

# **ZyXEL Prestige P100 2.41(C.01)**

## **Release Note/Manual Supplement**

***Date: March 30, 2001***

This Release Note/Manual Supplement contains information about the features, and bug fixes.

### ***Supported Platforms***

---

V2.41(C.01) supports Prestige model: P100.

**\*Note:** Since the default configuration for ZyNOS 2.41 is not compatible with the one for the previous ZyNOS firmware, so if your P100 is upgraded from the previous ZyNOS versions, please also update the default configuration file for ZyNOS 2.41.

### ***New Features:***

---

#### **CLID callback support for dial-in users**

Dial-in user is capable for callback in Version 2.41.

#### **Outgoing data call bumping support**

Prestige will drop a channel in an MP bundle if there is a packet to other remote node.

#### **DHCP relay**

Prestige could be a middle role between DHCP server and DHCP client.

#### **More DHCP users**

The maximum IP address managed by DHCP server is 253.

#### **NetMeeting support for SUA/NAT**

NetMeeting is supported for both incoming and outgoing call.

#### **Minimum toll period support**

Prestige will try to use all the toll period at most with minimum toll period.

#### **Time and Date Setting**

Three time protocols Daytime (RFC-867), Time (RFC-868) and NTP (RFC-1305) are supported.

#### **Call Scheduling**

Prestige can allow the user to schedule a dial-up connection in specified time.

#### **NAT(Network Address Translation)**

Prestige supports four types NAT for IP packets: One to One, Many to One (current SUA), Many to Many Overload, and Many to Many No Overload.

#### **Others**

1. The ICMP discovery protocol is turned off by default ROM file, and if users want to turn on this protocol to let users' workstation (including PC) to recognize the P100 as one of default route, then users should follow the procedure below.

- Go to CI command mode (menu 24.8 or menu 24.4.22)
- sys edit autoexec.net
- Continue pressing n until finding the string as "ip icmp discovery enif0 off"

- Press d to delete.
- Press x to save. It will work at next boot up.
- 2. In order to make ICQ 99a to receive file behind SUA, you should do the following procedure.
  - open ICQ preference in ICQ icon.
  - open connections slot.
  - In "internet connect type" select "I am using a permanent internet connection(LAN)"
  - choose "I am behind a firewall or proxy"
  - enter firewall settings. Modify firewall time out to 80 seconds.
- 3.If you run NetMeeting program behind SUA to connect an outside user, the outside user will see two identical users in screen.
- 4.Add CI command : PPP LCP ACFC ON/OFF.
- 5.Support ISDN embedded protocol analyzer (EPA).
  - "isdn fw analyzer on" turn on EPA.
  - "isdn fw analyzer off" turn off EPA
  - "isdn fw analyzer dump" dump EPA raw data, it need another program to analyze it.

## ***Enhancement Details***

---

### **◆ CLID callback support for dial-in users**

#### **Functional Description**

CLID is an authentication method to identify dial-in user. CLID callback is used for toll saving on ISDN because the call is disconnected immediately without picking up the phone. In previous version, only remote node is capable for CLID callback because there is no outgoing information for dial-in users. In 2.40, the CLID outgoing information will be set in Menu 13, and dial-in user is capable for callback.

#### **SMT Changes**

In Menu 13, login and password is not only for mutual authentication but also for outgoing callback.

Menu 13 - Default Dial-in Setup	
<p>Telco Options:</p> <p style="padding-left: 20px;">CLID Authen= None</p> <p>PPP Options:</p> <p style="padding-left: 20px;">Recv Authen= CHAP/PAP</p> <p style="padding-left: 20px;">Compression= Yes</p> <p style="padding-left: 20px;">Mutual Authen= Yes</p> <p style="padding-left: 20px;"><b>O/G Login= p100</b></p> <p style="padding-left: 20px;"><b>O/G Password= *****</b></p> <p>Multiple Link Options:</p> <p style="padding-left: 20px;">Max Trans Rate(Kbps)= 128</p> <p>Callback Budget Management:</p> <p style="padding-left: 20px;">Allocated Budget(min)=</p> <p style="padding-left: 20px;">Period(hr)=</p>	<p>IP Address Supplied By:</p> <p style="padding-left: 20px;">Dial-in User= Yes</p> <p style="padding-left: 20px;">IP Pool= No</p> <p style="padding-left: 20px;">IP Start Addr= N/A</p> <p style="padding-left: 20px;">IP Count(1,2)= N/A</p> <p>Session Options:</p> <p style="padding-left: 20px;">Edit Filter Sets= No</p>
<p>Press ENTER to Confirm or ESC to Cancel:</p>	

#### **New CI command**

No new CI command.

