ZyXEL Prestige 1600

ZyNOS v3.20(X.00) | 09/08/2000

Release Notes & Manual Supplement

Date: Sept 8, 2000

Congratulations on your purchase of P1600 Access Concentrator. The Prestige 1600 is a scalable DSL, delivering networking services at multiple selectable speeds from 64Kbps and 2Mbps. It can be deployed at high rise buildings, Telcos, ISPs and System Integrators with various configurations.

Equipped with one 10/100M Ethernet port, three Network Module Slots, and one optional WAN interface and one four-ports 10M/100M LAN switch card, the architecture of the Prestige 1600 allows network modules of different generations to co-exist in the same chassis and to inter-operate with the same system module.

IDSL solution is available now. Each Prestige 1600 provides up to 32 IDSL ports, and is equipped with 10/100M Ethernet as a daisy chain for connecting up to five units (thus a maximum of 160 IDSL ports).

ADSL NM, and SDSL NM will be available in the future.

This document describes the features in the ZyXEL Prestige 1600 product for its 3.20(X.00) release. The Bug fixed section describes the fixed problems at beta test. The known problem list section describes problems currently under investigation and enhancement.

Supported Platform:

ZyXEL Prestige firmware V3.20(X.00) supports both P1600 Master and Slave hardware platforms.

Version:

ZyNOS F/W Version: V3.20(X.00) | 9/8/2000 8:59:14
BootBase: V1.07 | 9/7/2000 8:59:14

New Features:

Telnet Client

Embedded Telnet Client is available at this version, you can invoke the Telnet Client program login to the specified IP address host at Menu 24.8 by “ip telnet <xxx.xxx.xxx.xxx>”.

Trace Route

Embedded Trace Route application is available at this version, you can invoke the Trace Route application by Menu 24.8 CI command “ip traceroute <xxx.xxx.xxx.xxx>.

Main Menu Change

Main Menu 14 Port setup is moved to Menu 6.

Static Route

Up to 240 Static routes are allowed at Menu 12.

RADIUS Accounting Server

RADIUS(Remote Authentication Dial In User Service) is designed as a protocol for authenticating and authorizing login users. At 3.20 Release, Prestige 1600 supports RADIUS accounting to extends the use of the protocol to cover delivery of accounting information from the Network Access Server(NAS) to a RADIUS accounting server.

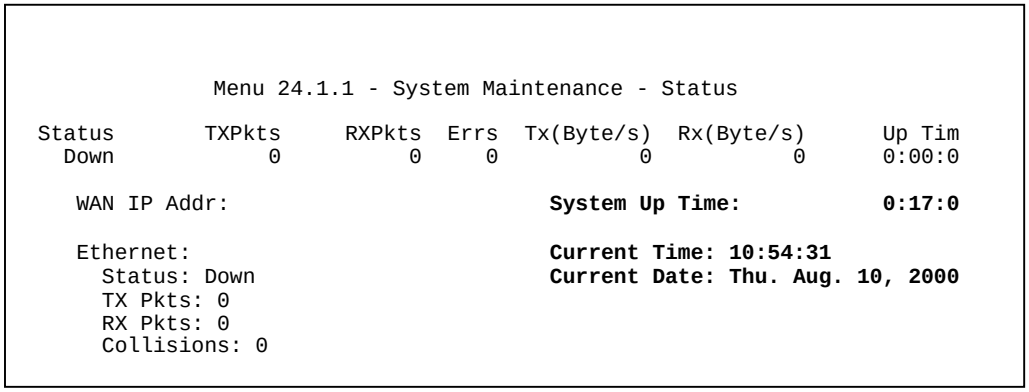
After setup menu 23.2 Accounting Server Address, Port (default is 1646) and Key, P1600 will send out the Acct-Status-Type, User-Name, NAS-IP-Address, Acct-Input-Octets, Acct-Output-Octets, Acct-Session-Time, Acct-Terminate-Cause, NAS-Port accounting information to the specific Radius Accounting Server.

```
Menu 23.2 - System Security - External Server

          Authentication Server:
            Active= No
            Type: RADIUS
            Server Address=
            Port #= 1645
            Key= ********

          Accounting Server:
            Active= Yes
            Type: RADIUS
            Server Address= 192.168.10.100
            Port #= 1646
            Key= ********
```

Time and Date Setting
P1600 supports Real Time Clock (RTC) to store current Time and Date at this version.

```
Menu 24.9 - System Maintenance - Time and Date Setting


   Current Time:                          03 : 22 : 32
   New Time (hh:mm:ss):                   3  : 22 : 32

   Current Date:                          2000 - 01 -01
   New Date (yyyy-mm-dd):                 2000 - 1 - 1
```

And Menu 24.1.1 now can show the system up time and current Date and Time.



NAT(Network Address Translation)

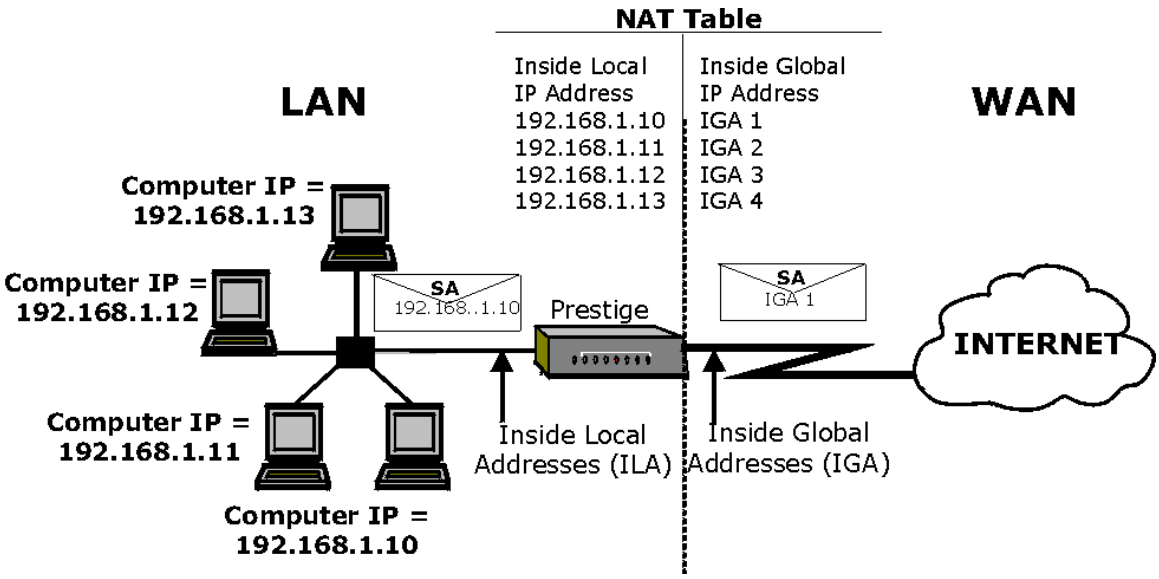
Introduction
NAT (Network Address Translation - NAT, RFC 1631) is the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and “unmaps” the global IP addresses on incoming packets back into local IP addresses. The IP addresses for the NAT can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see below), NAT offers the additional benefit of firewall protection. If no server is defined in these cases, all incoming inquiries will be filtered out by your Prestige, thus preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT).*

