ZyXEL Prestige 310-S
V3.25(M.00)
For Standard Release Note

Date: July 12 2001

Supported Platforms:

ZyXEL Prestige 310-S, Prestige 310, Prestige 314

Versions:

RAS F/W Version : V3.25(M.01) | 7/25/2001

Notes:

1. Telnet , FTP and Web incoming from the WAN port is disabled in default configuration romfile. This can be change in SMT Menu 24.11.
2. If you use NetMeeting application behind SUA to connect to an outside user the outside user will see two identical users in screen.
3. We need to register MIRC to make the DCC work at version 5.31. So far, we don't support MIRC DCC after version 5.31.
4. If you can not get an IP address from your ISP. Please do the following.
   ** Your ISP will check your PC's hostname.
   ➔ Please set your PC's computer name to Prestige in Menu 1. (Appendix 2)
   ** Your ISP will check the MAC address.
   ➔ Please inform your ISP that you have bought a new network device.
   Or Use Menu 2 to clone the PC's MAC address to WAN. (Append ix 2)
   ** Your ISP only allows one MAC to connect to Internet.
   ➔ Please power down your cable modem and let router's WAN port connects to cable modem directly.
   ** Your ISP needs a special login program.
   ➔ We support the Times Warner Road Runner login program. Please select the correct service type in Menu 4. We support two kinds of RoadRunner login method. The first one is the Toshiba authentication method and the other one is RoadRunner Manager authentication method. Please make sure which login method you are using.
5. This version support Web configuration.
   Username: Admin
   Password: <your telnet password> (default: 1234)

Features:

Modification in V3.25(M.01) 7/25/2001
1. Bug: Modify the help message.

Modification in V3.25(M.00) 7/12/2001
1. Modify the Web page and help.
2. Bug: SMT24.4 select 1 ping and press left-arrow twice will crash. Fixed.
3. Modify the SNMP counter to add the FCS in Ethernet channel.
4. Bug: SNMP counter count the wrong information.

5. Modify SNMP ifOperStat to show the state down when the channel state is idle.
6. Add default filter to filter the SNMP.
7. Bug: SNMP V2.0 packet will crash. Fixed.
8. Change antiprobe default value to 1 to enable the Anti-Probe.
9. Add new CPU type support. (S3C4510B)
10. Add protection for old ODM hardware. (only zyxel hardware can download zyxel firmware).
11. Added Full Web configuration support.
12. Added Range port forwarding support.
13. Added SMT24_11 Remote Server management. (see appendix 19)
14. Added NAT NetBIOS over TCP support.
15. Added WAN TCP MSS adjustment setting support. "ip adjmss <value>"
16. Added Telnet Terminal type support.
17. Added "ip arp reply [<0|1>]" to disable the router to send the ARP reply for none interface ip address.
18. Added the default NTP time server support. If you set the wrong time server then we will try to find one.
19. Added Restore factor default romfile support in Web.
20. Added Multi-NAT support.

Modification in V3.23(M.01) 3/29/2001
1. Added Anti-Probe support. ("ip antiprobe <0|1>" 0: disable 1:enable (default)for Netgear)
2. Bug: Can not remove Domain Name in Web Configuration.
3. Bug: Can not set Roandrunner username password in Web configuraion.
4. Bug: Web configuraion PPTP will not work until reboot.
5. Added ICQ Phone support.
6. Added Net2phone support.
7. Remove www.ddns.org support.
8. Added 3COM PPPoE support. ("poe ether [3com|rfc]").
9. Added new flash type support. (28F800C3B).
10. Bug: NAT TCP checksum fail problem.
11. Bug: Encapsulation PPPoE dial out device filter can not work problem.
12. Added Daylight saving support.
13. Modify Time server IP address field to support Domain Name.
14. Bug: ICMP source quench will close connection. Fixed. It will solve the Half Life game problem.
15. Added display for DHCP client host name. "ip dhcp enif0 st".