## ◆ **Outgoing data call bumping support**

### **Functional Description**

Call bumping is a feature which Prestige will manage a MP bundle dynamically for different traffic. That means Prestige will drop a channel in a bundle when necessary, and reconnect it when possible. The current implementation works for POTS call only. For data packet, Prestige won't drop a channel for it if all channels are occupied. With outgoing data call bumping, Prestige will drop a channel in an MP bundle if there is a packet to other remote node.

### **SMT Changes**

No changes.

### **New CI command**

No new CI command.

## ◆ **DHCP relay**

### **Functional Description**

DHCP stands for Dynamic Host Configuration Protocol. It includes three types of roles, DHCP server, DHCP relay and DHCP client. DHCP server is a server who manages the IP addresses to DHCP clients. DHCP relay is a middle role between server and client. Whenever DHCP client request an IP address, DHCP relay will forward the request to a DHCP server and forward the response to the DHCP client from the DHCP server. We have supported DHCP server in 1.40. And DHCP relay will be supported in 2.40.

### **SMT Changes**

New option will be added in 3.2 for DHCP relay.

Menu 3.2 - TCP/IP and DHCP Ethernet Setup

**DHCP= Relay**  
Configuration:  
Client IP Pool Starting Address= N/A  
Size of Client IP Pool= N/A  
Primary DNS Server= N/A  
Secondary DNS Server= N/A  
Relay Server Address= 0.0.0.0

TCP/IP Setup:  
IP Address= 192.168.4.1  
IP Subnet Mask= 255.255.255.0  
RIP Direction= Both  
Version= RIP-2B

Press ENTER to Confirm or ESC to Cancel:  
Press Space Bar to Toggle.

#### New CI command

ip	dhcp	iface name	mode	server/relay/none	set DHCP mode for server/relay/none
			relay	server <ipaddr>	set DHCP relay server address

#### ◆ More DHCP users

##### Functional Description

The current IP addresses managed by DHCP server is 32 at maximum. In 2.40, the maximum will be increased to 253 at least.

##### SMT Changes

No changes.

#### New CI command

No new CI command.

#### ◆ NetMeeting support for SUA

##### Functional Description

In current version, NetMeeting does not work while SUA is enable. In 2.40, NetMeeting will be supported for both incoming and outgoing call. For outgoing call, there is no special setting. For incoming call, port 1503 and 1720 is required to set for server.

## SMT Changes

No changes.

## New CI command

No new CI command.

## ◆ Minimum Toll Period external specification

### Functional Description

Phone call is charged by time in most places. It is always rounded up at the charging period. For example, Prestige may be idled out and drop the call at 10 seconds in a 3 minutes toll period. That call is still charged for 3 minutes. That means the left 2 minutes and 50 seconds is wasted. With minimum toll period, Prestige will try to use all the toll period at most. In above case, Prestige will try to extend the idle timeout to the nearest 3 minutes. If there is any packet during the extended 2 minutes and 50 seconds, the idle timeout will be cleared and the second call is eliminated. Since the session time calculation by Prestige is not necessary synchronized with Telecom, Prestige will drop the channel 5 seconds shorter than the edge of toll period. Therefore, the minimum toll period won't work if the toll period is less than 5 seconds.

