

P-660R-Tx v2 Series

ADSL2+ Router

Support Notes

Version3.40

Jan. 2006



FAQ 4

ZyNOS FAQ 4

 1. What is ZyNOS? 4

 2. How do I access the P-660R-Tx v2 Command Line Interface (CLI)? ... 4

 3. How do I update the firmware and configuration file? 4

 4. How do I upgrade/backup the ZyNOS firmware by using TFTP client program via LAN? 4

 5. How do I restore P-660R-Tx v2 configurations by using TFTP client program via LAN? 4

 6. What should I do if I forget the system password? 5

 7. How to use the Reset button?..... 5

 8. What is SUA? When should I use SUA? 5

 9. What is the difference between SUA and Multi-NAT? 6

 10. Is it possible to access a server running behind SUA from the outside Internet? If possible, how? 6

 11. When do I need Multi-NAT?..... 6

 12. What IP/Port mapping does Multi-NAT support ? 6

 13. How many network users can the SUA/NAT support? 7

 14. What are Device filters and Protocol filters? 8

 15. How can I protect against IP spoofing attacks? 8

General FAQ 10

 1. How can I manage P-660R-Tx v2? 10

 2. What is the default password to logging web configurator? 10

 3. How do I know the P-660R-Tx v2's WAN IP address assigned by the ISP? 10

 4. What is the micro filter or splitter used for? 10

 5. The P-660R-Tx v2 supports Bridge and Router mode, what's the difference between them? 10

 6. How do I know I am using PPPoE? 11

 7. Why does my provider use PPPoE? 11

 8. What is DDNS? 11

 9. When do I need DDNS service? 11

 10. What is DDNS wildcard? Does the P-660R-Tx v2 support DDNS wildcard? 12

 11. Can the P-660R-Tx v2's SUA handle IPSec packets sent by the IPSec gateway? 12

 12. How do I setup my P-660R-Tx v2 for routing IPSec packets over SUA? 12

 13. What is Traffic Shaping? 13

 14. What do the parameters (PCR, SCR, MBS) mean? 13

 15. Why do we perform traffic shaping in the P-660R-Tx v2 ? 13

ADSL FAQ 14

 1. How does ADSL compare to Cable modems? 14

 2. What is the expected throughput? 14

3. What is the micro filter used for?	14
4. How do I know the ADSL line is up?	14
5. How does the P-660R-Tx v2 work on a noisy ADSL?	14
6. Does the VC-based multiplexing perform better than the LLC-based multiplexing?	15
7. How do I know the details of my ADSL line statistics?	15
8. What are the signaling pins of the ADSL connector?	15
Application Notes	16
General Application Notes	16
1. Internet Access Using P-660R-Tx v2 under Bridge mode	16
2. Internet Access Using P-660R-Tx v2 under Router mode	19
Set up your workstation	20
Set up your P-660R-Tx v2	20
3. Setup the P-660R-Tx v2 as a DHCP Relay	21
4. SUA Notes	22
Configure an Internal Server Behind SUA	26
Configure a PPTP server behind SUA	27
5. Using Multi-NAT	31
Configure NAT	32
NAT Server Sets	37
6. Using the Dynamic DNS (DDNS)	45
7. Network Management Using SNMP	47
8. Using IP Alias	50
9. Using IP Policy Routing	54
10. Using Call Scheduling	58
11. Using IP Multicast	61
12. Using Zero-Configuration	61
Support Tool	65
1. LAN/WAN Packet Trace	65
Online Trace	65
Offline Trace	67
Capture the detailed logs by Hyper Terminal	68
2. Firmware/Configurations Uploading and Downloading using TFTP	70
Using TFTP client software	70
Using TFTP command on Windows NT	72
Using TFTP command on UNIX	72
3. Using FTP to Upload the Firmware and Configuration Files	73
CI Command Reference	76

FAQ

ZyNOS FAQ

1. What is ZyNOS?

ZyNOS is ZyXEL's proprietary Network Operating System. It is the platform on all Prestige routers that delivers network services and applications. It is designed in a modular fashion so it is easy for developers to add new features. New ZyNOS software upgrades can be easily downloaded from our FTP sites as they become available.

2. How do I access the P-660R-Tx v2 Command Line Interface (CLI)?

You can access the P-660R-Tx v2 Command Line Interface via telnet.

3. How do I update the firmware and configuration file?

You can upload the firmware and configuration file to P-660R-Tx v2 from Web Configurator, or using FTP/TFTP client software. You CAN NOT upload the firmware and configuration file via Telnet because the Telnet connection will be dropped during uploading the firmware. Please do not power off the router right after the FTP or TFTP uploading is finished, the router will upload the firmware to its flash at this moment.

4. How do I upgrade/backup the ZyNOS firmware by using TFTP client program via LAN?

The Prestige allows you to transfer the firmware to Prestige by using TFTP program via LAN. The procedure for uploading ZyNOS via TFTP is as follows.

- a. Use the TELNET client program in your PC to login to your Prestige.
- b. Enter CI command **'sys stdio 0'** in menu 24.8 to disable console idle timeout
- c. To upgrade firmware, use TFTP client program to put firmware in file **'ras'** in the Prestige. After data transfer is finished, the Prestige will program the upgraded firmware into FLASH ROM and reboot itself.
- d. To backup your firmware, use the TFTP client program to get file **'ras'** from the Prestige.

5. How do I restore P-660R-Tx v2 configurations by using TFTP client program via LAN?

- a. Use the TELNET client program in your PC to login to your Prestige.

- b. Enter CLI command '**sys stdio 0**' in **CLI** to disable Stdio idle timeout.
- c. To backup the configurations, use TFTP client program to get file '**rom-0**' from the Prestige.
- d. To restore the configurations, use the TFTP client program to put your configuration in file **rom-0** in the Prestige.

