ZyXEL

Firmware Release Note

Prestige 314 Standard Version

Release 3.50(CA.3)C0

Date: Jun 10, 2003
Author: Gilbert Cheng

ZyXEL Prestige 314
Version 3.50(CA.3)C0
Release Note

Date: Jun 10, 2003

Supported Platforms:

ZyXEL Prestige 314

Versions:

ZyNOS Version : V3.50(CA.3) | 06/10/2003 15:01:34
Bootbase Version : V2.10 | 03/22/2002 14:38:58

Notes:

1. After uploading firmware in “FIRMWARE UPLOAD” Web page fails, please reboot the P314 first and retry upload firmware again. Because sometimes the system memory is not large enough to hold the uploading firmware.
2. Uploading the firmware from V3.25 to V3.50 through FTP or Console is suggested.

Features:

Modification in V3.50(CA.3)C0 | 06/10/2003

1. [BUG FIX]
   Symptom & Condition: Can't play XBox Live via Prestige 314.
2. [BUG FIX]
   Symptom & Condition: WAN connection will drop in case of using PPTP for ADSL modem (Alcatel ANT1000, Alcatel SpeedTouch Home and Thomson SpeedTouch 510), especially if there is "high speed" on ADSL (512/256).

Modification in V3.50(CA.2)C0 | 03/24/2003

1. [BUG FIX]
   Symptom: The system will allow the packet with DF=1 and packet length > MTU to pass through the router without any error message returned to the sender.
   Condition: When the packet with it's length > MTU and don't fragment big is set, the packet is allowed to pass through the router.
2. [BUG FIX]
   Symptom: Ping outside will get a high latency response time when using SUA mode.
   Condition: When the LAN PC pings outside, the response time is very high if the router using SUA mode.
3. [BUG FIX]
   [Symptom & Condition] XBox Live can't work through router.
4. [BUG FIX]
   Symptom: Configure the Remote Management MISC web page “Stealth mode” check box cannot work correctly.
   Condition: When the user configures the “Stealth mode” check box in the Remote Management MISC web page, the P314 cannot save the configuration correctly.
5. [BUG FIX]
   Symptom: Cannot save DDNS setting from eWC.
   Condition: In the DDNS web page, configure the DDNS related setting; actually P314 will not update the DDNS runtime data immediately. Use CI command " sys ddns disp" to view.

6. [BUG FIX]
Symptom: Web inept wording.
Condition: The Remote Management MISC web page have inept wording related with ZyWALL in the help page.
7. [BUG FIX]
Symptom: NAT default server does not active from web page setting.
Condition: When the user configure “Default Server” IP address in the In the SUA/NAT Port Forwarding web page, the P314 will not enable the active of the default server entry. (Issue CI command " ip nat server disp" to check), and this configuration will change the “ICMP respond to ping” from "LAN & WAN" to be "LAN" in the Remote management MISC web page.
8. [FEATURE CHANGE]
Remove the “Trusted Host” field in the Remote Management SNMP page. Users still can configure the trust host of the SNMP by the “Secured Client IP Address” field in the same page.
9. [FEATURE CHANGE]
Remove the unneeded filter setting, which is called “TEL_FTP_WEB_WAN” in the SMT Menu 21.3
10. [FEATURE CHANGE]
Remove unneeded call filter set in the Menu 11.5
11. [BUG FIX]
Symptom: NAT problem with DF flag packets.
Condition: When packets incoming on the WAN side with DF and MF bits sets are not working.
12. [NEW FEATURE]
Add “sys rn mtu” CI command to change MTU value.
13. [FEATURE CHANGE]
Add “NetBIOS_WAN”, “NetBIOS_LAN”, “Arp-Broadcast”, and “SNMPTRAP_RIP” filter set in SMT menu 21 but not enable by default. The user can apply these filter sets by himself.
14. [FEATURE CHANGE]
Add “Microsoft-DS” filter set in SMT menu 21 but not enable by default. The user can apply these filter sets by himself.
15. [BUG FIX]
[Symptom & Condition] When the IPSec packets pass through the P314, the NAT table of the P314 record 2 session of the UDP port 500 instead of one.

Modification in V3.50(CA.1)c0 | 10/17/2002
1.[ENHANCEMENT] Add protection mechanism to prevent from wrong firmware model uploaded..