## SMT Changes

Menu 11.1 - Remote Node Profile	
Rem Node Name= ?	Edit PPP Options= No
Active= Yes	Rem IP Addr= ?
Call Direction= Both	Edit IP= No
Incoming:	Telco Option:
Rem Login= ?	Transfer Type= 64K
Rem Password= ?	Allocated Budget(min)=
Rem CLID=	Period(hr)=
Call Back= No	Nailed-Up Connection= N/A
Outgoing:	<b>Toll Period(sec)= 0</b>
My Login=	Session Options:
My Password= *****	Edit Filter Sets= No
Authen= CHAP/PAP	Idle Timeout(sec)= 100
Pri Phone #= ?	
Sec Phone #=	
Press ENTER to Confirm or ESC to Cancel:	

## New CI command

No new CI command.

## ◆ Time and Date Setting

### Functional Description

During boot procedure, Prestige will try to connect to a time server somewhere in Internet to calibrate its system clock. In menu 24.10, Prestige administrator can choose which time protocol is preferred, where is the time server (i.e. its IP address) and the time zone of where Prestige is. The Prestige supports three time protocols, which are “Daytime (RFC-867)”, “Time (RFC-868)” and “NTP (RFC-1305)”. The former two protocols employ TCP protocol, and the last one use UDP protocol. Valid date value is from January 1, 1990 to February 5, 2036. The “Time Zone” field is referred to the time zone of where Prestige is located. It is NOT to the time server’s location.

**SPECIAL NOTE:** Daytime server offers reference time referred to server’s own local time, but not Greenwich Mean Time (GMT). So, the “Time Zone” field DOES NOT apply to this time service. The other two kinds of time service offer GMT reference time.

### SMT design

Menu 24.10 - System Maintenance - Time and Date Setting	
Use Time Server when Bootup= None/Daytime/ Time/NTP	
Time Server IP Address= 202.132.154.169	
Current Time:	14 : 00 : 47
New Time (hh:mm:ss):	14 : 00 : 47
Current Date:	1999 - 12 - 21
New Date (yyyy-mm-dd):	1999 - 12 - 21
Time Zone= GMT+0800	
Press ENTER to Confirm or ESC to Cancel:	

### New CI command

sys	adjtime	calibrate system clock with time server
-----	---------	---

## ◆ Call Scheduling

## Functional Description

Prestige can allow the user to schedule a dial-up connection in specified time. It can let the ISP or the remote nodes in menu 11 to connect or to be dropped down automatically. User may configure a remote node with multiple schedules on a specified day or weekdays. Just like what the scheduled recording function in a video recorder, you can schedule a remote node to connect in a specified date and time.

## SMT design

Menu 26 'Schedule Setup' is added in Main Menu.

Copyright (c) 1994 – 2000 ZyXEL Communications Corp.

Prestige 100 Main Menu

Getting Started	Advanced Management
1. General Setup	21. Filter Set Configuration
2. ISDN Setup	
3. Ethernet Setup	23. System Password
4. Internet Access Setup	24. System Maintenance
Advanced Applications	<b>26. Schedule Setup</b>
11. Remote Node Setup	
12. Static Routing Setup	
13. Default Dial-in Setup	
14. Dial-in User Setup	
15. NAT Setup	99. Exit

Enter Menu Selection Number:

There are twelve individual schedule sets in Menu 26.

Menu 26 - Schedule Setup

Schedule Set #	Name	Schedule Set #	Name
1	hinet	7	
2		8	
3		9	
4		10	
5		11	
6		12	

Enter Schedule Set Number to Configure= 1

Edit Name= hinet

Press ENTER to Confirm or ESC to Cancel:

- Select a schedule number first.
- Give it a name and enter menu 26.1.  
(P.S. If clear the 'Name' field to blank, Prestige will delete this schedule.)