6. What should I do if I forget the system password?

In case you forget the system password, you can erase the current configuration and restore factory defaults this way:

Use the **RESET button** on the rear panel of P-660R-Tx v2 to reset the router. After the router is reset, the LAN IP address and the password will be reset to '**192.168.1.1**' and '**1234**'.

7. How to use the Reset button?

- a. Turn your Prestige off and then on. Make sure the **SYS** led is on (not blinking)
- b. Press the **RESET** button for one second and then release it, the P-660R-Tx v2 will reboot.
- c. Press the **RESET** button for five seconds and then release it. If the **SYS** LED begins to blink, the defaults have been restored and the Prestige restarts.

8. What is SUA? When should I use SUA?

SUA (Single User Account) is a unique feature supported by Prestige router which allows multiple people to access Internet concurrently for the cost of a single user account.

When Prestige acting as SUA receives a packet from a local client destined for the outside Internet, it replaces the source address in the IP packet header with its own address and the source port in the TCP or UDP header with another value chosen out of a local pool. It then recomputes the appropriate header checksums and forwards the packet to the Internet as if it is originated from Prestige using the IP address assigned by ISP. When reply packets from the external Internet are received by Prestige, the original IP source address and TCP/UDP source port numbers are written into the destination fields of the packet (since it is now moving in the opposite direction), the checksums are recomputed, and the packet is delivered to its true destination. This is because SUA keeps a table of the IP addresses and port numbers of the local systems currently using it.

9. What is the difference between SUA and Multi-NAT?

SUA (Single User Account) in previous ZyNOS versions is a NAT set with 2 rules, Many-to-One and Server. The P-660R-Tx v2 now has **Full Feature** NAT support to map global IP addresses to local IP addresses of clients or servers. With multiple global IP addresses, multiple servers of the same type (e.g., FTP servers) are allowed on the LAN for outside access. In previous ZyNOS versions that supported SUA 'visible' servers had to be of different types. The P-660R-Tx v2 supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The P-660R-Tx v2 supports 8 sets since there are 8 remote nodes. The default SUA (Read Only) Set in menu 15.1.255 is a convenient, pre-configured, read only, Many-to-One mapping set, sufficient for most purposes and helpful to people already familiar with SUA in previous ZyNOS versions.

10. Is it possible to access a server running behind SUA from the outside Internet? If possible, how?

Yes, it is possible because P-660R-Tx v2 delivers the packet to the local server by looking up to a SUA server table. Therefore, to make a local server accessible to the outside users, the port number and the inside IP address of the server must be configured in Web Configurator, **Advanced Setup -> NAT -> Edit NAT/SUA Server Set**.

11. When do I need Multi-NAT?

- Make local server accessible from outside Internet

When NAT is enabled the local computers are not accessible from outside. You can use Multi-NAT to make an internal server accessible from outside.

- Support Non-NAT Friendly Applications

Some servers providing Internet applications such as some mIRC servers do not allow users to login using the same IP address. Thus, users on the same network can not login to the same server simultaneously. In this case it is better to use Many-to-Many No Overload or One-to-One NAT mapping types, thus each user login to the server using a unique global IP address.

12. What IP/Port mapping does Multi-NAT support?

NAT supports five types of IP/port mapping. They are: One to One, Many to One, Many to Many Overload, Many to Many No Overload and Server. The details of the mapping between ILA and IGA are described as below. Here we define the local IP addresses as the Internal Local Addresses (ILA) and the global IP addresses as the Inside Global Address (IGA).

- **One to One**

In One-to-One mode, the P-660R-Tx v2 maps one ILA to one IGA.

- **Many to One**

In Many-to-One mode, the P-660R-Tx v2 maps multiple ILA to one IGA. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyNOS routers supported (the SUA only option in today's routers).

- **Many to Many Overload**

In Many-to-Many Overload mode, the P-660R-Tx v2 maps the multiple ILA to shared IGA.

- **Many One-to-One**

In Many One-to-One mode, the P-660R-Tx v2 maps each ILA to unique IGA.

- **Server**

In Server mode, the P-660R-Tx v2 maps multiple inside servers to one global IP address. This allows us to specify multiple servers of different types behind the NAT for outside access. Note, if you want to map each server to one unique IGA please use the One-to-One mode.

The following table summarizes these types.

NAT Type	IP Mapping
One-to-One	ILA1<--->IGA1
Many-to-One (SUA/PAT)	ILA1<--->IGA1 ILA2<--->IGA1 ...
Many-to-Many Overload	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA1 ILA4<--->IGA2 ...
Many One-to-One	ILA1<--->IGA1 ILA2<--->IGA2 ILA3<--->IGA3 ILA4<--->IGA4 ...
Server	Server 1 IP<--->IGA1 Server 2 IP<--->IGA1

13. How many network users can the SUA/NAT support?

The Prestige does not limit the number of the users but the number of the NAT sessions. The P-660R-Tx v2 supports 1024 sessions that you can use the 'ip nat session' in **CLI** to see. You can also use '**ip nat iface wanif0 st'** command to view the current active sessions.

14. What are Device filters and Protocol filters?

In ZyNOS, the filters have been separated into two groups. One group is called 'device filter group', and the other is called 'protocol filter group'. Generic filters belong to the 'device filter group', TCP/IP and IPX filters belong to the 'protocol filter group'. You can configure the filter rule in **CLI**.

Note: In ZyNOS, you can not mix different filter groups in the same filter set.