Modification in V3.50(CA.0) | 09/09/2002
1.[FEATURE CHANGE] Add SNMP and DNS remote management control in SMT24.11. Please refer Appendix 1.
2.[NEW FEATURE] Add Trigger Port support. For more information, please refer Appendix 2.
3.[ENHANCEMENT] Add two CI commands : "ppp lcp echo time" and "ppp lcp echo retry" to control echo timer and retry counts. Set one of them to 0 will disable echo request
4.[ENHANCEMENT] Add “ip nat timeout” to setup NAT timeout value.
5.[NEW FEATURE] Add a new CI command to Increase IKE source port. This CI command is used to switch CISIC/Nortel.
ip nat incikeport <on|off>
Note: Only for some CISIO servers, you need to turn on this CI command.
6.[ENHANCEMENT] Add 3rd DNS and WINS server for DHCP server option.
ip dhcp <iface name> server <dns server>
ip dhcp <iface name> server <wins server> to add server IP.
7.[ENHANCEMENT] Add a CI command to control NAT IRC service turned on/off.
ip nat service irc <on|off> to control the service.
8.[ENHANCEMENT] Add C/I commands to support the remote node option setting feature:
sys rn load <entry no.> , load instruction
sys rn disp <entry no.> , display instruction (0:working buffer)
sys rn nat <none|sua|full_feature> , NAT setting instruction.
sys rn nailup <no|yes> , Enable/Disable NAIL-UP feature.

sys rn save <entry no.> , save instruction.

9. [NEW FEATURE] Add Traffic Redirect. (Appendix 3)
10.[NEW FEATURE] New CI command for NetBIOS filter. Please refer to Appendix 4
Note: Remove the related NetBIOS filter set in SMT menu 3.1, 11.5, and 21.
11. [ENHANCEMENT] Suppore Custom, Static DDNS type.
12. [ENHANCEMENT] Add SNMP linkup and linkdown trap of enet0, enet1, poe0, pns0 channel
13.[BUG FIXED]
Sympton:NAT loopback server problem.
Condition:When a server in the LAN site and there exists a NAT server set directed to it, WAN site traffic can access the WAN IP, then be redirected to the server. But the LAN site cannot use the WAN IP to access the server. It only can access the server through LAN IP. A new CI command "`ip nat loopback`" is added to turn on the feature, "NAT server loopback". When it turns on, PC on LAN site can access the LAN site server through WAN IP. NOTE: Turn on the feature will cause throughput decreased.
14. [BUG FIXED]
Sympton:PPPOE client cannot dial successfully any more when the router try to dail for a long time.
Condition:PPPOE client (NAIL-UP feature enable)cannot re-connect any more if previous disconnection time took too long.
15. [BUG FIXED]
Symptom:The IP address which is boundel in SNMP Trap sometimes is not correct.
Condition:When the PC receive the router's trap, the user will find that the IP address of the trap is always the router's LAN ip address, no matter this trcp packet is issue from the router's WAN or LAN.It should be with related interface's IP address, not always LAN's IP.
16.[BUG FIX]
Sympton: SMT menu 24.2.1 will not show correct system name
Condition: Once user configure the system and domain name in SMT menu 1, SMT menu 24.1 will show the string which join system name and domain, but SMT menu 24.2.1 just display the system name.
17.[BUG FIX]
Sympton: Configure the email field of the DDNS web page will cause system reboot.
Condition:When the user configures the DDNS email field with too long string(this is an illegal string), the system will reboot.
18.[BUG FIX]
Symptom: The SUA/ NAT web page can not save the user port frowarding configuration.
Condition: When the user configures the P314 port forwarding in SUA/NAT web page, the P314 will not store the user configuration after the user click "Apply" button.
19.[BUG FIX]
Symptom: mIRC "DCC SEND file" function can't work.
Condition: Behind NAT router, when user tries to send a file by using mIRC DCC SEND function, The file transfer will not only succeed, but also will cause disconnection from mIRC server.
20[FEATURE CHANGE] Default ROM file. Remove the "SNMP_WAN" filter set from SMT menu 11.5 and SMT menu 21
21.[BUG FIX]
Symptom: The user cannot connect the embedded server of the router any more.
Condition: When the router receives the TCP packets with both SYN and ACK bits set, the corresponding remote management service is no longer available.
22[BUG FIX]
Symptom: The embedded DHCP client of the prestige may be not get a WAN IP address from the DHCP server..
Condition:The prestige request a WAN IP address just once. When the DHCP server is in busy state, the prestige may not be get a assigned WAN IP address.
23.[BUG FIXED] Fix DNS server IP address runtime value will be cleaned.
24.[BUG FIX] Fragment packet with DF can't pass the NAT issue.
25.[BUG FIXED] Bug fix for multi-IPSEC Pass through problem
26.[BUG FIXED] IP ALias cannot fake MAC address in SMT2 and WEB