Menu 26.1 is the schedule configuration

<p style="text-align: center;"><b>Menu 26.1 Schedule Set Setup</b></p> <p>Active= Yes/No Start Date(yyyy-mm-dd)= 1990 - 1 - 1 How Often= Once/Weekly Once:     Date(yyyy-mm-dd)= 1990 - 1 - 1 Weekdays:     Sunday= Yes/No or N/A     Monday= Yes/No or N/A     Tuesday= Yes/No or N/A     Wednesday= Yes/No or N/A     Thursday= Yes/No or N/A     Friday= Yes/No or N/A     Saturday= Yes/No or N/A Start Time(hh:mm)= 12 : 00 Duration(hh:mm)= 16 : 00 Action= Forced On/Forced Down/Disable Dial-on-demand         /Enable Dial-on-demand</p> <p style="text-align: center;">Press ENTER to Confirm or ESC to Cancel:</p>
---

- Active: schedule will be run or not.
- Start Date: valid from this day; doesn't mean the first running day.
- How Often: selecting 'Once', and the schedule will be executed only on the 'Once''Date'. If selecting 'Weekly', it will run on selected weekdays during each week.
- Start Time: hour and minute for start this schedule
- Duration: how long will this schedule continue?
- Action
  - Forced On: during the period, the remote node will always keep online (idle timeout will be disabled).
  - Forced Down: during the period, this remote node will always keep down, If this remote node is already connected, then it will be dropped. Demanded dial or trigger call from LAN will be ignored.
  - Enable Dial-on-demand: Enable Dial-on-demand: during the period, this remote node will allow to connect. D.O.D. is default to a remote node without schedules. This scheduled action can be used to override the other actions, like 'Forced Down'.



- Disable Dial-on-demand: during the period, this remote node will deny any demand dial. If there are any connection online, will not drop it. After that connection is dropped manually or by idle timeout, remote node can't be triggered up then.
- When out of duration, scheduler will do nothing to this remote node. If a remote node with schedule 'Forced On' is over, it will return to normal operation 'dial-on-demand', not opposite 'Forced Down'.

You can assign 1~4 schedule sets to a remote node in menu 11.1

Menu 11.1 - Remote Node Profile	
Rem Node Name= Hinet	Edit PPP Options= No
Active= Yes	Rem IP Addr= 192.168.50.22
Call Direction= Outgoing	Edit IP= No
Incoming:	Telco Option:
Rem Login= N/A	Transfer Type= 64K
Rem Password= N/A	Allocated Budget(min)=
Rem CLID= N/A	Period(hr)=
Call Back= N/A	<b>Schedules= 1,3,2,11</b>
Outgoing:	Nailed-Up Connection= No
My Login= abcd	Toll Period(sec)= 0
My Password= ****	Session Options:
Authen= CHAP/PAP	Edit Filter Sets= No
Pri Phone #= 4125678	Idle Timeout(sec)= 100
Sec Phone #=	
Press ENTER to Confirm or ESC to Cancel:	

## New CI command

No new CI command.

## ◆ NAT(Network Address Translation)

### Functional Description

NAT only applies to IP packets. NAT will change a packet's IP address and port number to allow networks which do not have legal Internal address to access the Internet. NAT has four types: One to One, Many to One, Many to Many Overload, and Many to Many No Overload. The current SUA is considered NAT type Many to One. Multiple NAT entries can be set up to handle different IP address ranges on the LAN.

NAT types Many to One and Many to Many Overload use Port Address Translation (PAT). PAT utilizes port number and IGA(Internal Global Address: The outside IP address) to determine the ILA(Internal Local Address: The inside IP address). Each IGA can be shared by multiple ILAs.

Each remote node can be assigned one NAT set. When NAT is turned on, the rules in this set will be applied to all traffic through this remote node. One IP address per remote node can be designated as

the SUA Server IP address. Packets received by the SUA Server can be redirected to an inside server as defined by the user.

### **SMT design**

The menu 15 is changed from “SUA Server Setup” to “NAT Setup”.

Copyright (c) 1994 - 2000 ZyXEL Communications Corp.	
Prestige 100 Main Menu	
Getting Started	Advanced Management
1. General Setup	21. Filter Set Configuration
2. ISDN Setup	
3. Ethernet Setup	23. System Password
4. Internet Access Setup	24. System Maintenance
Advanced Applications	26. Schedule Setup
11. Remote Node Setup	
12. Static Routing Setup	
13. Default Dial-in Setup	
14. Dial-in User Setup	
15. <b>NAT Setup</b>	99. Exit
Enter Menu Selection Number:	

Menu 15 - NAT Setup
1. Address Mapping Sets
2. NAT Server Sets
Enter Menu Selection Number:

Menu 15.1 - Address Mapping Sets
1. hinet
2.
3.
4.
5.
6.
7.
8.
255. SUA (Read Only)
Enter Set Number to Edit:

Menu 15.1.1 - Address Mapping Rules

Set Name= hinet

Idx	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1.	0.0.0.0	255.255.255.255	0.0.0.0		M-1
2.	Server Set= 1		0.0.0.0		Server
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Action= Edit, Select Rule= 0

Press ENTER to Confirm or ESC to Cancel:

- Note:**
- 4 actions are “Edit”, “Insert Before”, “Delete”, and “Save Set”; the default is “Edit”. “**Edit**” means to edit the selected rule. “**Insert Before**” means to insert a rule before the select rule and all the rules after the selected rule will be drawn back one rule. “**Delete**” means to delete the selected rule and all the rules after the selected one will advance one rule. “**Save Set**” means to save the whole set and when users choose the action as that, “**Select Rule**” item will be disabled.
  - The system processes the rules by turn.

Menu 15.1.1.1 - hinet - Rule 1

Type: Many-to-One

Local IP:  
Start= 0.0.0.0  
End = 255.255.255.255

Global IP:  
Start= 0.0.0.0  
End = N/A

Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

Menu 15.1.1.2 - hinet - Rule 2

Type: Server

Local IP:

Start= N/A

End = N/A

Global IP:

Start= 0.0.0.0

End = N/A

Server Mapping Set= 1

Press ENTER to Confirm or ESC to Cancel:

**Note:**

1. Total 5 types, “One-to-One”, “Many-to-One”, “Many-to-Many Overload”, “Many-to-Many No Overload” and “Server”.
2. Whichever Local IP or Global IP, the end address must be after the start address.
3. If the rule is for all local IP, put start address as 0.0.0.0 and end address as 255.255.255.255.
4. If dynamic IP, put the value of Global Start IP as 0.0.0.0.
5. The server mapping set is mapped in menu 15.2.

Menu 15.2 - NAT Server Sets

1. Server Set 1
2. Server Set 2
3. Server Set 3
4. Server Set 4
5. Server Set 5
6. Server Set 6
7. Server Set 7
8. Server Set 8
9. Server Set 9
10. Server Set 10

Enter Set Number to Edit:

Menu 15.2.1 - Multiple Server Configuration

Port #	IP Address
-----	-----
1. Default	0.0.0.0
2. 0	0.0.0.0
3. 0	0.0.0.0
4. 0	0.0.0.0
5. 0	0.0.0.0
6. 0	0.0.0.0
7. 0	0.0.0.0
8. 0	0.0.0.0
9. 0	0.0.0.0
10. 0	0.0.0.0
11. 0	0.0.0.0
12. 0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

Remote node setting is in menu 11.3 and menu 4

Menu 11.3 - Remote Node Network Layer Options

Rem IP Addr: 0.0.0.0  
Rem Subnet Mask= 0.0.0.0  
My WAN Addr= 0.0.0.0

**NAT= Full Feature**  
**Address Mapping Set= 1**

Metric= 2  
Private= No  
RIP Direction= Both  
Version= RIP-2B

Press ENTER to Confirm or ESC to Cancel:

Menu 4 - Internet Access Setup

ISP's Name= hinet  
Pri Phone #= 4125678  
Sec Phone #=  
My Login= icchung  
My Password= \*\*\*\*\*  
My WAN IP Addr= 0.0.0.0

**NAT= [None/SUA Only/Full Feature]**  
**Address Mapping Set= 1**

Telco Options:  
Transfer Type= 64K

Multilink= Off  
Idle Timeout= 300

Press ENTER to Confirm or ESC to Cancel:

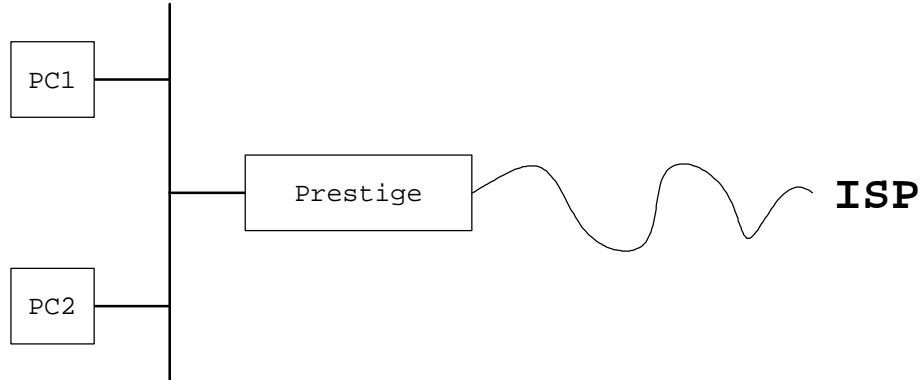
**Note:** To leave "My WAN IP Addr" as 0.0.0.0 means dynamic IP.

**New CI command**

ip	nat	iamt		Display NAT system information.
		iface	<iface name>	Show the NAT status of an interface.
		lookup	<set #>	List all the active rules in a set.
		new-lookup	<set #>	List all the new rules which are not yet used due to conflicts with old rules.
		reset	<iface name>	This deletes all the entries inside the session table and IAMT table but not the lookup table.
		server		Display server table.
		update		Updates the runtime NAT data to what is in ROM.

- **Examples**

**Case 1 (ISP case, internet access only)**



In ISP case with internet access only, we need one rule that all ILAs share one dynamic IGA assigned by ISP for outgoing packet.

Enter to menu 15.1 and choose a set to create an address mapping set named ISP (the first set is used in this case).

<p style="text-align: center;">Menu 15.1 - Address Mapping Sets</p> <ol style="list-style-type: none"><li>1.</li><li>2.</li><li>3.</li><li>4.</li><li>5.</li><li>6.</li><li>7.</li><li>8.</li><li>255. SUA (Read Only)</li></ol> <p style="text-align: center;">Enter Set Number to Edit:</p>
---

In menu 15.1.1, give the set a name (ISP in this case), then toggle action to edit and select rule 1 to edit.

Menu 15.1.1 - Address Mapping Rules

Set Name= ISP

Idx	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
---	-----	-----	-----	-----	-----
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Action= Edit , Select Rule= 0

Press ENTER to Confirm or ESC to Cancel:

Toggle type to many-to-one because more than one machines share 1 IP in the most ISP case, enter local start IP as 0.0.0.0 and local end IP as 255.255.255.255 to mean this rule is used by all machines in local LAN, and enter global IP as 0.0.0.0 to mean the IGA is a dynamic IP.

Menu 15.1.1.1 - ISP - Rule 1

Type: Many-to-One

Local IP:  
Start= 0.0.0.0  
End = 255.255.255.255

Global IP:  
Start= 0.0.0.0  
End = N/A

Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:



After doing that, the user will watch the menu 15.1.1 as following:

Menu 15.1.1 - Address Mapping Rules					
Set Name= ISP					
Idx	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
---	-----	-----	-----	-----	-----
1.	0.0.0.0	255.255.255.255	0.0.0.0		M-1
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
Action= Edit , Select Rule= 0					
Press ENTER to Confirm or ESC to Cancel:					

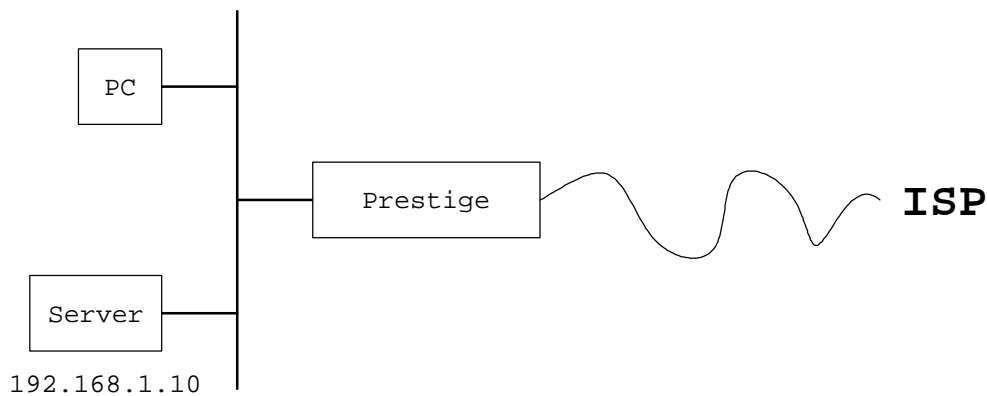
Toggle action to Save Set to save all the set.