15. How can I protect against IP spoofing attacks?

The Prestige's filter sets provide a means to protect against IP spoofing attacks. The basic scheme is as follows:

For the input data filter:

- Deny packets from the outside that claim to be from the inside
- Allow everything that is not spoofing us

Filter rule setup:

- Filter type =TCP/IP Filter Rule
- Active =Yes
- Source IP Addr =a.b.c.d
- Source IP Mask =w.x.y.z
- Action Matched =Drop
- Action Not Matched =Forward

Where a.b.c.d is an IP address on your local network and w.x.y.z is your netmask:

For the output data filters:

- Deny bounceback packet
- Allow packets that originate from us

Filter rule setup:

- Filter Type =TCP/IP Filter Rule
- Active =Yes
- Destination IP Addr =a.b.c.d
- Destination IP Mask =w.x.y.z
- Action Matched =Drop
- Action No Matched =Forward

Where a.b.c.d is an IP address on your local network and w.x.y.z is your netmask.

General FAQ

1. How can I manage P-660R-Tx v2?

- Web configurator
- CLI (Command Line Interface)
- Telnet remote management
- TFTP (Trivial File Transfer Protocol) and FTP firmware upgrade and configuration backup and restore

2. What is the default password to logging web configurator?

The default password is '1234'. You can change the password when login to web configurator in the **Advanced Setup->Password**.

Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

3. How do I know the P-660R-Tx v2's WAN IP address assigned by the ISP?

You can view "**My WAN IP <from ISP> : 200.1.1.1**" shown in Web Configurator, **Maintenance -> System Status -> WAN Information** to check this IP address.

4. What is the micro filter or splitter used for?

Generally, the voice band uses the lower frequency ranging from 0 to 4KHz, while ADSL data transmission uses the higher frequency. The micro filter acts as a low-pass filter for your telephone set to ensure that ADSL transmissions do not interfere with your voice transmissions. For the details about how to connect the micro filter please refer to the user's manual.

5. The P-660R-Tx v2 supports Bridge and Router mode, what's the difference between them?

When the ISP limits some specific computers to access Internet, that means only the traffic to/from these computers will be forwarded and the other will be filtered. In this case, we use bridge mode which works as an ADSL modem to connect to the ISP. The ISP will generally give one Internet account and limit only one computer to access the Internet.

For most Internet users having multiple computers want to share an Internet account for Internet access, they have to add another Internet sharing device,

like a router. In this case, we use the router mode which works as a general Router plus an ADSL Modem.

6. How do I know I am using PPPoE?

PPPoE requires a user account to login to the provider's server. If you need to configure a user name and password on your computer to connect to the ISP you are probably using PPPoE. If you are simply connected to the Internet when you turn on your computer, you probably are not. You can also check your ISP or the information sheet given by the ISP. Please choose PPPoE as the encapsulation type in the P-660R-Tx v2 if the ISP uses PPPoE.

7. Why does my provider use PPPoE?

PPPoE emulates a familiar Dial-Up connection. It allows your ISP to provide services using their existing network configuration over the broadband connections. Besides, PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.

8. What is DDNS?

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet. To use the service, you must first apply an account from several free Web servers such as <http://www.dyndns.org/>.

Without DDNS, we always tell the users to use the WAN IP of the P-660R-Tx v2 to reach our internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the P-660R-Tx v2, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the P-660R-Tx v2.

When the ISP assigns the P-660R-Tx v2 a new IP, the P-660R-Tx v2 updates this IP to DDNS server so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

9. When do I need DDNS service?

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address we can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname. Whenever

the ISP assigns you a new IP, the P-660R-Tx v2 sends this IP to the DDNS server for its updates.

10. What is DDNS wildcard? Does the P-660R-Tx v2 support DDNS wildcard?

Some DDNS servers support the wildcard feature which allows the hostname, *.yourhost.dyndns.org, to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful when there are multiple servers inside and you want users to be able to use things such as www.yourhost.dyndns.org and still reach your hostname.

Yes, the P-660R-Tx v2 supports DDNS wildcard that <http://www.dyndns.org/> supports. When using wildcard, you simply enter yourhost.dyndns.org in the Host field in Menu 1.1 Configure Dynamic DNS.

11. Can the P-660R-Tx v2's SUA handle IPSec packets sent by the IPSec gateway?

Yes, the P-660R-Tx v2's SUA can handle IPSec ESP Tunneling mode. We know when packets go through SUA, SUA will change the source IP address and source port for the host. To pass IPSec packets, SUA must understand the ESP packet with protocol number 50, replace the source IP address of the IPSec gateway to the router's WAN IP address. However, SUA should not change the source port of the UDP packets which are used for key managements. Because the remote gateway checks this source port during connections, the port thus is not allowed to be changed.

12. How do I setup my P-660R-Tx v2 for routing IPSec packets over SUA?

For outgoing IPSec tunnels, no extra setting is required.

For forwarding the inbound IPSec ESP tunnel, A 'Default' server set in menu 15.2.1 is required. It is because SUA makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. So, to make an internal server for outside access, we must specify the service port and the LAN IP of this server in Menu 15. Thus SUA is able to forward the incoming packets to the requested service behind SUA and the outside users access the server using the P-660R-Tx v2's WAN IP address. So, we have to configure the internal IPsec as a default server (unspecified service port) in menu 15.2.1 when it acts a server gateway.

13. What is Traffic Shaping?

Traffic Shaping is a feature in the P-660R-Tx v2. It allocates the bandwidth to WAN dynamically and aims at boosting the efficiency of the bandwidth. If there are several VCs in the P-660R-Tx v2 but only one VC activated at one time, the P-660R-Tx v2 allocates all the Bandwidth to the VC and the VC gets full bandwidth. If another VCs are activated later, the bandwidth is yield to other VCs after ward.