Modification in V3.23(M.00) 11/24/2000
1. Bug: It will cause systrem crash when run the ViaVideo application.

Modification in V3.23(M.00)b3 10/19/2000
1. Bug: TFTP upload firmware will cause system crash. Fixed.
2. Add new sua spport. (MSNP)
3. Arp entry ==> arp entries
4. smt21.x.1 ICMP=1, TCP = 6.. => ICMP=1, IGMP = 2. add IGMP = 2 hint.
5. Bug: m11 dis-active remote cause m4 can not enter. Fixed.

Modification in V3.23(M.00)b2 9/21/2000
1. Bug: The wrong version number.
2. Added New Intel flash support.

Modification in V3.23(M.00)b1 9/20/2000
First release.

Appendix:

1.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

2. DHCP Problems.

The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. We implement the DHCP server in the LAN port to manager the local LAN IP address and the DHCP client in the WAN port to acquire the configuration from the ISP. There are many configuration information carried by DHCP option. We will process the following information coming for the ISP: IP address, Gateway, Network Mask, Domain Name, Domain Name Server and Lease Time of DHCP client.

The traditional dial up networking will provide the user name and password for the ISP to manage the client by using the PPP. The DHCP doesn't provide this kind of mechanism. However, the ISP still can authorize the client by using the following method.

a. The ISP can check client PC's MAC address.

When you install the Cable/xDSL service, the ISP will record the MAC address of your NIC card. Thus, any unrecorded MAC address will be silently discarded. We can solve this problem by one of the following methods.

- Tell you ISP that you have bought a new NIC card and you want to change the MAC address.
- Clone the PC's MAC address to the WAN site. You can connect your network like the following.

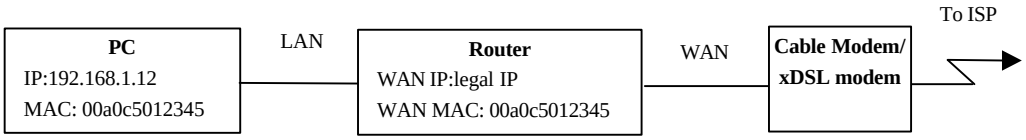


Figure 1 Clone MAC Address

Configure the SMT Menu 2 as following.

```
Menu 2 - WAN Setup

MAC Address:
  Assigned By= IP address attached on LAN
  IP Address= 192.168.1.12
```

If you configure correctly then it will clone the PC's MAC address to the WAN port. This MAC address will be saved in the configuration file and will not be lost unless you reconfigure the Menu 2 or unload a configuration file.

b. The ISP can check hostname options in the DHCP option. When you install the Cable/xDSL service, the ISP will record your PC computer name or assign a new computer name to your PC. The Windows DHCP client will send the PC's computer name to DHCP server. Any unrecorded hostname option will be silently discarded.

We can solve this problem by setting the PC's computer name to router's system name in Menu 1.

3. Domain name support.

The Prestige is enhanced to provide the domain suffix to its DHCP clients. The domain suffix may be provided by the ISP via the DHCP or statically configured by the user. If it is provided by the ISP, the Prestige assigns it to the clients via the DHCP over LAN. Otherwise, we can enter the domain suffix in menu 1 directly if we know the domain suffix already. In case the domain suffix is set in menu 1 and the ISP also provides one using DHCP, the Prestige will take the settings in menu 1 to assign to the client. You can go to SMT Menu 24.8 by typing "sys domainname" to see the current domain name using by the router.

```
Menu 1 - General Setup

System Name= P310      ← Your PC's computer name.
Domain Name=zyxel.com.tw ← Your domain name
```

Before this feature is available, one has to enable DNS in the network settings of every client and list xx.yy.zz.com as a default domain suffix. Now, with this new feature, whenever you use mail or news or

even www, your PC will add the default domain suffix after these and route you properly to the ISP intranet addresses.

4. ICQ problems.

What is ICQ?