Advantages of NAT
NAT is a cost-effective solution to access the Internet or other remote TCP/IP networks as NAT conserves on the number of global IP addresses that a company needs in its communication with the outside world.
NAT supports popular Internet applications such as MS traceroute, CuSeeMe, IRC, RealAudio, VDOLive, Quake and PPTP with no extra configuration needed.
NAT supports servers, including multiple servers of the same type, to be accessible to the outside world.
NAT can provide firewall protection if you do not specify a server (for Many-to-One and Many-to-Many Overload mapping) and all incoming inquiries will be filtered out by your Prestige.

UDP and TCP packets can be routed. In addition, partial ICMP, including echo and traceroute, is supported.

How NAT works

Each packet consists of two addresses – a source address and a destination address. For outgoing packets, the ILA is the source address on the LAN, and the IGA is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. The term "Inside" refers to the set of networks that are subject to translation. Network Address Translation operates by mapping private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) and then forwards each packet to the Internet ISP, thus making them appear as if they had come from the NAT system itself (e.g., the Prestige). The Prestige keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following diagram illustrates this.



How NAT Works

NAT Mapping Types

NAT supports six types of IP/port mapping. They are:

One to One: In One-to-One mode, the Prestige maps one local IP address to one global IP address.

One to One (range): In One-to-One (range) mode, the Prestige maps the each local IP addresses to unique global IP addresses.

Many to One: In Many-to-One mode, the Prestige maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the SUA Only option in today's routers).

Many to Many Overload: In Many-to-Many Overload mode, the Prestige maps the multiple local IP addresses to shared global IP addresses.

No-Change: In No-Change mode, Prestige can bypass a range of valid internal IP addresses you already used.

Server: This type allows us to specify multiple inside servers of different types behind the NAT.

Port numbers do *not* change for One-to-One and Many-to-Many-No Overload NAT mapping types.

The following table summarizes these types.

NAT Mapping Types

Type	IP Mapping	SMT abbreviation
One-to-One	ILA1←→ IGA1	1-1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M-1
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M-M Ov
One-to-One (range)	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …	1-1 Ra
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server
NO-Change	Valid 1 IP Valid 2 IP	No-Chg

SUA (Single User Account) Versus NAT

SUA (Single User Account) in previous ZyNOS versions is a NAT set with 2 rules, Many-to-One and Server.. The Prestige supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node.
.

SMT Menus
Applying NAT in the SMT Menus
You apply NAT via menus 4 or 11.3 as displayed next. The next figure how you apply NAT for Internet access in Menu 4. Enter 4 from the Main Menu to go to **Menu 4 - Internet Access Setup**.

```
Menu 4 - Internet Access Setup

 ISP's Name= ISP
 My Login=
 My Password= ********

 Network Address Translation= Full Feature
   My IP Addr= N/A
   Address Mapping Set= 1
```

Applying NAT for Internet Access

```
Menu 11.3 - Remote Node Network Layer Options

    Rem IP Addr:
    Rem Subnet Mask= 0.0.0.0
    My WAN Addr= 0.0.0.0
    Network Address Translation= Full Feature
      Address Mapping Set= 1
    Metric= 2
    Private= No
    RIP Direction= Both
      Version= RIP-2B
    Multicast= N/A
    IP Policies=
```

Applying NAT to the Remote Node

This figure shows how you apply NAT to the remote node in Menu 11.1.

Step 1. Enter 11 from the Main Menu.

Step 2. Move the cursor to the **Edit IP** field, press the [SPACEBAR] to toggle the default **No** to **Yes**, then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**

This figure shows how you apply NAT to the remote node in Menu 3.2

```
Menu 3.2 - TCP/IP Setup

  TCP/IP Setup:
    IP Address= 192.168.100.1
    IP Subnet Mask= 255.255.255.0
    RIP Direction= Both
      Version= RIP-2B
    Multicast= N/A
    IP Policies=

    Network Address Translation= Full Feature
      Address Mapping Set= 1
```

Applying NAT to LAN

The following table describes the options for Network Address Translation.

Applying NAT in Menus 4 & 11.3 & 3.2

Field	Options	Description
Network Address Translation	**Full Feature**	When you select this option the SMT will use Address Mapping Set 1
	None	NAT is disabled when you select this option.

Network Address Translation	**Full Feature**	When you select this option the SMT will use Address Mapping Set 1
	None	NAT is disabled when you select this option.
	SUA Only	When you select this option the SMT will use Address Mapping Set 255 (Menu 15.1 – *see section 0*). It is a convenient, pre-configured, read only Many-to-1 port mapping set, sufficient for most purposes and helpful to people already familiar with SUA in previous ZyNOS versions. Note that there is also a **Server** type whose IGA is **0.0.0.0** in this set.

Configuring NAT
To configure NAT, enter 15 from the Main Menu to bring up the following screen.

Menu 15 NAT Setup

```
                    Menu 15 – NAT Setup

                1.    Address Mapping Sets
                2.    NAT Server Sets


              Enter Menu Selection Number:
```

Address Mapping Sets and NAT Server Sets:

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to machines on the LAN. Each remote node must specify which NAT Address Mapping Set to use. When you select **SUA Only**, the SMT will use the pre-configured Set 255 (read only) .

