings.

COMT	REND	Device Info	Basic Setup	Advanced Setur	Diagnostics	Management	
		Device Into	busic occup	Advanced Secup	Diagnostics	Management	Logour
English V Settings Backup Update Restore Default System Log SNMP Agent TR-069 Client Internet Time Access Control	Update Settings Update Broadband Route File Name:	er settings. You may (Browse	update your router sel	tings using your saved files ate Settings			
Reboot							

8.1.3 Restore Default

Click Restore Default Settings to restore factory default settings.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English V Settings Backup Update Restore Default System Log SNMP Agent TR-069 Client Internet Time Access Control Update Software Reboot	Restore Default Setting Restore Broadband Router	gs r settings to the factor	y defaults. Restore De	fault Settings			

After **Restore Default Settings** is clicked, the following screen appears.

DSL Router Restore

The DSL Router configuration has been restored to default settings and the router is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Close the browser and wait for 2 minutes before reopening it. It may also be necessary, to reconfigure your PC IP configuration to match any new settings.

NOTE: This entry has the same effect as the **Reset** button. The VR-3063 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 10 seconds, the current configuration data will be erased. If the **Reset** button is continuously pressed for more than 60 seconds, the boot loader will erase all configuration data saved in flash memory and enter bootloader mode.

8.2 System Log

This function allows a system log to be kept and viewed upon request.

Follow the steps below to configure, enable, and view the system log.

STEP 1: Click **Configure System Log**, as shown below (circled in **Red**).

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English V	System Log						
Settings	The System Log dialog all	lows you to view the S	ystem Log and config	ure the System Log options.			
System Log	Click 'View System Log' to	view the System Log.					
SNMP Agent	Click 'Configure System Lo	og' to configure the Sy	stem Log options.				
TR-069 Client							
Internet Time		ſ	View System Log	Configure System Log			
Access Control		l	view System Log	Conligure System Log			
Update Software							
Reboot							

STEP 2: Select desired options and click **Save/Apply**.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English V Settings System Log SNMP Agent TR-069 Client Internet Time Access Control Update Software Reboot	System Log If the log mode is enable level will be logged. For th Remote' or 'Both,' events or 'Both,' events will be re Select the desired values Log:	d, the system will begin he Display Level, all loy will be sent to the spy and click 'Apply/Save' sable © Enable Debugging • Error • Local •	n to log all the selecte gged events above or scified IP address and emory. to configure the syste	id events. For the Log Level equal to the selected level v UDP port of the remote sys im log options.	, all events above or e will be displayed. If th log server. If the sele	qual to the selected e selected mode is ted mode is 'Local'	

Consult the table below for detailed descriptions of each system log option.

Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, select the Enable radio button and then click Save/Apply .



Option	Description
Log Level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the VR-3063 SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level.
	The log levels are defined as follows:
	 Emergency = system is unusable Alert = action must be taken immediately Critical = critical conditions Error = Error conditions Warning = normal but significant condition Notice= normal but insignificant condition Informational= provides information for reference Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only
Display	Allows the user to select the logged events and displays on the View
Level	System Log window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

STEP 3: Click **View System Log**. The results are displayed as follows.

System Log					
	Message	Severity	Facility	Date/Time	
0+0000	BCM96345 started: BusyBox v0.60.4 (2004.09.14-06:30+0	emerg	syslog	Jan 1 00:00:12	
	klogd: USB Link UP.	crit	user	Jan 1 00:00:17	
	klogd: eth0 Link UP.	crit	user	Jan 1 00:00:19	
_	klogd: USB Link UP. klogd: eth0 Link UP.	crit crit	user user	Jan 1 00:00:17 Jan 1 00:00:19	

8.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device. Select the **Enable** radio button, configure options, and click **Save/Apply** to activate SNMP.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English 🔻	SNMP - Configuratio	n					
Settings System Log SNMP Agent TR-069 Client Internet Time Access Control Update Software Reboot	Simple Network Manag status from the SNMP a Select the desired value SNMP Agent Read Community: Set Community: System Name: System Name: System Location: System Contact: Trap Manager IP:	ement Protocol (SNMP agent in this device. es and click "Apply" to Disable public private Broadcom unknown unknown 0.0.0.0	allows a manageme configure the SNMP () Save/Apply	ent application to retrieve st	atistics and		

8.4 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select desired values and click **Save/Apply** to configure TR-069 client options.

COMT	REND	Device Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout		
English T	TR-069 client - Config	uration							
	WAN Management Proto	col (TR-069) allows a	Auto-Configuration S	erver (ACS) to perform auto	-configuration,				
Settings	provision, collection, and	provision, collection, and diagnostics to this device.							
System Log	Select the desired values	and click 'Apply/Save	e' to configure the TR-	-069 client options.					
SNMP Agent	OUI-serial			Serialnumber					
TR-069 Client	Inform		Disable	Enable					
Internet Time									
Access Control	Inform Interval:		300						
Update Software	ACS URL:								
Reboot	ACS Username:		admin						
	ACS Password:			NI -					
	WAN Interface:		Any_wA						
	 Connection Request 	Authentication							
	Connection Request User	name:	admin						
	Connection Request Pass	word:	•••••						
	Connection Request URL:								
		Save/A	pply Get RPC Meth	hod					

The table below is provided for ease of reference.

Option	Description
OUI-serial	The serial number used to identify the CPE when making a connection to the ACS using the CPE WAN Management Protocol. Select MAC to use the router's MAC address as serial number to authenticate with the ACS or select serial number to use the router's serial number.
Inform	Disable/Enable TR-069 client on the CPE.
Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.



Option	Description			
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.			
WAN Interface used by TR-069 client	Choose Any_WAN, LAN, Loopback or a configured connection.			
Connection Request				
Authentication	Tick the checkbox ☑ to enable.			
User Name	Username used to authenticate an ACS making a Connection Request to the CPE.			
Password	Password used to authenticate an ACS making a Connection Request to the CPE.			
URL	IP address and port the ACS uses to connect to the router.			

The **Send Inform** button forces the CPE to establish an immediate connection to the ACS.



8.5 Internet Time

This option automatically synchronizes the router time with Internet timeservers. To enable time synchronization, tick the corresponding checkbox \square , choose your preferred time server(s), select the correct time zone offset, and click **Save/Apply**.

COMT	REND	vice Info	Basic Setup	Advanced Setup	Diagnostics	Management	Logout
English Settings System Log SNMP Agent TR-069 Client	Time Settings This page allows you to the ma Automatically synchronize First NTP time server:	with Internet	figuration. time servers	•	_		
Internet Time Access Control Update Software Reboot	Fourth NTP time server: Fourth NTP time server: Fifth NTP time server: Time	None None None	Tiiuana	• • • • • • • •			
	offset:	ienie rinie,	Save/Apply				

NOTE: Internet Time must be activated to use. See 5.5 Parental Control. The internet time feature will not operate when the router is in bridged mode, since the router would not be able to connect to the NTP timeserver.