Menu 15.1 - Address Mapping Sets	
1.	ISP
2.	
3.	
4.	
5.	
6.	
7.	
8.	
255.	SUA (Read Only)
Enter Set Number to Edit:	

Edit menu 4 as following,

Menu 4 - Internet Access Setup	
ISP's Name=	ISP
Pri Phone #=	4125678
Sec Phone #=	
My Login=	icchung
My Password=	*****
My WAN IP Addr=	0.0.0.0
<b>NAT= [None/SUA Only/Full Feature]</b>	
<b>Address Mapping Set= 1</b>	
Telco Options:	
Transfer Type=	64K
Multilink=	Off
Idle Timeout=	300
Press ENTER to Confirm or ESC to Cancel:	

#### Case 2 (ISP case, with internal server)



In ISP case, we need to add one extra rule in menu 15.1.1 as one server rule for incoming packet. Firstly, go to menu 15.2, and select a NAT server set to edit (set 1 in this case), and then edit the default value as 192.168.1.10 shown as below.

Menu 15.2 - NAT Server Sets

1. Server Set 1
2. Server Set 2
3. Server Set 3
4. Server Set 4
5. Server Set 5
6. Server Set 6
7. Server Set 7
8. Server Set 8
9. Server Set 9
10. Server Set 10

Enter Set Number to Edit:

Menu 15.2.1 - Multiple Server Configuration

Port #	IP Address
-----	-----
1. Default	192.168.1.10
2. 0	0.0.0.0
3. 0	0.0.0.0
4. 0	0.0.0.0
5. 0	0.0.0.0
6. 0	0.0.0.0
7. 0	0.0.0.0
8. 0	0.0.0.0
9. 0	0.0.0.0
10. 0	0.0.0.0
11. 0	0.0.0.0
12. 0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

Secondly, go to menu 15.1.1.2 (rule 1 is used for outgoing packet), and then toggle type to Server, and insert global IP as 0.0.0.0 (dynamic IP) and server mapping set as 1.

Menu 15.1.1.2 - ISP - Rule 2

Type: Server

Local IP:

Start= N/A

End = N/A

Global IP:

Start= 0.0.0.0

End = N/A

Server Mapping Set= 1

Press ENTER to Confirm or ESC to Cancel:

Then the user can watch the menu 15.1.1 as following,

Menu 15.1.1 - Address Mapping Rules

Set Name= ISP

Idx	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1.	0.0.0.0	255.255.255.255	0.0.0.0		M-1
2.	Server Set= 1		0.0.0.0		Server
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Action= Edit , Select Rule= 0

Press ENTER to Confirm or ESC to Cancel:

Toggle action to Save Set to save all the set.

Menu 4 - Internet Access Setup

ISP's Name= ISP

Pri Phone #= 4125678

Sec Phone #=

My Login= icchung

My Password= \*\*\*\*\*

My WAN IP Addr= 0.0.0.0

NAT= Full Feature

Address Mapping Set= 1

Telco Options:

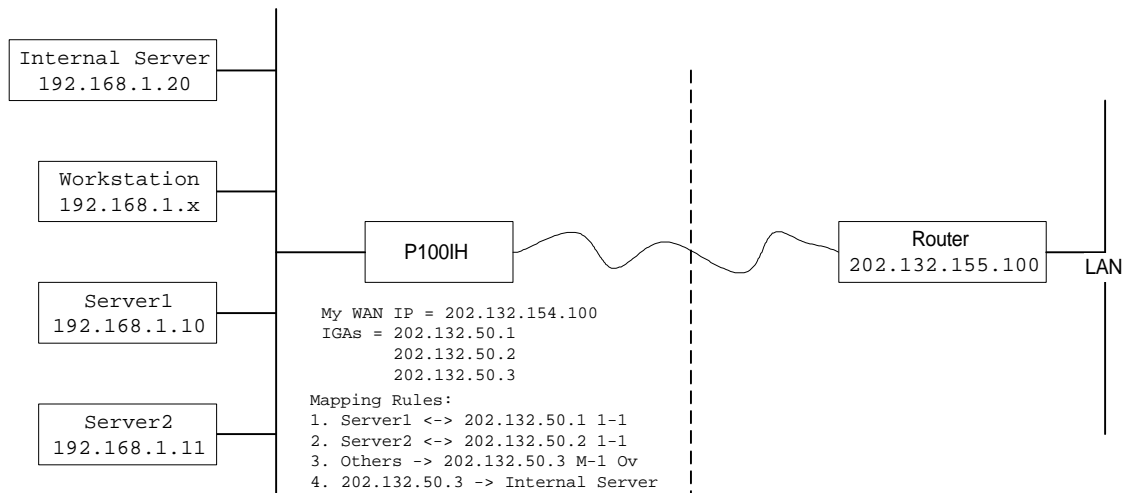
Transfer Type= 64K

Multilink= Off

Idle Timeout= 300

Press ENTER to Confirm or ESC to Cancel:

### Case 3 (General case, with 3 IGAs)



In this example, user has to configure 4 rules, 2 for one-to-one mapping (one-to-one for both incoming packets and outgoing packets), one for outgoing packets, and the other for incoming packets. The address mapping set has to be configured as following (use set 1 in this case).

Menu 15.1.1 - Address Mapping Rules					
Set Name= test					
Idx	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1.	192.168.1.10		202.132.50.1		1-1
2.	192.168.1.11		202.132.50.2		1-1
3.	0.0.0.0	255.255.255.255	202.132.50.3		M-1
4.	Server Set= 1		202.132.50.3		Server
5.					
6.					
7.					
8.					
9.					
10.					
Action= Edit , Select Rule= 0					
Press ENTER to Confirm or ESC to Cancel:					

Another, the server set 1 has to be set as following.

Menu 15.2.1 – Multiple Server Configuration	
Port #	IP Address
-----	-----
1. Default	192.168.1.20
2. 0	0.0.0.0
3. 0	0.0.0.0
4. 0	0.0.0.0
5. 0	0.0.0.0
6. 0	0.0.0.0
7. 0	0.0.0.0
8. 0	0.0.0.0
9. 0	0.0.0.0
10. 0	0.0.0.0
11. 0	0.0.0.0
12. 0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

In this case, menu 11.3 has to be configured as following,

Menu 11.3 - Remote Node Network Layer Options	
Rem IP Addr: 202.132.155.100	
Rem Subnet Mask= 255.255.255.0	
My WAN Addr= 202.132.154.100	
<b>NAT= Full Feature</b>	
<b>Address Mapping Set= 1</b>	
Metric= 2	
Private= No	
RIP Direction= Both	
Version= RIP-2B	

Press ENTER to Confirm or ESC to Cancel:

### ***Bug fixes:***

---

The list is the bug fix since V2.41(C.00).

#### **ZyXEL Prestige P100 2.41(C.01):**

1. Fix the ISDN layer 2 link problem.
2. Connect two remote nodes with SUA only, the packets only gets through on the node that got dialed last.

### ***Known Bugs:***

---

1. For DSS-1 version, Prestige may stop placing outgoing data calls after Call Waiting/Call Hold/ Call Retrieve scenario if both of POTS ports are assigned the identical phone number. When it happens, the B-channel status shown on Menu 24.1 is wrong.
2. Prestige performance will be degraded if there exists a telnet session in Menu 24.1 via LAN at the same time.
3. When ISDN line is unplugged, there may be some garbage characters displayed after system initialization.
4. If the DRAM of P100 is 512KB size, there could be not enough memory to allocate for Prestige to perform full function.