The NAT Server set is a list of LAN side servers mapped to external ports. To use this set, a server rule must be set up inside the NAT Address Mapping set.
Enter 1 to bring up **Menu 15.1 – Address Mapping Sets**.

```
                Menu 15.1 - Address Mapping Sets


                  1. _________
                  2. _________
                  3. _________
                  4. _________
                  5. _________
                  6. _________
                  7. _________
                  8. _________
                  9. _________
                 10. _________
                255. SUA (read only)
```

Address Mapping Sets

Let's look first at Option 255. Option 255 is equivalent to SUA in previous ZyXEL routers. The fields in this menu cannot be changed. Entering 255 brings up this screen.

```
                    Menu 15.1.255 - Address Mapping Rules

  Set Name= SUA

 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.                                    0.0.0.0                           Server
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.



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

SUA Address Mapping Rules

The following table explains the fields in this screen.

Please note that the fields in this menu are read-only. The Type, Local and Global Start/End IPs are normally (not for this read-only menu) configured in Menu 15.1.1.1 (described later) and the values are displayed here.

SUA Address Mapping Rules

Field	Description	Options/Example
Set Name	This is the name of the set you selected in Menu 15.1 or enter the name of a new set you want to create.	**SUA**
Idx	This is the index or rule number.	**1**
Local Start IP Local End IP	Local Start IP is the starting local IP address (ILA) . Local End IP is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	**0.0.0.0** **255.255.255.255**
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the Global Start IP.	**0.0.0.0**
Global End IP	This is the ending global IP address (IGA).	**N/A**
Type	These are the mapping types discussed above . Type **Server** allows us to specify multiple servers of different types behind NAT to this machine.	**Server**

Note: For all Local and Global IPs, the End IP address must begin after the IP Start address.

Now let's look at Option 1 in Menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note that, this screen is not read only, so we have extra **Action** and **Select Rule** fields. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

Please note that if the Set Name field is left blank, the entire set will be deleted.

First Set in Menu 15.1.1

```
                    Menu 15.1.1 - Address Mapping Rules

 Set Name= ?

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=

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

The Type, Local and Global Start/End IPs are configured in Menu 15.1.1.1 (described later) and the values are displayed here.

Ordering Your Rules

Ordering your rules is important. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

The description of the other fields is as described above. The Type, Local and Global Start/End IPs are configured in Menu 15.1.1.1 (described later) and the values are displayed here.

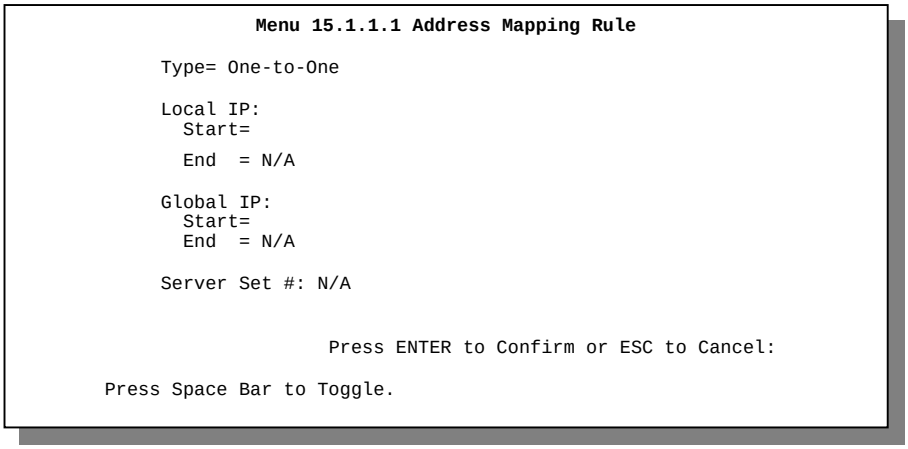
Menu 15.1.1

Field	Description	Option
Set Name	Enter a name for this set of rules. This is a required field. Please note that if this field is left blank, the entire set will be deleted.	
Action	There are 4 actions. The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **Save Set** means to save the whole set (note when you choose this action, the **Select Rule** item will be disabled).	**Edit** **Insert Before** **Delete** and **Save Set**
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	

N.B.: Save Set in the Action field means to save the whole set. You must do this if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Be careful when ordering your rules as each rule is executed in turn beginning from rule 1.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the Type, Local and Global Start/End IPs displayed in Menu 15.1.1.



Editing an Individual Rule in a Set

The following table describes the fields in this screen.

Menu 15.1.1.1 – configuring an individual rule

Field	Description	Option/Example
Type	Press the [SPACEBAR] to toggle through a total of 5 types. These are the mapping types discussed above. Type **Server** allows us to specify multiple servers of different types behind NAT to this machine.	**One-to-One** **Many-to-One** **Many-to-Many** **Overload** **One-to-One range and Server**
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.	
Start	This is the starting local IP address (ILA).	**0.0.0.0**
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for **One-to-One** and **Server** types**.**	**255.255.255.255**
Global IP		
Start	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to **0.0.0.0** only if the types are **Many-to-One** or **Server**.	**0.0.0.0**
End	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One, Many-to-One** and **Server** types.	**172.16.23.55**