14. What do the parameters (PCR, SCR, MBS) mean?

Traffic shaping parameters (PCR, SCR, MBS) can be set in Menu 4 and Menu 11.6 and is valid for both incoming and outgoing direction since G.shdsl is symmetric.

Peak Cell Rate(PCR): The maximum bandwidth allocated to this connection. The VC connection throughput is limited by PCR.

Sustainable Cell Rate(SCR): The least guaranteed bandwidth of a VC. When there are multi-VCs on the same line, the VC throughput is guaranteed by SCR.

Maximum Burst Size(MBS): The amount of cells transmitted through this VC at the Peak Cell Rate before yielding to other VCs. Total bandwidth of the line is dedicated to single VC if there is only one VC on the line. However, as the other VC asking the bandwidth, the MBS defines the maximum number of cells transmitted via this VC with Peak Cell rate before yielding to other VCs.

The P-660R-Tx v2 holds the parameters for shaping the traffic among its virtual channels. If you do not need traffic shaping, please set SCR = 0, MBS = 0 and PCR as the maximum value according to the line rate (for example, 2.3 Mbps line rate will result PCR as 5424 cell/sec.)

15. Why do we perform traffic shaping in the P-660R-Tx v2 ?

The P-660R-Tx v2 must manage traffic fairly and provide bandwidth allocation for different sorts of applications, such as voice, video, and data. All applications have their own natural bit rate. Large data transactions have a fluctuating natural bit rate. The P-660R-Tx v2 is able to support variable traffic among different virtual connections. Certain traffic may be discarded if the virtual connection experiences congestion. Traffic shaping defines a set of actions taken by the P-660R-Tx v2 to avoid congestion; traffic shaping takes measures to adapt to unpredictable fluctuations in traffic flows and other problems among virtual connections.

ADSL FAQ

1. How does ADSL compare to Cable modems?

ADSL provides a dedicated service over a single telephone line; cable modems offer a dedicated service over a shared media. While cable modems have greater downstream bandwidth capabilities (up to 30 Mbps), that bandwidth is shared among all users on a line, and will therefore vary, perhaps dramatically, as more users in a neighborhood get online at the same time. Cable modem upstream traffic will in many cases be slower than ADSL, either because the particular cable modem is inherently slower, or because of rate reductions caused by contention for upstream bandwidth slots. The big difference between ADSL and cable modems, however, is the number of lines available to each. There are no more than 12 million homes passed today that can support two-way cable modem transmissions, and while the figure also grows steadily, it will not catch up with telephone lines for many years. Additionally, many of the older cable networks are not capable of offering a return channel; consequently, such networks will need significant upgrading before they can offer high bandwidth services.

2. What is the expected throughput?

In our test, we can get about 1.6Mbps data rate on 15Kft using the 26AWG loop. The shorter the loop, the better the throughput. Besides, please do not stay in menu 24.1 it will slow down the throughput.

3. What is the micro filter used for?

Generally, the voice band uses the lower frequency ranging from 0 to 4KHz, while ADSL data transmission uses the higher frequency. The micro filter acts as a low-pass filter for your telephone set to ensure that ADSL transmissions do not interfere with your voice transmissions. For the details about how to connect the micro filter please refer to the user's manual.

4. How do I know the ADSL line is up?

You can see the DSL LED on the P-660R-Tx v2's front panel is green on when the ADSL physical layer is up.

5. How does the P-660R-Tx v2 work on a noisy ADSL?

Depending on the line quality, the P-660R-Tx v2 uses "Fall Back" and "Fall Forward" to automatically adjust the data rate.

6. Does the VC-based multiplexing perform better than the LLC-based multiplexing?

Though the LLC-based multiplexing can carry multiple protocols over a single VC, it requires extra header information to identify the protocol being carried on the virtual circuit (VC). The VC-based multiplexing needs a separate VC for carrying each protocol but it does not need the extra headers. Therefore, the VC-based multiplexing is more efficient.

7. How do I know the details of my ADSL line statistics?

You can use the following CLI commands to check the ADSL line statistics.

```

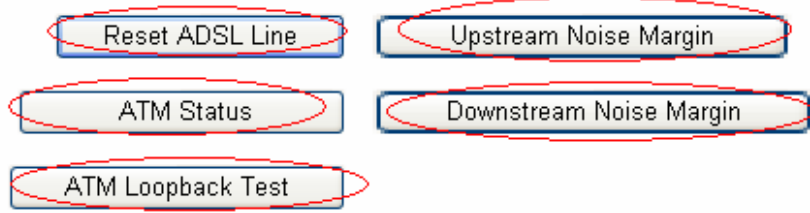
Cl> wan adsl perfdata
Cl> wan adsl status
Cl> sys log disp
Cl> wan adsl linedata far
Cl> wan adsl linedata near
    
```

You can also do it in Web Configurator, **Maintenance -> Diagnostic -> DSL Line:**

Diagnostic - DSL Line

```

noise margin downstream: 0 db
output power upstream: 0 db
attenuation downstream: 0 db
tone 0- 31: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
tone 32- 63: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
tone 64- 95: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
tone 96-127: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
tone 128-159: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
tone 160-191: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
tone 192-223: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
tone 224-255: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
tone 256-287: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
tone 288-319: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
tone 320-351: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
tone 352-383: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    
```



8. What are the signaling pins of the ADSL connector?

The signaling pins on the P-660R-Tx v2's ADSL connector are pin 3 and pin 4. The middle two pins for a RJ11 cable.