ICQ stands for 'I seek you'. It's originally developed by Mirabils, an Israeli software company. Then it's bought by America On-Line. ICQ is an Internet messaging tool. You can use ICQ to send messages to your friends, and see if he/she is online. Every ICQ user has one ID called UIN in ICQ. It's an identifier for ICQ.

How ICQ works?

When you launch ICQ, it will try to logon a server which is operated by AOL by the UIN. After the logon is completed, ICQ will try to ask server if any selected UIN is logon too. This process is done periodically, so you will know your friend is online when he launch his ICQ client. To ensure the link, ICQ will send a keep-alive packet periodically to inform the server the user is still here, and send current status if there is anything changed. The default time of keep-alive packet is 120 seconds. And all client/server communication are through UDP port 4000. Whenever a user-to-user communication is requested, there is a TCP session established. The port is negotiated by the client/server session.

How to make ICQ work with SUA?

As described above, ICQ will communicate with server with port 4000 and send keep-alive packets to inform server it's online. The keep-alive packet is sent every 120 seconds. The default SUA UDP session timeout in Prestige is 90 seconds. It will cause problem because the keep-alive will be sent to different port translation due to session timeout. To fix it, you need to specify your ICQ client to shorten its keep-alive timer. It's in the connection tab under firewall setting. Set the keep-alive timer to 80 seconds to ensure the session is not timeout in Prestige. Because the user-to-user communication is negotiated by the first connection, set the ICQ connection behind the firewall. It will inform ICQ to perform operation friendly with firewall such as SUA in Prestige.

I have done the above setting, but it doesn't work perfectly. Why?

As ICQ is a proprietary protocol, it's not published. As we know, there are many versions of ICQ protocols and some of them are encrypted during communication. With some experiment, we suspect the ICQ doesn't work reliably with different keep-alive timer other than default value. The new SUA will prolong the session timeout period to 180 seconds to cover the default time of ICQ. So the keep-alive timer is not necessary to be altered later. However, the connection is still set to behind firewall because we do not know how to alter the packet at this time. We will try our best to find out the protocol details in ICQ in the future. It's not easy job since the protocol is encrypted and may be changed in the future. We can not promise any firm date on that support.

5. Delete the Filter Set in the SMT Menu 21

Go the SMT Menu 21 and select the right filter set. Leave the Edit Comment field as a blank and you can delete the filter set.

6. PPP over Ethernet (PPPoE)

What is PPPoE?

Point-to-Point Protocol over Ethernet is an IETF Draft standard that specifies how to connect multiple hosts at a remote site through common customer premises equipment (CPE). It facilitates the interaction of a host with a broadband modem (xDSL, cable, wireless, etc.), to achieve access to the growing number of high-speed data networks, via a familiar "dial-up networking" user interface. PPPoE provides a major advantage for service providers by maximizing integration with - and minimizing disruption of - service providers' existing dial network infrastructures. PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.

PPPoE Protocol Overview.

- PPPoE has two distinct stages.

- Discovery State
- PPP Session State

- Discovery stage
  - ETHER_TYPE field in Ethernet frame is set to 0x8863.
  - Stateless client-server protocol
  - Required whenever a client wishes to establish a PPP connection.
  - The host can discover all Access Concentrators and then select one.
  - Use peer MAC address and PPPoE session ID to identify the unique PPPoE session.
  - Four steps of Discovery stage.
    - The host broadcasting an Initiation packet.
    - One or more Access Concentrators sending Offer packets.
    - The host sending a unicast Session Request packet.
    - The selected Access Concentrator sending a Confirmation packet.

- PPP Session stage.
  - PPP data is sent as in any other PPP encapsulation.
  - Maximum-Receive-Uint (MRU) must be less than 1492.
  - All Ethernet packets are unicast.
  - ETHER_TYPE field in Ethernet frame is set to 0x8864.