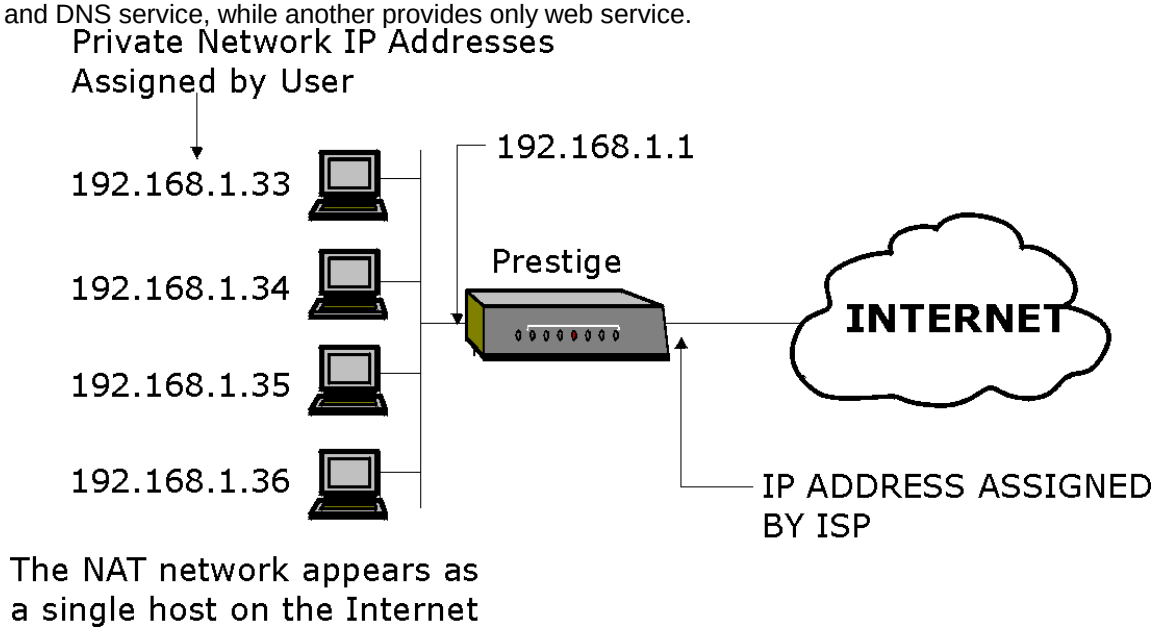
Note: For all Local and Global IPs, the End IP address must begin after the IP Start address, i.e., you cannot have an End IP address beginning before the Start IP address.

NAT Server Sets

The NAT Server set is a list of LAN side servers mapped to external ports (similar to the old SUA menu 15.1 of before). If you're using **Ethernet Encapsulation** with either **RR-Manager** or **RR-Toshiba Service Type** port 12 set to 1025 (non-editable).

Multiple Servers behind NAT

If you wish, you can make inside servers for different services, e.g., web or FTP, visible to the outside users, even though NAT makes your whole inside network appear as a single machine to the outside world. A service is identified by the port number, e.g., web service is on port 80 and FTP on port 21.
As an example (see the following figure), if you have a web server at 192.168.1.36 and an FTP server 192.168.1.33, then you need to specify for port 80 (web) the server at IP address 192.168.1.36 and for port 21 (FTP) another at IP address 192.168.1.33.
Please note that a server can support more than one service, e.g., a server can provide both FTP and DNS service, while another provides only web service.



Multiple Servers Behind NAT

Configuring a Server behind NAT

Follow the steps below to configure a server behind NAT:

Step 1. Enter 15 in the main menu to go to **Menu 15 – NAT Setup.**

Step 2. Enter 2 to go to **Menu 15.2 - NAT Server Setup**.

Step 3. Enter the service port number in the **Port #** field and the inside IP address of the server in the IP Address field.

Step 4. Press [ENTER] at the "Press ENTER to confirm …" prompt to save your configuration after you define all the servers or press **ESC** at any time to cancel.

Note: If you're using Ethernet Encapsulation with either RR-Manager or RR-Toshiba Service Type, then the SMT does not allow you to change the port 1025 entry.

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to our PNC Disk for more examples and details on NAT.

```
                Menu 15.2 - NAT Server Setup
Port #            IP  Address
----              ---------------
                  0.0.0.0
 1.Default
2.21              192.168.1.33
3.23              192.168.1.34
4.25              192.168.1.35
5.80              192.168.1.36
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. 1025          RR Reserved

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

Menu 15.2 – NAT Server Setup

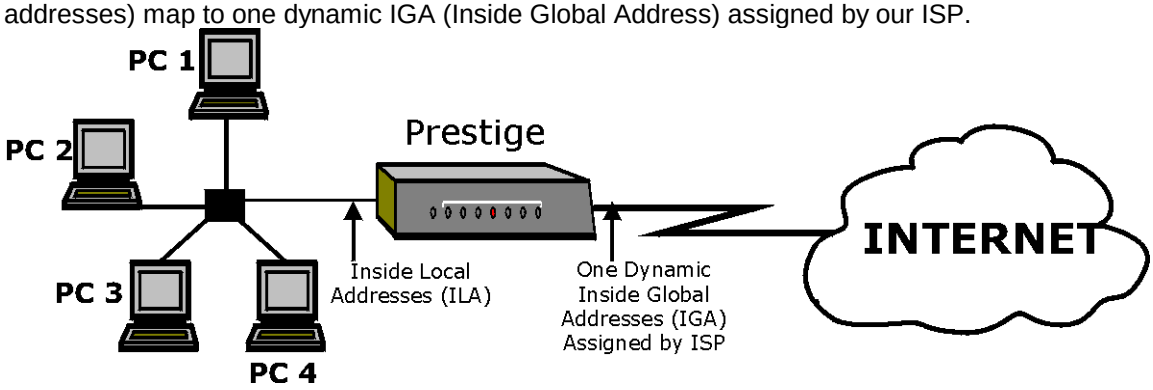
Services & Port numbers

Services	Port Number
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS(Domain Name System)	53
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
PPTP (Point-to-Point Tunneling Protocol)	1723

Examples

Example 1 – Internet Access Only

In our Internet access example, we only need one rule where all our ILAs (Inside Local addresses) map to one dynamic IGA (Inside Global Address) assigned by our ISP.



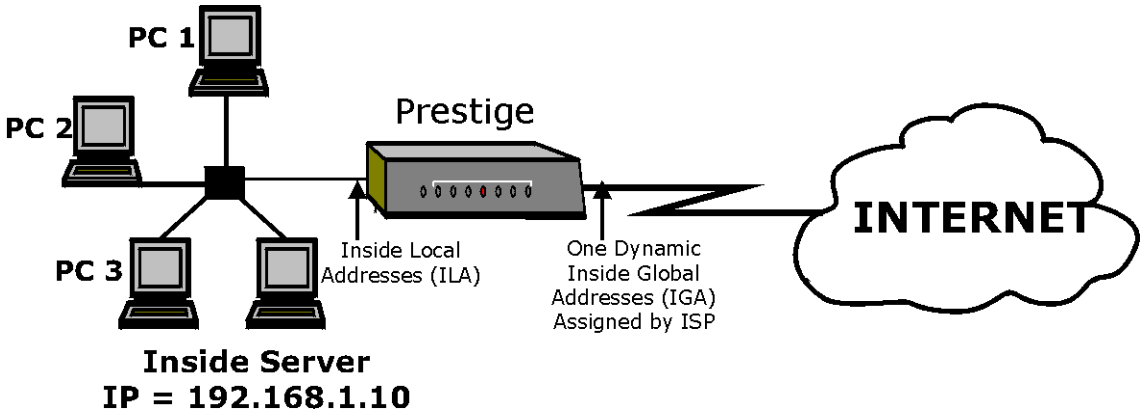
NAT Example 1