Appendix 1 Remote Management Enhancement (Add SNMP & DNS Control)

1. New function

1. You can change the server port, except DNS server.
2. You can set the security IP address for each type of server.
3. You can define the rule for server access. (WAN only/LAN only, None, ALL).
4. The port of the DNS server is read only.
5. The default server access of the servers are LAN only.

2. Modification

1. We **removed** the default TEL_FTP_WEB filter in Menu 11.5.
2. The default value for Server access rule are **LAN only**.
3. Under the default setting: You can setup the Menu 15 to forwarding the server to LAN IP address. Thus you can configure the router through the WAN and you don't need to modify the server management or filter.

```
4.     Menu 24.11 - Remote Management Control

 TELNET Server:     Port = 23         Access = LAN only
                       Secured Client IP = 0.0.0.0

 FTP Server:         Port = 21         Access = LAN only
                       Secured Client IP = 0.0.0.0

 Web Server:         Port = 80         Access = LAN only
                       Secured Client IP = 0.0.0.0

 SNMP server:        Port = 161        Access = LAN only
                       Secured Client IP = 0.0.0.0

 DNS server:         Port = 53         Access = LAN only
                       Secured Client IP = 0.0.0.0


                    Press ENTER to Confirm or ESC to Cancel:
```

4. CI Commands

1. sys server load : *load the remote management stored data*.
2. sys server access <telnet|ftp|web|icmp|snmp|dns> < 0: ALL, 1: None, 2:LAN only, 3:WAN only>
   Ex: sys server access telnet 2 -> User can't telnet into the router via WAN, only LAN is permitted.
3. sys server secureip <telnet|ftp|web|icmp|snmp|dns><IP address> : setup serure IP.
   Ex: sys server secureip ftp 1.1.1.1
4. sys server port <telnet|ftp|web|icmp|snmp|dns><port number> : setup port number
   Ex: sys server port ftp 550
5. sys server save : save the configuration

Appendix 2 Trigger Port

Introduction

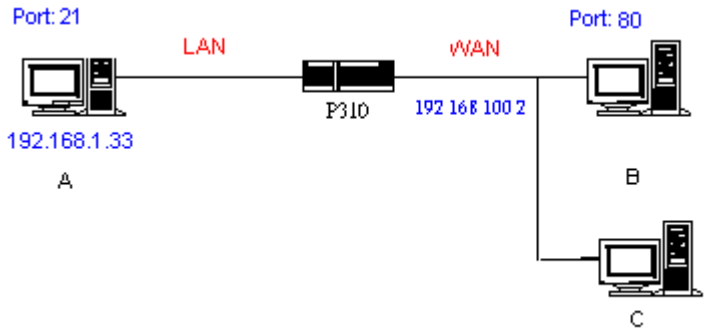
Some routers try to get around this "one port per customer" limitation by using "triggered" maps. Triggered maps work by having the router watch ***outgoing*** data for a specific port number and protocol. When the router finds a match, it remembers the IP address of the computer that sent the matching data. When the requested data wants to come back ***in*** through the firewall, the router uses the port mapping rules that are linked to the trigger, and the IP address of the computer that "pulled" the trigger, to get the data back to the proper computer.

How to use it

Following table is a configuration table.

Name	Incoming	Trigger
Napster	**6699**	**6699**
Quicktime 4 Client	**6970-32000**	**554**
Real Audio	**6970-7170**	**7070**
User	**1001-1100**	**1-100**

How it works



For example, you are running a FTP Server on port 21 of machine A. And you may want this server accessible from the Internet without enabling NAT-based firewall. There are one Web Server on port 80 of machine B and another client C on the Internet.

(1) As Prestige receives a packet from a local client A destined for the outside Internet machine B, it will check the destination port in the TCP/UDP header to see if it matches the setting in "Trigger Port" (80). If it matches, Prestige records the source IP of A (192.168.1.33) in its internal table.