How can I make PPPoE work on router.

a. You must enter Service Name for PPPoE discover stage.(SMT Menu 4 or SMT Menu 11.1)
b. You must configure User Name and Password for PPP session stage.(SMT Menu 4 or SMT Menu 11.1)

7. Added FTP firmware uploading support.

We build in an FTP server in ROUTER. You can use FTP client to upload the RAS code or configuration file.

Requirement:

You must have FTP client and you must have the ability to connect to the ROUTER.
You must have the upgrade firmware - the RAS code or Configuration file.
You must rename the filename of RAS code to "ras" and configuration file to "rom-0".
Connect IP : The ROUTER's LAN IP from LAN or WAN IP from WAN.
Username : ROUTER
Password : <ROUTER Telenet Password>

Procedure:

Open your FTP client to connect to ROUTER. After you login to ROUTER, you will see two list files - the "rom-0" and "ras". You can upload and download the RAS code or configuration file.

notes:

The upload file should be the same filename in the ROUTER listing according to RAS code or configuration file. **The upload file is binary file.**

8. SMT modify

SMT Menu 2:

Remove Half/Full duplex setting in WAN port. It will always be in the half duplex mode.

Menu 2 - WAN Setup

MAC Address:
Assigned By= Factory default/IP address attached on LAN
IP Address= N/A /a.b.c.d

SMT Menu 4:

We add Encapsulation field to distinguish from Ethernet connection to PPPoE connection. The Edit Filter, RIP direction and RIP version are moved to SMT Menu 11.1 and SMT Menu 11.3. We will have different screen layout according to different Encapsulation.

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
Service Type= Standard
My Login= N/A
My Password= N/A
Login Server IP= N/A

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Single User Account= Yes

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= PPPoE
Service Type= N/A
My Login=ras@poellc
My Password= *********
Idle Timeout= 100 ← **Connection idle timeout fordialup service.**

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Single User Account= Yes

SMT Menu 11.1, SMT Menu 11.3, SMT Menu 11.5.:

The IP address setting is moved to SMT Menu 11.3. If you change the Encapsulation then we will request you to check the IP address setting in SMT Menu 11.3. It will also have different SMT menu layout according to different Encapsulation.

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe 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
My Password= N/A
Server IP= N/A

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Single User Account= Yes
Metric= N/A
Private= N/A
RIP Direction= None
Version= N/A

Menu 11.5 - Remote Node Filter

Input Filter Sets:
protocol filters=
device filters=
Output Filter Sets:
protocol filters= 1
device filters=

If the Encapsulation is set to PPPoE then we add the budget management.

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe Route= IP
Active= Yes

Encapsulation= PPPoE **Edit IP= No**
Service Type= Standard Telco Option:
Service Name= poellc **Allocated Budget(min)= 0**
Outgoing= **Period(hr)= 0**
My Login= ras@poellc
My Password= ********
Authen= CHAP/PAP
Session Options:
Edit Filter Sets= No
Idle Timeout(sec)= 100

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
Rem IP Addr: N/A
Rem Subnet Mask= N/A
My WAN Addr= 0.0.0.0

Single User Account= Yes
Metric= 1
Private= No
RIP Direction= None
Version= N/A

```
Multicast= IGMP-v2
```

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
    device filters=
Output Filter Sets:
  protocol filters= 1
    device filters=
Call Filter Sets:
  protocol filters=
    device filters=
```

9. Modified TELNET_FTP_WAN to TEL_FTP_WEB_WAN

We block the Telent, FTP and Web connection request from the WAN side.

```
Menu 21.3 - Filter Rules Summary

# A Type                Filter Rules                M m n
- - ---- ----------------------------------------------------------------------------------------- - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23          N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21          N D N
3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80          N D F
4 N
5 N
6 N
```

10. SMT Menu 24.9, SMT Menu 24.9.3, SMT Menu 24.9.4

We add SMT Menu 24.9.3 to monitor the budget and you can reset the budget in this menu. The call history are shown in the SMT Menu 24.9.4.The PPPoE service name are shown in the phone number field. In SMT Menu 24.9.3 you can press "1" to clear budget and press "0" to update screen.