```
                Menu 4 - Internet Access Setup

ISP's Name= ISP
My Login=1234
My Password= ********

Network Address Translation= SUA only
  My IP Addr= 0.0.0.0
  Address Mapping Set= N/A
```

Internet Access & NAT Example

From Menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 0.* The **SUA Only** read only option from the **Network Address Translation** field in Menus 4 and 11.3 is specifically pre-configured to handle this case.

Example 2 – Internet Access with an Inside Server



NAT Example 2

In this case, we do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to Menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

```
                Menu 15.2 - NAT Server Setup
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. 1025          RR Reserved

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

Specifying an Inside Sever

Example 3 – General Case

In this example, we have 3 IGAs from our ISP. We have many departments but two have their own FTP server. All departments share the same router. We want to reserve 1 IGA for each department with an FTP server and the other IGA is used by all. We want to map the FTP servers to the first two of our IGAs and the other LAN traffic to the remaining IGA. We also want to map out third IGA to an inside web server and mail server. We need to configure 4 rules, 2 bi-directional and 2 one directional as follows.

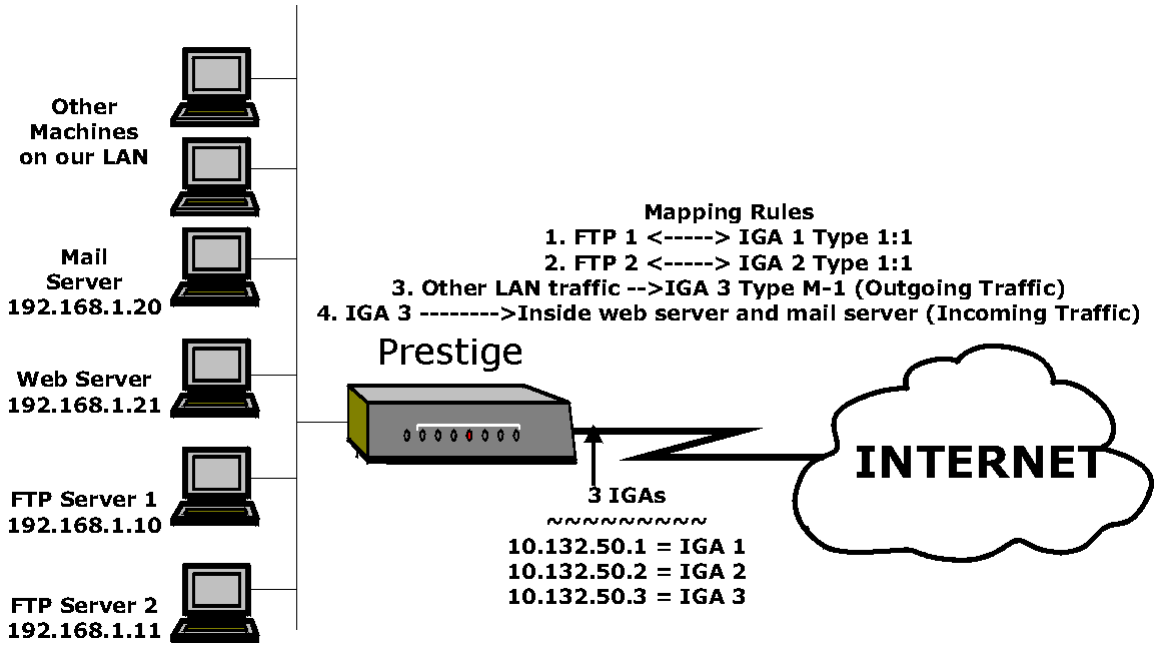
Rule 1. We map our first IGA to our first inside FTP server for FTP traffic in both directions (**1: 1** mapping, giving both local and global IP addresses).

Rule 2. We map our second IGA to our second inside FTP server for FTP traffic in both directions (**1: 1** mapping, giving both local and global IP addresses).

Rule 3. We map our other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

Rule 4. We also map our third IGA to our web server and mail server on the LAN. Type **Server** allows us to specify multiple servers, of different types, to other machines behind NAT on the LAN.

Our situation looks somewhat like this:



NAT - Example 3

Step 1. In this case we need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore we must choose the **Full Feature** option from the **Network Address Translation** field (in Menu 4 or Menu 11.3) in .

Step 2. Then enter 15 from the Main Menu.

Step 3. Enter 1 to configure the Address Mapping Sets.

Step 4. Choose 1 to begin configuring this new set. Enter a **Set Name**, choose the **Edit Action** and then select **1** from **Select Rule** field. Press [ENTER] to confirm.

Step 5. Select **Type=** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (*See)*

Step 6. Repeat the previous step for rules 2 to 4 as outlined above.

```
Menu 11.3 - Remote Node Network Layer Options

        Rem IP Addr:
        Rem Subnet Mask= 0.0.0.0
        My WAN Addr= 0.0.0.0
        Network Address Translation= Full Feature
          Address Mapping Set= 1
        Metric= 2
        Private= No
        RIP Direction= Both
          Version= RIP-2B
        Multicast= N/A
        IP Policies=
```

Example 3 – Menu 11.3

The following figure shows how to configure the first rule.

```
                Menu 15.1.1.1 Address Mapping Rule

        Type= One-to-One

        Local IP:
          Start= 192.168.1.10
          End  = N/A

        Global IP:
          Start= 10.132.50.1
          End  = N/A

        Server Set #: N/A


                          Press ENTER to Confirm or ESC to Cancel:

    Press Space Bar to Toggle.
```