(2) Now client C (or client B) tries to access the FTP server in machine A. When Prestige to forward any un-requested traffic generated from Internet, it will first check the rules in port forwarding set. When no matches are found, it will then check the "Incoming Port". If it matches, Prestige will forward the packet to the recorded IP address in the internal table for this port. (This behavior is the same as we did for port forwarding.)

(3) The recorded IP in the internal table will be cleared if machine A disconnect from the sessions that matches the "Trigger Port".

Notes

(1) Trigger events can't happen on data coming from ***outside*** the firewall because the NAT router's sharing function doesn't work in that direction.

(2) Only one computer can use a port or port range at a time on a given real (ISP assigned) IP address.

Appendix 3 Traffic Redirect

1. Introduction

These features is used to keep Internet connectivity of the P314. The Connectivity Monitor is running at interval to detect if the P314 can reach a desired host/address or the adjacent upstream gateway. Once the P314 has detected the connectivity is broken, it tries to forward the traffic to another gateway that user has specified.

2. Menu 11.6 - Traffic Redirect Setup

```
      Menu 11.1 - Remote Node Profile

Rem Node Name= Normal_route   Route= IP
Active= Yes

Encapsulation= Ethernet        Edit IP= No
Service Type= Standard         Session Options:
Service Name= N/A               Edit Filter Sets= No
Outgoing:
  My Login= N/A                  Edit Traffic Redirect= YES
  My Password= N/A
  Server IP= N/A

    Press ENTER to Confirm or ESC to Cancel:
```

```
    Menu 11.6 - Traffic Redirect Setup

         Active= No
         Configuration:
           Backup Gateway IP Address= 0.0.0.0
           Metric= 2
           Check WAN IP Address= 0.0.0.0
             Fail Tolerance= 0
             Period(sec)= 0
             Timeout(sec)= 0

    Press ENTER to Confirm or ESC to Cancel:
```

(1) Configure "Active" to "YES" if you want this feature work.
(2) "Backup Gateway". When the primary ISP or the check point is unreachable, traffic will be handed over to this backup gateway. [In IP address format]
(3) "Metric". Please reference section "**Metric**"
(4) "Check WAN IP Address". The Connectivity Monitor will probe the connectivity to a check-point. In general case, this check-point is the adjacent upstream gateway, which is typically assigned by ISP. However, if user desires to check a more significant point on the Internet, it can be specified here. A special case should be noticed that, even the ISP is online, this check-point maybe not reachable. The hand-over mechanism will function when the check-point failed. Leave it to 0.0.0.0, and the P314 will take the upstream gateway as the default check-point.
(5) "Fail Tolerance" is the check failure upper limit. For example, if this value is 2. When P314 failed to reach the check-point at the 3rd try, Connectivity Monitor will invalidate the corresponding route and promote candidate to be the default route.
(6) "Period". The Connectivity Monitor will examine physical link signal and then probe the check-point at a interval of "period" seconds.
(7) "Timeout". The check-point is expected to response P314's probe within a reasonable time. After that, P314 will log a failure. When the fail tolerance is exceeded, traffic will be handed over to the candidate route.

The probing mechanism employs ICMP echo request/reply. Some hosts or routers on Internet may discard such packets.

3. Metric

Once the traffic redirect and dial-backup mechanism were activated, P314 will have 3 default routes to Internet. The first one is the normal route that designated by ISP or the static route mechanism; the second one is the traffic-redirect route (i.e. the backup gateway); the third one is the dial-backup route.

Customable metrics are provided in the menu 11.6 (Traffic Redirect) and menu 11.3 (Dial-backup) to determine the priority of the 3 default routes. For example, if the normal route has a metric "1" and traffic-redirect route has a metric "2" and dial-backup route has a metric "3", then the normal route is the first priority candidate to be the primary default route. If the normal route failed to get on Internet, the traffic-redirect route will be the successor. By the same theorem, dial-backup route is the successor after traffic-redirect route failed. For any two of the default routes match the same metric, a pre-defined priority is taken:

Normal route > Traffic-redirect route

For another example, if user want P314 to use dial-backup route prior than traffic-redirect route or even the normal route, all need to do is to make metric of dial-backup route to be "1" and the others to be equal to "2" (or greater).

4. C/I commands

A set of C/I commands are provided.