```
Menu 24.9 - System Maintenance - Call Control

  1. Budget Management
  2. Call History
```

```
Menu 24.9.3 - Budget Management

  Remote Node   Connection Time/Total Budget   Elapsed Time/Total Period

 1.ChangeMe          0:06/1:00              0:06/24:00
```

```
Menu 24.9.4 - Call History

  Phone Number    Dir  Rate  #call     Max       Min       Total
 1. poellc        OUT     1      0:00:48   0:00:48   0:00:48
 2.
 3.
```

```
4.
5.
6.
7.
8.
9.
10.

        Enter Entry to Delete(0 to exit):
```

11. Enhance Unix Syslog feature.

We add the function to select the syslog type in SMT Menu 24.3.2.

Notes: You must do the following to enable filter log.

1. Enable Filter log in SMT 24.3.2.
2. Setting correct filter rule and enable log in SMT Menu 21.x.x.
3. Apply the filter log to correct interface.(SMT Menu 3.1 or SMT Menu 11.5).
4. You must have syslog server and the packets must match the log condition .

```
Menu 24.3.2 - System Maintenance - UNIX Syslog

Syslog:
Active= No
Syslog IP Address= 192.168.1.3
Log Facility= Local 1

Types:
CDR= No
Packet triggered= No
Filter log= YES
PPP log= No
```

12. IP Alias Support.

The IP Alias feature can let you use three logical LAN interfaces via its single physical Ethernet interface. The Prestige is the gateway for all the LAN networks. You can also route packets from one network to another. The IP alias feature allows your Prestige to have extra IP addresses that may be in completely different subnets than the first IP address. The ability to partition physical network into logical network over the same Ethernet interface is referred to as IP Alias functionality.

You can configuraion the IP Alias feature in the Menu 3.2.1 by selecting the Menu 3.2 **Edit IP Alias field** to **YES.**

```
Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP= Server
Configuration:
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 32
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0

TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
```

```
        Version= RIP-1
      Multicast= None
      Edit IP Alias= Yes
```

```
          Menu 3.2.1 - IP Alias Setup

    IP Alias 1= Yes
      IP Address= 192.168.2.1
      IP Subnet Mask= 255.255.255.0
      RIP Direction= None
        Version= RIP-1
      Incoming protocol filters=
      Outgoing protocol filters=
    IP Alias 2= Yes
      IP Address= 192.168.3.1
      IP Subnet Mask= 255.255.255.0
      RIP Direction= None
        Version= RIP-1
      Incoming protocol filters=
      Outgoing protocol filters=
```

Field	Description	Example
IP Alias	Choose **Yes** to configure the LAN network for the Prestige.	**Yes**
IP Address	Enter the IP address of your Prestige in dotted decimal notation	**192.168.2.1**
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige	**255.255.255.0**
RIP Direction	Press the space bar to select the RIP direction from **Both/In Only/Out Only.**	**Both**
Version	Press the space bar to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	**RIP-1**
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.	
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.	
When you have completed this menu, press [Enter] at the prompt [Press ENTER to Confirm …] to save your configuration, or press [Esc] at any time to cancel.		

13. IP multicast.

Traditionally, IP packets are transmitted in two ways - unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. Host groups are identified by class D IP addresses, i.e., those with "1110" as their higher-order bits. In dotted decimal notation, host group addresses range from 224.0.0.0 to 239.255.255.255. Among them, 224.0.0.1 is assigned to the permanent IP hosts group, and 224.0.0.2 is assigned to the multicast routers group.

IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC2236). IP hosts use IGMP to report their multicast group membership to any immediate-neighbor multicast routers so the multicast routers can decide if a multicast packet needs to be forwarded. At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige updates the information by periodic queries. The Prestige implementation of IGMP is also compatible with version 1. The multicast setting can be turned on or off on Ethernet and remote nodes.