Example 3 – Menu 15.1.1.1

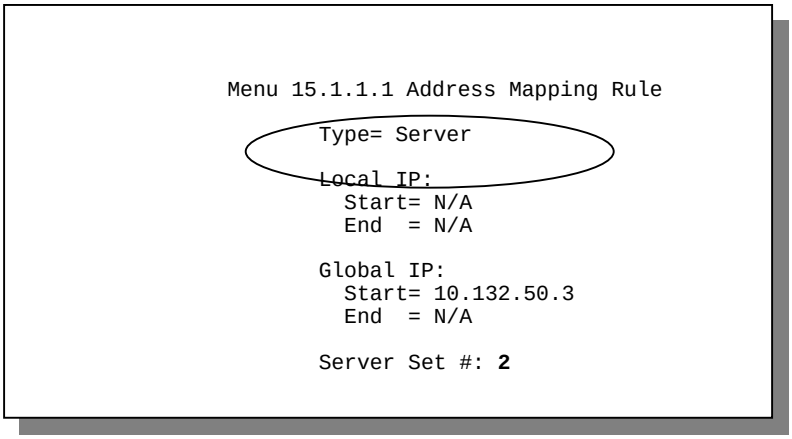
When we have configured all four rules, Menu 15.1.1 should look as follows.

```
                Menu 15.1.1 - Address Mapping Rules

 Set Name= Example3

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1. 192.168.1.10                      10.132.50.1                       1-1
```

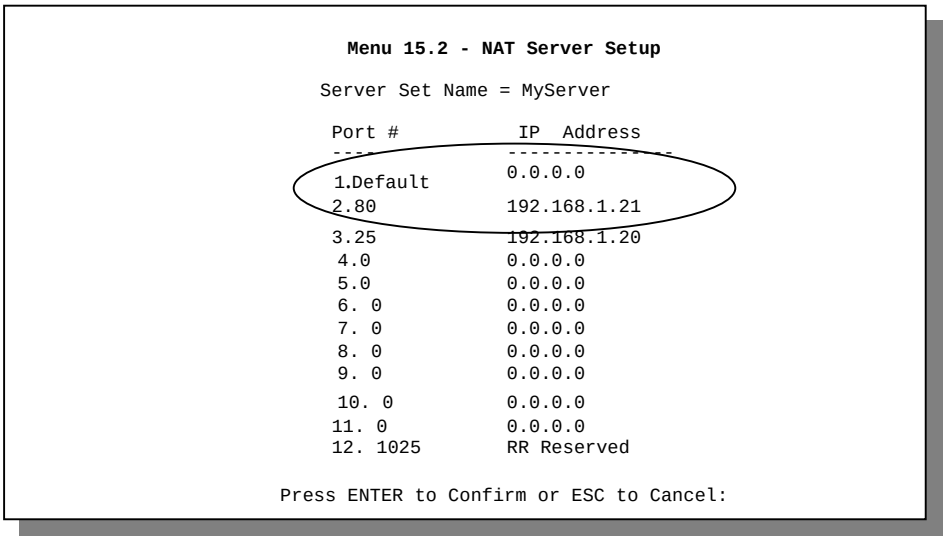
```
                Menu 15.2 - NAT Server Sets

                   1.   (Used by SUA)
                   2.  MyServer
                   3.  _________
                   4.  _________
                   5.  _________
                   6.  _________
                   7.  _________
                   8.  _________
                   9.  _________
                  10.  _________


                  Enter Set Number to Edit:
```

Example 3 Final Menu 15.1.1

The following figure shows how to configure the server type rule.
Select Address Mapping Rule Type to Server, and set IGA3 IP address 10.132.50.3



Now we configure our IGA3 to map to our web server and mail server on the LAN.
Step 7. Enter 15 from the Main Menu.
Step 8. Now enter 2 from this menu and configure it as shown in the table.

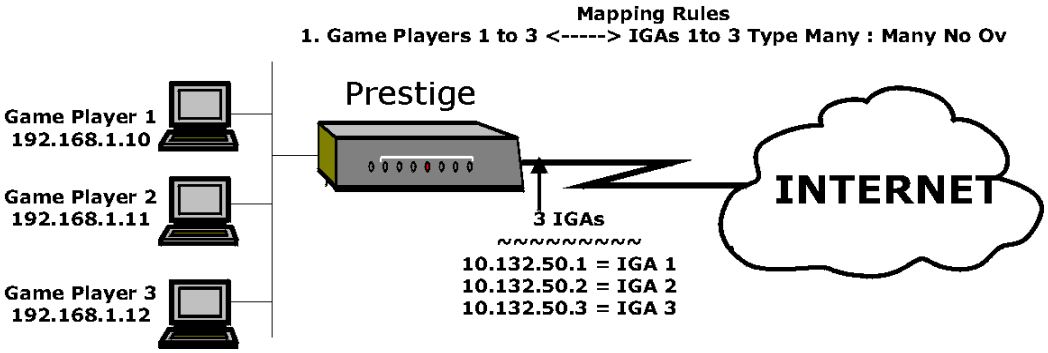


Example3 – Menu 15.2

Example 4 – Non NAT Friendly Application Programs

Many applications, for example gaming programs do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **One-to-One (range)** mapping as port

numbers do *not* change for **One-to-One (range)** (and **One-to-One**) NAT mapping types. The following figure illustrates this.



NAT Example 4

Some applications still won't work through NAT even when using types One-to-One **and** Many-to-Many No Overload **mapping types.**