(1) "ip tredir active [on/off]" to enable/disable traffic redirect.
(2) "ip tredir partner" IP address of the backup gateway.
(3) "ip tredir target" IP address of the check target.
(4) "ip tredir failcount" to setup fail tolerance.
(5) "ip tredir checktime" to setup checking period.
(6) "ip tredir timeout" to setup check timeout.
(7) "ip tredir disp" to show system value and run time value.
(8) "ip tredir save" will save the configuration.

5.Note

(1) Turn off "RIP" in SMT3.2 is recommended.
(2) When traffic redirect is turned on, and encapsulation type is PPPOE or PPTP, "Nail-UP" function in SMT11.1 will be enabled
(3) A useful WINDOWS commands "tracert" can be used to verify the packet routing.
(4) Connectivity Monitor can not be disabled. However, traffic redirect and dial-backup mechanism can be enabled/disabled independently.

Appendix 4 Hard-coded packet filter for "NetBIOS over TCP/IP" (NBT)

The new set C/I commands is under "sys filter netbios" sub-command.

There are two CI commands:
(1) "sys filter netbios disp": It will display the current filter mode.

Example ouput:
```
================ NetBIOS Filter Status ================
      LAN to WAN:       Forward
      WAN to LAN:       Forward
      IPSec Packets:    Forward
      Trigger Dial:     Disabled
```

(2) "sys filter netbios config <type> {on|off}": To configure the filter mode for each type.
Current filter types and their description are:

Type	Description	Default mode
0	LAN to WAN	Forward
1	WAN to LAN	Forward
6	IPSec pass through	Forward
7	Trigger dial	Disabled

Example commands:
sys filter netbios config 0 on => block LAN to WAN NBT packets
sys filter netbios config 1 off => pass LAN to DMZ NBT packets
sys filter netbios config 6 on => block IPSec NBT packets
sys filter netbios config 7 off => disable trigger dail

(3) Type 6 (IPSec pass through) filter has precedence over type 0 (LAN to WAN)

Appendix 5 SUA Support Table

The required settings of Menu 15 for some applications are listed in the following table.

SUA Support Table

Traffic Type	Application Version	Required Settings in Menu 15 Port/IP	
		Outgoing Connection	Incoming Connection
HTTP	Netscape, IE	None	80/client IP
FTP	Windows FTP, Cuteftp	None	21/client IP
TELNET	Windows Telnet, Neterm	None	23/client IP (and remove Telnet filter in WAN port)
POP3	Eudora	None	110/clinet IP
SMTP	Eudora	None	25/client IP
IRC	mIRC,Microsoft Chat	None for Chat. DCC support: MIRC < 5.31	None
PPTP	Windows PPTP	None	1723/client IP
ICQ	ICQ 99a	None for Chat. For file transfer, we must enable ICQ-preference-connections-firewall and set the firewall time out to 80 seconds in firewall setting.	Default/client IP
Cu-SeeMe	Cornell 1.1	None	7648/client IP
	White Pine 3.1.2	7648/client IP & 24032/client IP	Default/client IP
	White Pine 4.0 (CuSeeMe Pro)	7648/client IP & 24032/client IP	Default/client IP
NetMeeting	Microsoft NetMeeting 2.1 & 2.11	None	1720/client IP 1503/client IP
Cisco IP/TV	Cisco IP/TV 2.0.0	Default/client IP	
RealPlayer	RealPlayer G2	None	
VDOLive		None	
Quake	Quake1.06	None	Default/client IP
QuakeII	QuakeII2.30	None	Default/client IP
QuakeIII	QuakeIII1.05beta	None	
StartCraft		6112/client IP	
Quick Time	Quick Time 4.0	None	
IPSEC (ESP)		None (only one client)	Default
MSNP	Microsoft Messenger service V3.0	6901/client IP	6901/client IP

Annex A CI Command List

Command Class List Table		
System Related Command	Exit Command	IP Related Command
Ethernet Related Command		