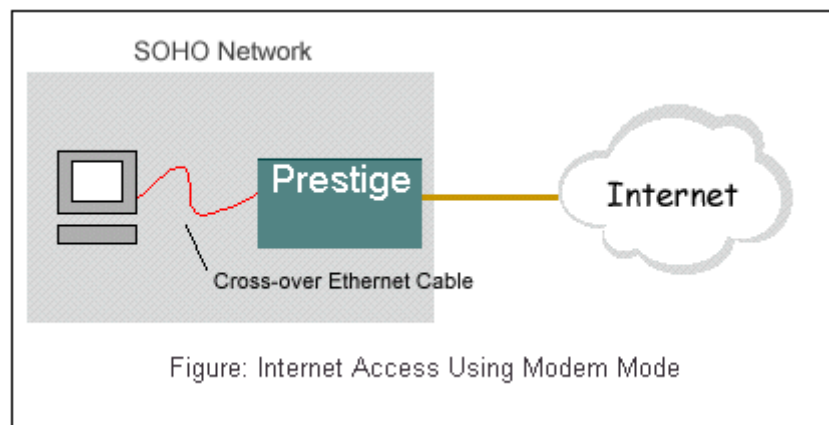
Application Notes

General Application Notes

1. Internet Access Using P-660R-Tx v2 under Bridge mode

- Setup your workstation .
- Setup your P-660R-Tx v2 under bridge mode

If the ISP limits some specific computers to access Internet, that means only the traffic to/from these computers will be forwarded and the other will be filtered. In this case, we use P-660R-Tx v2 which works as an ADSL bridge modem to connect to the ISP. The ISP will generally give one Internet account and limit only one computer to access the Internet. See the figure below for this setup.



Set up your workstation

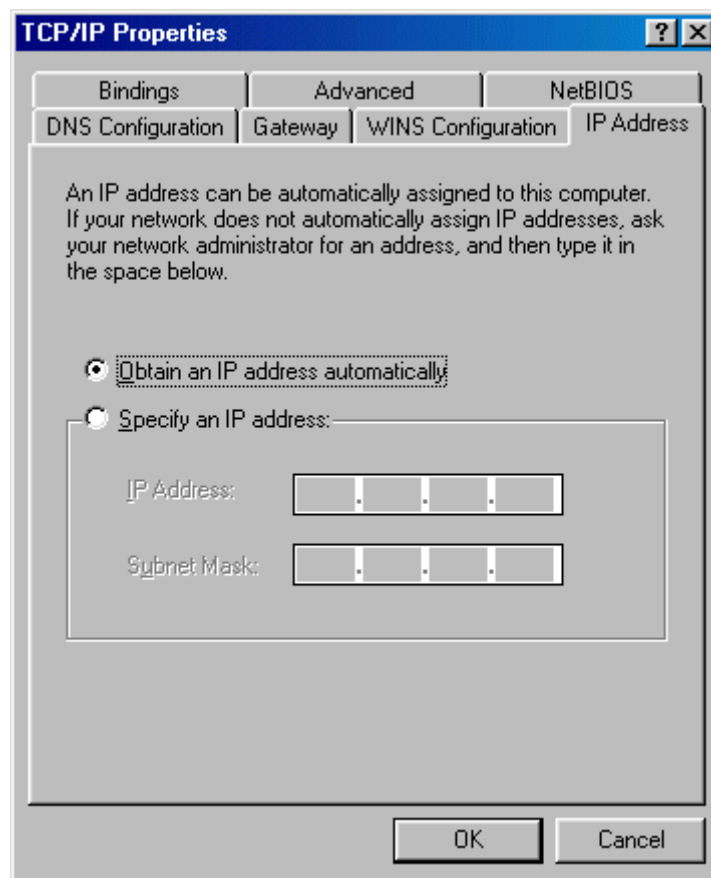
1. Ethernet connection

To connect your computer to the P-660R-Tx v2's LAN port, the computer must have an Ethernet adapter card installed. For connecting a single computer to the P-660R-Tx v2, we use a **cross-over** Ethernet cable.

2. TCP/IP configuration

In most cases, the IP address of the computer is assigned by the ISP dynamically so you have to configure the computer as a DHCP client which obtains the IP from the ISP using DHCP protocol. The ISP may also provide the gateway, DNS via DHCP if they are available. Otherwise, please enter the static IP addresses for all that the ISP gives to you in the network TCP/IP

settings. For Windows, we check the option '**Obtain an IP address automatically**' in its TCP/IP setup, please see the example shown below.



Setup your P-660R-Tx v2 under bridge mode

The following procedure shows you how to configure your P-660R-Tx v2 as an ADSL Modem for bridging traffic. We will use Web Configurator to guide you through the related menu.

(1) Configure P-660R-Tx v2 as bridge mode in **Winzard Setup -> ISP Parameters for Internet Access**.

Wizard Setup - ISP Parameters for Internet Access

Mode	Bridge
Encapsulation	Bridge
Multiplex	LLC
Virtual Circuit ID	
VPI	8
VCI	35

Next

(2) Configure a LAN IP for the P-660R-Tx v2 and turn off DHCP Server in **Advanced Setup -> LAN -> LAN Setup**. We use 192.168.1.1 in this case.

LAN - LAN Setup

DHCP	
DHCP	None
Client IP Pool Starting Address	N/A
Size of Client IP Pool	N/A
Primary DNS Server	N/A
Secondary DNS Server	N/A
Remote DHCP Server	N/A
TCP/IP	
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
RIP Direction	Both
RIP Version	RIP-2B
Multicast	IGMP-v2
Any IP Setup	
<input checked="" type="checkbox"/> Active	

(3) Configure for Internet setup parameters in **Advanced Setup -> WAN -> WAN Setup**.