Follow the steps outlined in example 3 above to configure these two menus as follows.

```
                    Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One (range)

Local IP:
  Start= 192.168.1.10
  End  = 192.168.1.12

Global IP:
  Start= 10.132.50.1
  End  = 10.132.50.3

Server Set #: N/A




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

Example 4- Menu 15.1.1.1 - Address Mapping Rule

After you've configured this menu, you should see the following screen.

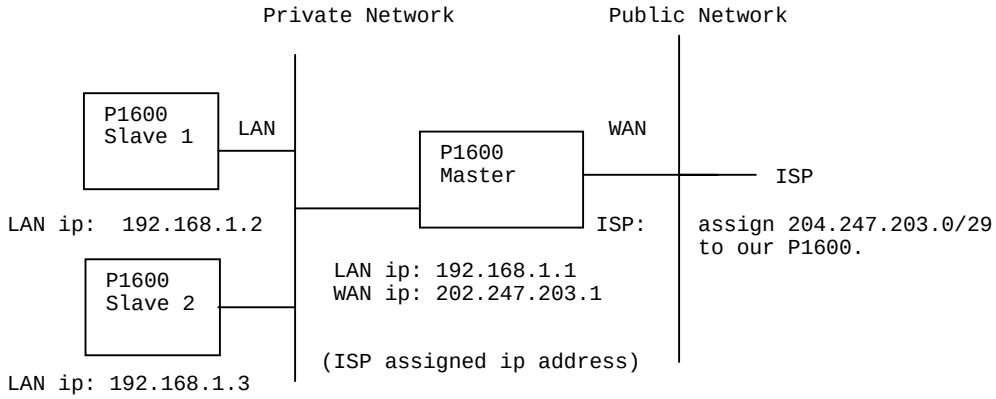
```
                        Menu 15.1.1 - Address Mapping Rules

      Set Name= Example4

     Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
     ---  ---------------  ---------------  ---------------  ---------------  ------
      1.  192.168.1.10     192.168.1.12     10.132.50.1      10.132.50.3      1-1 Ra
      2.
      3.
      4.
      5.
      6.
      7.
      8.
      9.
     10.

                       Action= Edit          Select Rule=

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

Example 4 - Menu 15.1.1 - Address Mapping Rules

Example 5 – NAT Application for Remote Management

P1600 are deployed as master-slave configurations. Remote management through Telnet can be achieved using Multi-NAT feature provided by Release 3. Most of the configuration is performed at the Master P1600 machine.

Configuration Diagram:



In the configuration above, we have the following information:

1. ISP assigns 204.247.203.1 to P1600 master and 204.247.203.2 thru 204.247.203.6 are assigned to Slave P1600 units.

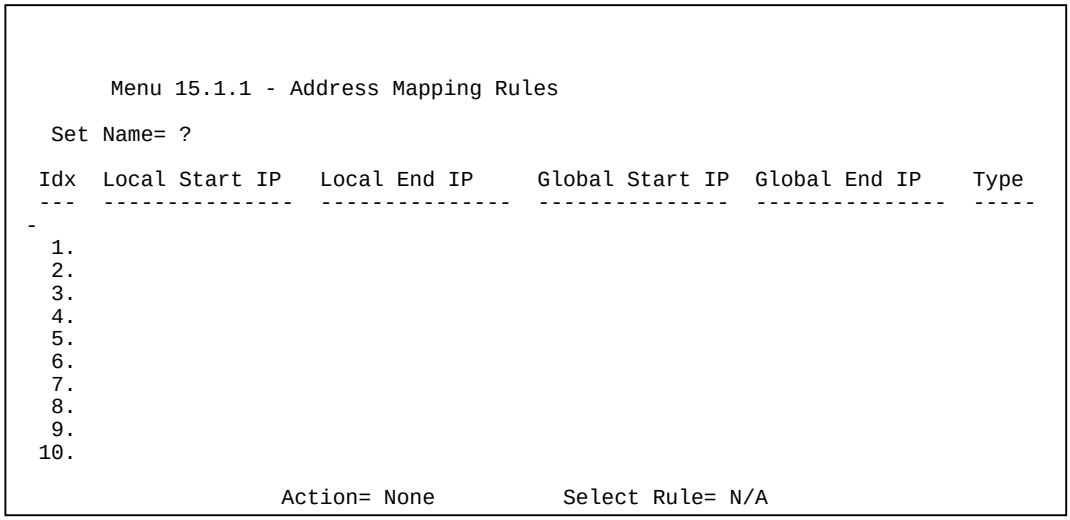
2. In the private LAN, the ip address for P1600 master is 192.168.1.1. Slave 1 and 2 have 192.168.1.2 and 192.168.1.3 respectively.
3. We want to map 204.247.203.2 to p1600 Slave 1 and 204.247.203.3 to P1600 Slave 2.

Detailed configuration setup procedures for P1600 Master unit:

Menu 15: NAT Setup:

We need to setup rules to let the Multi-NAT knows that we want to map 204.247.203.2 to Slave 1 private ip address(192.168.1.2) and map 204.247.203.3 to Slave 2 private ip address(192.168.1.3). Just go to Menu 15 and select one available slot. You should see the following screen.

Note: Assume set 1 is picked.



```
      Menu 15.1.1 - Address Mapping Rules

  Set Name= ?

 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= None          Select Rule= N/A
```

Enter the set name and go to ‘Action’. Press space bar and toggle it to ‘edit’. Enter the rule ID you want to use to the ‘Select Rule’ field.

```
      Menu 15.1.1 - Address Mapping Rules

 Set Name= Management

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= 1
```

Press ‘ENTER’ to proceed. You will go to the following screen. Enter the high lighted information shown below. The type we are using is call ‘one-to-one mapping' which maps an public IP address to the private IP address at the other end.

```
                Menu 15.1.1.1   Address Mapping Rule

        Type = one-to-one
        Local IP:
           Start = 192.168.1.2
           End = N/A

        Global IP:
           Start = 202.247.203.2
           End = N/A

        Server Set #: N/A
```

Repeat the same procedure for Slave 2 but pick another rule(ex. Rule # 2).

```
                Menu 15.1.1.2   Address Mapping Rule

           Type = one-to-one

           Local IP:
             Start = 192.168.1.3
             End = N/A

           Global IP:
             Start = 202.247.203.3
             End = N/A

           Server Set #: N/A
```

Now, from Menu 15.1.1, you should have the following setup available:

```
                          Menu 15.1.1 – Address Mapping Rule

Set Name = test
Idx     Local Start IP Local End IP   Global Start IP       Global End IP  Type
1.      192.168.1.2                   202.247.203.2                         1-1
2.      192.168.1.3                   202.247.203.3                         1-1
```

Up to this point, rule setup is finished. The next step is to let the WAN connection uses the Multi-NAT rule we just defined.