System Related Command

Home

Command				Description
sys				
	adjtime			retrive date and time from Internet
	callhist			
		display		display call history
		remove	<index>	remove entry from call history
	countrycode		[countrycode]	set country code
	date		[year month date]	set/display date
	domainname			display domain name
	edit		<filename>	edit a text file
	extraphnum			maintain extra phone numbers for outcalls
		add	<set 1-3> <1st phone num> [2nd phone num]	add extra phone numbers
		display		display extra phone numbers
		node	<num>	set all extend phone number to remote node <num>
		remove	<set 1-3>	remove extra phone numbers
		reset		reset flag and mask
	feature			display feature bit
	hostname		[hostname]	display system hostname
	log			
		clear		clear log error
		disp		display log error
		online	[on|off]	turn on/off error log online display
	rn			
		load	<entry no.>	load remote node information
		disp	<entry no.>(0:working buffer)	display remote node information
		nat	<none|sua|full_feature>	config remote node nat
		nailup	<no|yes>	config remote node nailup
		save	[entry no.]	save remote node information
	stdio		[second]	change terminal timeout value
	support			not support in this product
	time		[hour [min [sec]]]	display/set system time
	trcdisp	parse, brief, disp		monitor packets
	trclog			
	trcpacket			
	syslog			
		server	[destIP]	set syslog server IP address
		facility	<FacilityNo>	set syslog facility
		type	[type]	set/display syslog type flag
		mode	[on|off]	set syslog mode
	version			display RAS code and driver version
	view		<filename>	view a text file
	wdog			
		switch	[on|off]	set on/off wdog

		cnt	[value]	display watchdog counts value: 0-34463
	socket			display system socket information
	filter			
		netbios		
	roadrunner			
		debug	<level>	enable/disable roadrunner service 0: diable <default> 1: enable
		display	<iface name>	display roadrunner information iface-name: enif0, wanif0
		restart	<iface name>	restart roadrunner
	ddns			
		debug	<level>	enable/disable ddns service
		display	<iface name>	display ddns information
		restart	<iface name>	restart ddns
		logout	<iface name>	logout ddns
	cpu			
		display		display CPU utilization

Exit Command

Home

Command				Description
exit				exit smt menu

Ethernet Related Command

Home

Command				Description
ether				
	config			display LAN configuration information
	driver			
		cnt		
			disp <name>	display ether driver counters
		ioctl	<ch_name>	Useless in this stage.
		status	<ch_name>	see LAN status
	version			see ethernet device type

IP Related Command

Home

Command				Description
ip				
	address		[addr]	display host ip address
	alias		<iface>	alias iface
	aliasdis		<0|1>	disable alias
	arp			
		status	<iface>	display ip arp status
	dhcp		<iface>	
		client		
			release	release DHCP client IP
			renew	renew DHCP client IP
		status	[option]	show dhcp status

	dns			
		query		
		stats		
	httpd			
	icmp			
		status		display icmp statistic counter
		discovery	<iface> [on|off]	set icmp router discovery flag
	ifconfig		[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	configure network interface
	ping		<hostid>	ping remote host
	route			
		status	[if]	display routing table
		add	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add route
		addiface	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add an entry to the routing table to iface
		addprivate	<dest_addr|default>[/<bits>] <gateway> [<metric>]	add private route
		drop	<host addr> [/<bits>]	drop a route
	status			display ip statistic counters
	udp			
		status		display udp status
	rip			
	tcp			
		status	[tcb] [<interval>]	display TCP statistic counters
	tftp			
	xparent			
		join	<iface1> [<iface2>]	join iface2 to iface1 group
		break	<iface>	break iface to leave ipxparent group
	anitprobe		<0|1> 1:yes 0:no	set ip anti-probe flag
	tredir			
		failcount	<count>	set tredir failcount
		partner	<ipaddr>	set tredir partner
		target	<ipaddr>	set tredir target
		timeout	<timeout>	set tredir timeout
		checktime	<period>	set tredir checktime
		active	<on|off>	set tredir active
		save		save tredir information
		disp		display tredir information
		debug	<value>	set tredir debug value
	igmp			
		debug	[level]	set igmp debug level
		forwardall	[on|off]	turn on/off igmp forward to all interfaces flag
		querier	[on|off]	turn on/off igmp stop query flag
		iface		
			<iface> grouptm <timeout>	set igmp group timeout
			<iface> interval <interval>	set igmp query interval
			<iface> join <group>	join a group on iface
			<iface> leave <group>	leave a group on iface
			<iface> query	send query on iface
			<iface> rsptime [time]	set igmp response time
			<iface> start	turn on of igmp on iface
			<iface> stop	turn off of igmp on iface
			<iface> ttl <threshold>	set ttl threshold

			<iface> v1compat [on|off]	turn on/off v1compat on iface
		robustness	<num>	set igmp robustness variable
		status		dump igmp status