WAN - WAN Setup

Name	<input type="text" value="MyISP"/>
Mode	<input type="text" value="Routing"/>
Encapsulation	<input type="text" value="ENET ENCAP"/>
Multiplex	<input type="text" value="LLC"/>
Virtual Circuit ID	
VPI	<input type="text" value="8"/>
VCI	<input type="text" value="35"/>
ATM QoS Type	<input type="text" value="UBR"/>
Cell Rate	
Peak Cell Rate	<input type="text" value="0"/> cell/sec
Sustain Cell Rate	<input type="text" value="0"/> cell/sec
Maximum Burst Size	<input type="text" value="0"/>
IP Address	
<input checked="" type="radio"/> Obtain an IP Address Automatically	
<input type="radio"/> Static IP Address	
IP Address	<input type="text" value="0.0.0.0"/>
Subnet Mask	<input type="text" value="0.0.0.0"/>
ENET ENCAP Gateway	<input type="text" value="0.0.0.0"/>
Zero Configuration	<input type="text" value="Yes"/>

Key Settings:

Option	Description
Encapsulation	Select the correct Encapsulation type that your ISP supports. For example, RFC 1483.
Multiplexing	Select the correct Multiplexing type that your ISP supports. For example, LLC.
VPI & VCI number	Specify a VPI (Virtual Path Identifier) and a VCI (Virtual Channel Identifier) given to you by your ISP.

2. Internet Access Using P-660R-Tx v2 under Router mode

For most Internet users having multiple computers want to share an Internet account for Internet access, they have to install an Internet sharing device, like a router. In this case, we use the P-660R-Tx v2 which works as a general Router plus an ADSL Modem.

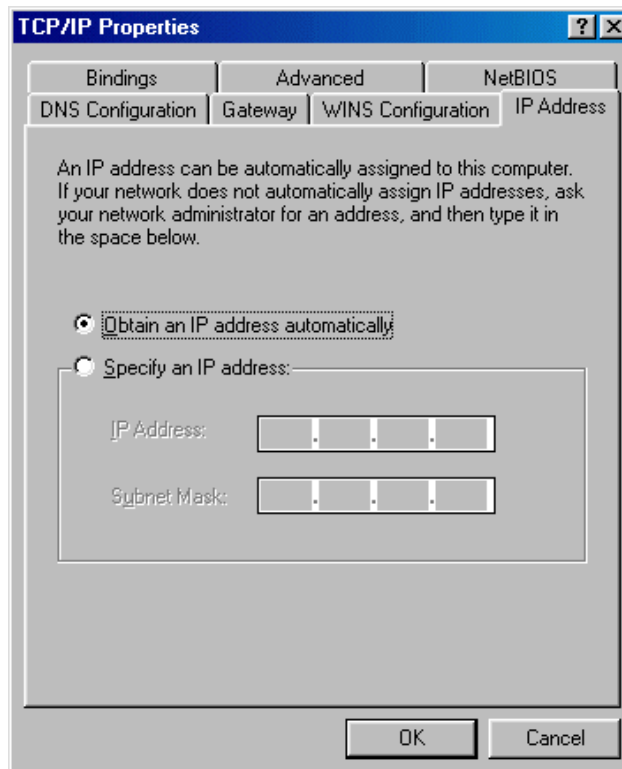
Set up your workstation

(1) Ethernet connection

Connect the LAN ports of all computers and the P-660R-Tx v2 to a HUB using a straight Ethernet cable.

(2) TCP/IP configuration

Since the P-660R-Tx v2 is set to DHCP server as default, so you need only to configure the workstations as the DHCP clients in the networking settings. In this case, the IP address of the computer is assigned by the P-660R-Tx v2. The P-660R-Tx v2 can also provide the DNS to the clients via DHCP if it is available. For this setup in Windows, we check the option '**Obtain an IP address automatically**' in its TCP/IP setup. Please see the example shown below.



Set up your P-660R-Tx v2

The following procedure shows you how to configure your P-660R-Tx v2 as Router mode for routing traffic. We will use SMT menu to guide you through the related menu. You can use console or Telnet for finishing these configurations.

(1) Configure P-660R-Tx v2 as routing mode in **Winzard Setup -> ISP Parameters for Internet Access**.

(2) Configure a LAN IP for the P-660R-Tx v2 and the DHCP settings in **Advanced Setup -> LAN -> LAN Setup**.

(3) Configure for Internet setup parameters in **Advanced Setup -> WAN -> WAN Setup**.

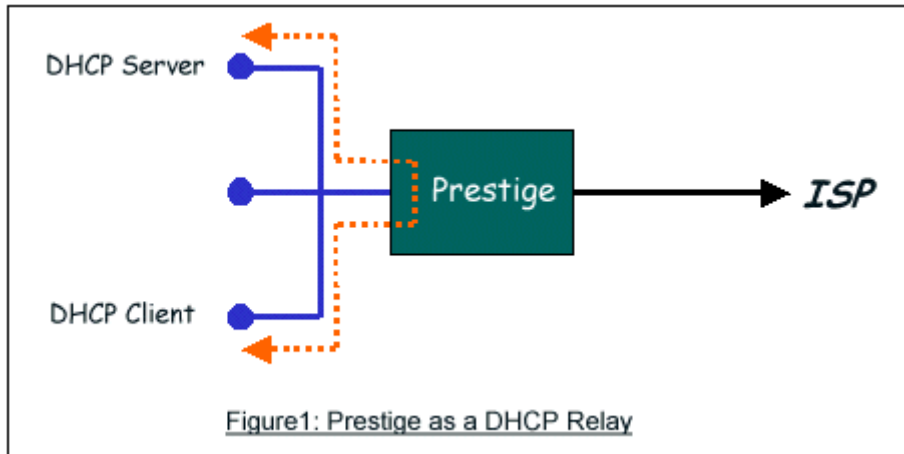
Key Settings:

Option	Description
Encapsulation	Select the correct Encapsulation type that your ISP supports. For example, RFC 1483.
Multiplexing	Select the correct Multiplexing type that your ISP supports. For example, LLC.
VPI & VCI number	Specify a VPI (Virtual Path Identifier) and a VCI (Virtual Channel Identifier) given to you by your ISP.
Network Address Translation	Set to SUA Only if you only have a single IP account for sharing with local computers.
IP Address Assignment	Set to Dynamic if the ISP provides the IP for the P-660R-Tx v2 dynamically. Otherwise, set to Static and enter the IP in the following IP Address field.
IP Address	This field can not be configured if the ISP provides the IP for the P-660R-Tx v2 dynamically. Otherwise, enter the IP that the ISP gives to you.