```
          Menu 3.2 - TCP/IP and DHCP Ethernet Setup
```

```
DHCP= Server
Configuration:
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 32
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0

TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-1
  Multicast= None
```

```
Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Single User Account= Yes
Metric= N/A
Private= N/A
RIP Direction= None
  Version= N/A
Multicast= None
```

14. SNMP support.

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version two (SNMPv2).

Note: Keep in mind that SNMP is only available if TCP/IP is configured on your Prestige .

```
        Menu 22 - SNMP Configuration

SNMP:
  Get Community= public
  Set Community= public
  Trusted Host= 192.168.1.15
  Trap:
    Community= public
    Destination= 192.168.1.15
```

Field	Description	Option
Get Community	Enter the Get Community, which is the password for the incoming Get- and GetNext- requests from the management station.	Public

Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.	Public
Trusted Host	If you enter a trusted host, your Prestige 1600 will only respond to SNMP messages from this address. If you leave the field blank (default), your Prestige 1600 will respond to all SNMP messages it receives, regardless of source.	Blank
Trap: Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.	Public
Trap: Destination	Enter the IP address of the station to send your SNMP traps to.	Blank
Once you have completed filling in **Menu 22 - SNMP Configuration**, press [ENTER] at the message [Press ENTER to Confirm...] to save your configuration, or press [ESC] to cancel.		

15. PPTP support.

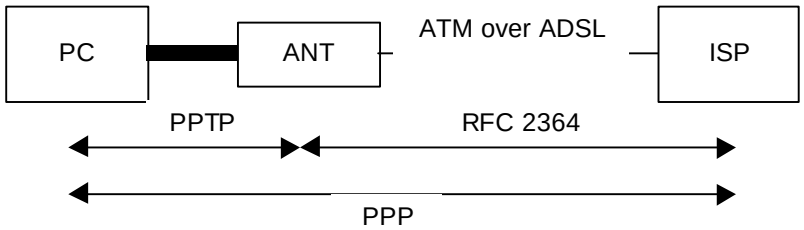
PPTP (Point-to-Point Tunneling Protocol) is a protocol to tunnel PPP frames over an IP substrate and thus is a layer 1 protocol in the OSI scheme of things. PPTP is a Microsoft's proprietary protocol; even though there is an RFC 2637 for PPTP, it's only informational. What Microsoft calls "VPN" is in essence tunneling through PPTP.

This implementation of PPTP is specifically for the French market where Alcatel's ANT (ADSL Network Termination) is deployed. Most, if not all, broadband modems (ADSL and cable modem) are equipped with Ethernet instead of RS-232 because RS-232 is too slow. It is therefore impossible to use them in the same way as the traditional analog modem and ISDN TA.. A mechanism is needed to transport the PPP frames from a PC to the broadband modem over Ethernet. Before PPPoE was formalized, Alcatel came up with the idea of building PPTP into their ANT for this purpose.

Instead of using the Internet to transport PPP frames anywhere in the world as originally envisioned, Alcatel's solution uses PPTP only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364). The PPP connection, however, is still between the PC and the ISP.

The drawback of this solution is that it requires one separate ATM VC per destination. It is understood that this is a temporary solution, because the industry is moving toward PPPoE that allows multiple PPP sessions over a single VC.

The various connections in this setup are depicted in the following diagram.



When the P-310 is deployed in such a setup, it must appear as a PC to the Alcatel modem. Therefore, our implementation will mimic a Windows workstation and not a full-blown PPTP stack.