Menu 4:Internet Access Setup

From Menu 4, change ‘Network Address Translation’ into ‘Full Feature’ and modify ‘Address Mapping Set’ to 1(we used set 1 when we configured Menu 15).

```
                  Menu 4 - Internet Access Setup

                 ISP's Name= ATT
                 My Login= ZyXEL
                 My Password= ********

                 Network Address Translation= Full Feature
                   My IP Addr= 0.0.0.0
                   Address Mapping Set= 1



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

The configuration is done at this point. You can test it by using ‘telnet 204.247.203.2’ and you should be able to connect to the Slave 1 P1600 unit.

Know Problem List:

1. IP multicast is not supported at this release.
2. Default romfile 320x00c0.rom is for master P1600 whose 32 IDSL ports have been active already. A slave romfile will be released at Slave P1600 HW release.
3. **Due to Hardware limitation, C2-2 sample can only support 8M bytes flash memory. For C2-2 user, please use b03 Firmware version only. This release can not be applied to C2-2 sample.**
4. The default menu 3.2 TCP/IP IP Address setting are 192.168.1.1 at P1600 and other Prestige series products. It may happen you can not ping successfully to the P100L/P128L at P1600 CI command mode if they have same IP address at menu 3.2. Change IP address at one of them will solve the problem.

5. At menu 24.6 Restore Configuration do not have a timeout design at Xmodem protocol.
6. ICMP Packet length exceed 1500 bytes can not pass through NAT. P1600 will adjust TCP MSS to let TCP packets not exceed 1500 bytes. SUA has no problem for all kinds of protocol.
7. Login to P1600 by telnet, the password can not exceed 22 characters.
8. The interface identifiers of P1600 are changed from “idslxx” to “xdslxx”, it may cause problem if your SNMP management system still looks for original name.

Bugs Fixed:

1. Menu 1 DNS Server IP address setup will fail at first configuration, it is fixed at this version.
2. Slave P1600 can not be accessed by private IP address is solved by NAT new feature.
3. Only after reboot, menu 22 SNMP Trap Server IP Address will take effect, this bug is fixed at this version.

How To Update P1600

P1600

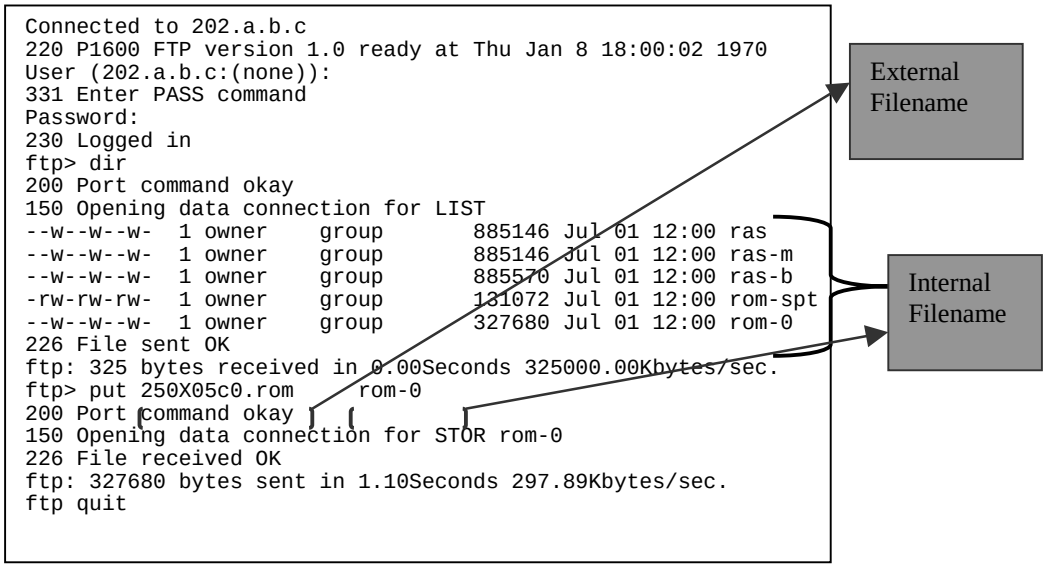
Versions:
ZyNOS F/W Version: V3.20(X.00) | 9/7/2000 8:59:14
BootBase: V1.07 | 9/7/2000 8:59:14

Boot Extension Commands:
ATBAx: Where x = baud rate
options available are:
1= 38.4K
2= 19.2K
3= 9.6K
4= 57.6K
5= 115.2K
ATUR: Upload Firmware file via XMODEM
File Name : p1600.bin

Romfile: p1600.rom
ATUR3: Upload Romfile and clear all settings, the setting will change to manufactory setting, baud rate sets to 9.6K, please change to 9.6K for further configuration.

FTP Upgrade

There are two set of filenames: internal (in P1600) and external (in PC, MAC, or UNIX). Each set contains ZyNOS firmware and the configuration file. Firmware file contains the firmware and the configuration file contains the SMT menu settings, defaults etc. The internal names are ras-m and ras-b (firmware files) and rom-spt and rom-0 (configuration files).



FTP Example

Usually, the external firmware filename is the router model name with a bin extension, e.g., p1600mas.bin. Rename it as “ras-m” or “ras-b” when uploading to the Prestige main block and backup block respectively using TFTP or FTP. You don’t have to rename the file when using XMODEM protocol.

The external configuration filename is usually the router model name with a *.rom extension, e.g.1600mas.rom. Rename it as rom-spt and rom-0 when transferring files to the Prestige. Renaming is not necessary if you transfer files using XMODEM protocol.

Table Filenames

Internal Filename	Description	External Filename	FTP Command Example
rom-spt	The rom-spt file is the user configuration file. It contains your Prestige configurations such as IP addresses, Remote Node settings etc. as well as your password.	*.rom	get rom-spt (backup) put rom-spt (restore)
rom-0	The rom-0 configuration file is the entire factory configuration file. It includes rom-spt, default settings, file system, log, etc. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (including the baud rate and default password), the error log and the trace log.	*.rom	put p1600.rom rom-0 (upload)
ras	This is the firmware filename for all Prestige models. This is ras-m when you upload the firmware to the main block and ras-b when you save the current firmware to the backup block.	*.bin	
ras-m	This is the router firmware filename on the Prestige 1600 when you are transferring files to the main block.	*.bin	put p1600.bin ras-m (upload)
ras-b	This is the router firmware filename on the Prestige 1600 when you are transferring files to the backup block.	*.bin	put p1600.bin ras-b (upload)