3. Setup the P-660R-Tx v2 as a DHCP Relay

- What is DHCP Relay?

DHCP stands for Dynamic Host Configuration Protocol. In addition to the DHCP server feature, the P-660R-Tx v2 supports the DHCP relay function. When it is configured as DHCP server, it assigns the IP addresses to the LAN clients. When it is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server. See figure 1.



- Setup the P-660R-Tx v2 as a DHCP Relay

Set the P-660R-Tx v2 to DHCP Relay in Web Configurator, Advanced Setup -> LAN -> LAN Setup and enter the IP address of the DHCP server in the **'Remote DHCP Server'** field.

LAN - LAN Setup

DHCP

DHCP	Relay
Client IP Pool Starting Address	N/A
Size of Client IP Pool	N/A
Primary DNS Server	N/A
Secondary DNS Server	N/A
Remote DHCP Server	192.168.1.2

TCP/IP

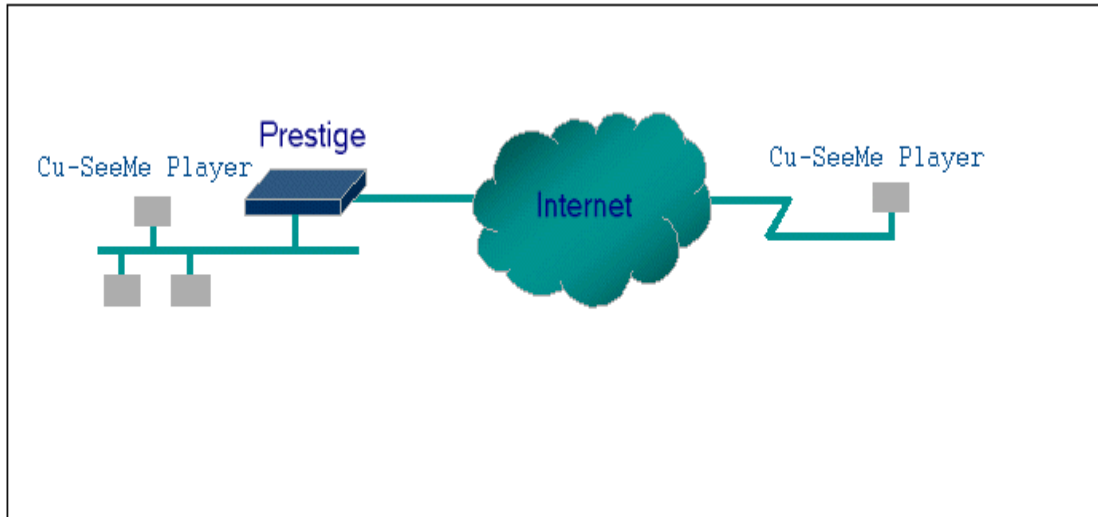
IP Address	192.168.1.1
IP Subnet Mask	255.255.255.0
RIP Direction	Both
RIP Version	RIP-2B
Multicast	IGMP-v2

Any IP Setup

Active

4. SUA Notes

Tested SUA/NAT Applications (e.g., Cu-SeeMe, ICQ, NetMeeting)



Introduction

Generally, SUA makes your LAN appear as a single machine to the outside world. LAN users are invisible to outside users. However, some applications such as Cu-SeeMe, and ICQ will need to connect to the local user behind the P-660R-Tx v2. In such case, a **SUA server** must be entered in menu 15.2.1 to forward the incoming packets to the true destination behind SUA. Generally, we do not need extra settings of menu 15.2.1 for an outgoing connection. But for some applications we need to configure Web Configurator, **Advanced Setup -> NAT ->Edit Details** to make the outgoing connection work. After the required settings are completed the internal server or client applications can be accessed by using the P-660R-Tx v2's **WAN IP** address.

SUA Supporting Table

The following are the required port forwarding settings for the various applications running SUA mode.

ZyXEL SUA Supporting Table¹

Application	Required Settings in Menu 15.2.1	
	Outgoing Connection	Incoming Connection
HTTP	None	80/client IP
FTP	None	21/client IP
TELNET	None	23/client IP (and remove Telnet filter in WAN port)
POP3	None	110/client IP
SMTP	None	25/client IP

mIRC	None for Chat. For DCC, please set Default/Client IP	
Windows PPTP	None	1723/client IP
ICQ 99a	None for Chat. For DCC, please set: ICQ -> preference -> connections -> firewall and set the firewall time out to 80 seconds in firewall setting.	Default/client IP
ICQ 2000b	None for Chat	None for Chat
ICQ Phone 2000b	None	6701/client IP
Cornell 1.1 Cu-SeeMe	None	7648/client IP
White Pine 3.1.2 Cu-SeeMe ²	7648/client IP & 24032/client IP	Default/client IP
White Pine 4.0 Cu-SeeMe	7648/client IP & 24032/client IP	Default/client IP
Microsoft NetMeeting 2.1 & 3.01 ³	None	1720/client IP 1503/client IP
Cisco IP/TV 2.0.0	None	
RealPlayer G2	None	
VDOLive	None	
Quake1.06 ⁴	None	Default/client IP
QuakeII2.30 ⁵	None	Default/client IP
QuakeIII1.05 beta	None	
StartCraft	6112/client IP	
Quick Time 4.0	None	
pcAnywhere 8.0	None	5631/client IP 5632/client IP 22/client IP
IPsec (ESP tunneling mode)	None (one client only)	Default/Client
Microsoft Messenger Service 3.0	6901/client IP	6901/client IP
Microsoft Messenger Service 4.6/ 4.7/ 5.0 (none UPnP) ⁶	None for Chat, File transfer ,Video and Voice	None for Chat, File transfer, Video and Voice
Net2Phone	None	6701/client IP