```
                Menu 4 - Internet Access Setup

               ISP's Name= ChangeMe
               Encapsulation= PPTP
```

```
                  Service Type= N/A
                  My Login= username            <= select encapsulation
                  My Password= ********         <= username
                  Idle Timeout= 100       <= password

                IP Address Assignment= Dynamic
                  IP Address= N/A
                  IP Subnet Mask= N/A
                  Gateway IP Address= N/A
                  Single User Account= Yes

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

```
                    Menu 11.1 - Remote Node Profile

  Rem Node Name= ChangeMe              Route= IP
  Active= Yes

  Encapsulation= PPTP                  Edit IP= No
  Service Type= Standard               Telco Option:
  Service Name= N/A                      Allocated Budget(min)= 0
  Outgoing=                              Period(hr)= 0
    My Login= username                   Schedules=
    My Password= ********
    Authen= CHAP/PAP
                                       Session Options:
  PPTP:                                  Edit Filter Sets= No
    My IP Addr= 10.0.0.140               Idle Timeout(sec)= 100
    Server IP Addr= 10.0.0.138
    Connection ID/Name= N:MyISP


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

To configure a PPTP client, you must configure username & password for PPP connection and My IP Address & Server IP Address for PPTP connection. Where the connection ID/Name is optional. It will depend on your xDSL modem requirement.

16. Time and Date Setting

There is no Real Time Chip (RTC) chip in the Prestige, so we have a software mechanism to get the current time and date from an external server when you power up your Prestige. **Menu 24.10** does just that – it allows you to update the time and date settings of your Prestige.

```
Menu 24.10 - System Maintenance - Time and Date Setting


 Use Time Server when Bootup= Daytime (RFC-867)
 Time Server IP Address= 192.168.1.15

 Current Time:                15 : 54 : 09
 New Time (hh:mm:ss):         15 : 54 : 09

 Current Date:              2000 - 01 - 26
 New Date (yyyy-mm-dd):       2000 - 01 - 26
```

```
Time Zone= GMT
```

Field	Description
Use Time Server when Bootup=	Enter the time service protocol that your timeserver will send when the Prestige powers up. Choices are Daytime (RFC 867), Time (RFC-868), NTP (RFC-1305) and None. The main differences between them are the format, e.g., the Daytime (RFC 867) format is day/month/date/year/time zone of the server while the Time (RFC-868) format gives a 4-byte integer giving the total number of seconds since 1/1/1970 at 0:0:0. The NTP (RFC-1305) format is similar. Not all timeservers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. If you select None (this is the default value), you can enter the time manually but each time the system is booted, the time & date will be reset to: 1/1/1970 0:0:0
Time Server IP Address=	Enter the IP address of the your timeserver. Check with your ISP/network administrator if you are unsure of this information.
Current Time: New Time	Enter the new time in hour, minute and second format.
Current Date: New Date	Enter the new date in month, date and year format.
Time Zone= GMT+0800	Press the [SPACE BAR] to set the time difference between your time zone and Greenwich mean Time (GMT). Be aware how daylight savings time affects the time difference for your time zone.
Once you have filled in the new time and date, press [ENTER] to save the setting and press [ESC] to return to Menu 24.	

Note:

1. **If your Time Server is put on the internet that it will cause a trigger dial when the wan link is not on.**
2. **A Time Server may have 3 protocols installed, or only 1. Select anyone protocol that works.**
3. **If select Daytime protocol, you don't have to configure the field 'Time Zone', and Prestige will update the date, time, and time zone from Daytime server. But if select 'time' or 'NTP' protocol, you have to change the 'Time Zone' manually because Prestige will get GMT (Greenwish Mean Time) from the Time server or NTP server.**
4. **After you configure the time protocol and IP address of its server, Prestige will ask you "Do you wish to calibrate system clock with time server now[y/n]". You can choose 'y' to adjust the time immediately. If you select 'n', it doesn't mean Prestige will not update the time. He will do it a few time later.**

17. Call Schedule Support

Call scheduling feature schedules the Prestige to run the remote node automatically. This feature is just like the scheduler in a video recorder (record the program you want in a specified time). You can select 1 to 4 schedule set in **Menu 11 - Remote Node Setup**, and configure each schedule in **Menu 26 - Schedule Setup**.

```
                Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe          Route= IP
Active= Yes

Encapsulation= PPTP              Edit IP= No
Service Type= Standard           Telco Option:
Service Name= N/A                  Allocated Budget(min)= 0
```

```
Outgoing=                          Period(hr)= 0
  My Login= username               Schedules=1
  My Password= ********
                                   Session Options:
PPTP:                                Edit Filter Sets= No
  My IP Addr= 10.0.0.140             Idle Timeout(sec)= 100
  Server IP Addr= 10.0.0.138
  Connection ID/Name= N:MyISP


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

As we can have multiple sets, the sets have priority based on their position. For example, if we program the sets as 1,2,3,4 in remote node, then set 1 will override set 2,3,4. Set 2 will override set 3,4, and so on. This design is very similar to Filter & IP policy routing. You can design 12 sets for schedule and apply these schedule in remote node setting.
Note: If you want to delete a schedule set, choose the set number and leave the name empty.

To setup a schedule set select the schedule set you want to setup from **Menu 26** (no. 1-12) and press [Enter]. You will enter **Menu 26.1 - Schedule Set Setup** as shown next.

```
            Menu 26.1 Schedule Set Setup

      Active= Yes
      Start Date(yyyy-mm-dd)= 2000 - 01 - 26
      How Often= Once
      Once:
        Date(yyyy-mm-dd)= 2000 - 01 - 26
      Weekdays:
        Sunday= N/A
        Monday= N/A
        Tuesday= N/A
        Wednesday= N/A
        Thursday= N/A
        Friday= N/A
        Saturday= N/A
      Start Time(hh:mm)= 15 : 00
      Duration(hh:mm)= 00 : 30
      Action= Forced On
```

Field	Description
Active	If this field is set to **No** then the next set will be applied.
Start Date	Start date of this schedule rule. It can refute weekday setting. For example, if Start Date is 1999/10/15 (FRIDAY), Friday setting in weekday can be **No**. The Valid date value is from January 1, 1990 to February 5, 2036.
How Often	Now it can be set as **once** and **weekly**. Both these options are mutually exclusive. If **once** is selected, then all weekday settings will be marked as N/A. And when the schedule rule is completed, it will be deleted automatically.
Duration	Duration of the schedule set.
Action	You can choose **Forced On**, **Forced Down, Enable Dial-On-Demand**, or **Disable Dial-On-Demand.**
Forced On	During this period, the P310 will dial the remote node and persist for the time period specified in the field **Duration** .
Forced Down	During this period, the P310 will shut connection to the remote node. If the remote node is already connected, then it will be dropped.
Enable Dialing-on-deman	During this period, this remote node will accept dial on demand.

d	
Disable Dial-on-demand	During the period, this remote node will deny any demand dial. If a connection has been already established, it will not drop it. Once the connection is dropped manually or because of idle timeout period, then that remote node can't be triggered up until the end of the **Duration**.

18. Dynamic DNS support

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname, allowing the host to be more easy accessed from various location on the internet.

We support two DDNS client in our router – WWW.DDNS.ORG, WWW.DYNDNS.ORG.

How to configure it?

1. First, you must go to the WWW.DDNS.ORG or WWW.DYNDNS.ORG to register a account. After success registered you will receive a password from email. You can key in the hostname, email address, username, password..
2. Put the corresponding information to Menu 1.1.

Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DDNS.ORG
Active= Yes
Host= p310.ddns.org
EMAIL= yourmail@yourmailserver
User = p310
Password= ********
Enable Wildcard = YES/NO

Notes:

1. We only support the basic feature and login in with inscure password in WWW.DDNS.ORG.
2. We will update the IP address when we configure Menu 1, DHCP client renew, or ipcp open.
3. It will have problems if your wan ip address are private.
4. Please read the FAQ provided by the DDNS service provider. It will have great help to trouble shooting your problem.

19. Remote Server Management.

New function.

1. You can change the server port.
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).

Modification.

1. We will remove the default TEL_FTP_WEB filter in Menu 11.5.
2. The default value for Server access rule is 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.

20. Reference Home Page

http://www.zyxel.com/html/product/wan/p310.html