Network Time Protocol (NTP)	None	123 /server IP
Win2k Terminal Server	None	3389/server IP
Remote Anything	None	3996 - 4000/client IP
Virtual Network Computing (VNC)	None	5500/client IP 5800/client IP 5900/client IP
AIM (AOL Instant Messenger)	None for Chat and IM	None for Chat and IM
e-Donkey	None	4661 - 4662/client IP
POLYCOM Video Conferencing	None	Default/client IP
iVISTA 4.1	None	80/server IP
Microsoft Xbox Live ⁷	None	N/A

¹ Since SUA enables your LAN to appear as a single computer to the Internet, it is not possible to configure similar servers on the same LAN behind SUA.

² Because White Pine Cu-SeeMe uses dedicate ports (port 7648 & port 24032) to transmit and receive data, therefore only one local Cu-SeeMe is allowed within the same LAN.

³ In SUA mode, only one local NetMeeting user is allowed because the outsiders can not distinguish between local users using the same internet IP.

⁴ Certain Quake servers do not allow multiple users to login using the same unique IP, so only one Quake user will be allowed in this case. Moreover, when a Quake server is configured behind SUA, P-660R-Tx v2 will not be able to provide information of that server on the internet.

⁵ Quake II has the same limitations as that of Quake I.

⁶ P-660R-Tx v2 support MSN Messenger 4.6/ 4.7/ 5.0 video/ voice pass-through NAT since new firmware version. In addition, for the Windows OS supported UPnP (Universal Plug and Play), such as Windows XP and Windows ME, UPnP supported in P-660R-Tx v2 is an alternative solution to pass through MSN Messenger video/ voice traffic. For more detail, please refer to UPnP application note.

⁷ P-660R-Tx v2 support Microsoft Xbox Live since the new firmware version. If your P-660R-Tx v2 firmware is too old to support such function, you may have a work-around solution, please refer to ZyXEL website -> Support -> Xbox Live service <http://www.zyxel.com/support/xbox.htm>

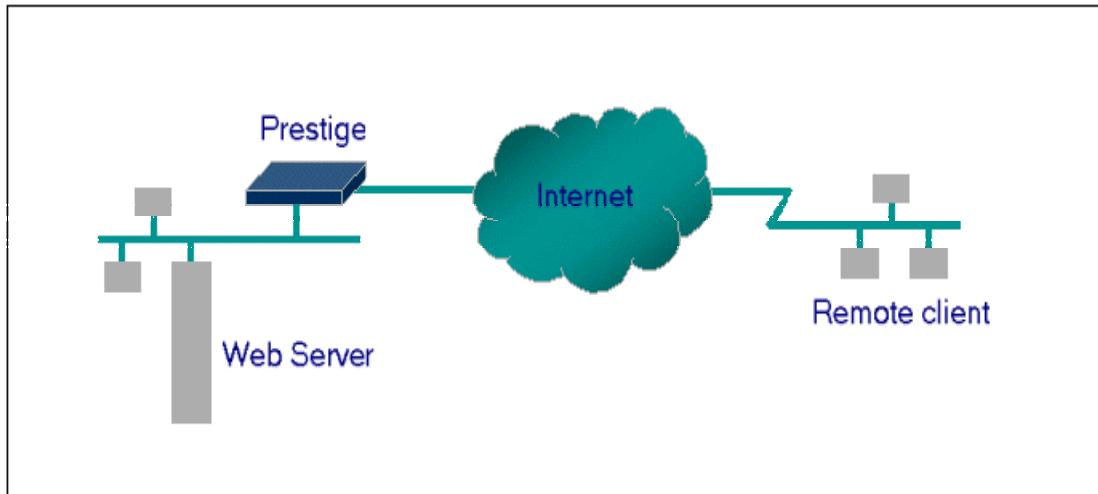
Configurations

For example, if the workstation operating Cu-SeeMe has an IP of 192.168.1.34, then the default SUA server must be set to 192.168.1.34. The peer Cu-SeeMe user can reach this workstation by using P-660R-Tx v2's **WAN IP** address which can be obtained from Web Configurator, **Maintenance -> System Status -> WAN Information**.

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	192.168.1.34

Configure an Internal Server Behind SUA



Introduction

If you wish, you can make internal servers (e.g., Web, ftp or mail server) accessible for outside users, even though SUA makes your LAN appear as a single machine to the outside world. A service is identified by the port number. Also, since you need to specify the IP address of a server in the P-660R-Tx v2, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time it is powered on.

In addition to the servers for specific services, SUA supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default server is not defined, the service request is simply discarded.

Configuration

To make a server visible to the outside world, specify the port number of the service and the inside address of the server in 'Menu 15.2.1', Multiple Server Configuration. The outside users can access the local server using the P-660R-Tx v2's **WAN IP** address which can be obtained from Web Configurator, **Maintenance -> System Status -> WAN Information**.

For example:

Configuring an internal Web server for outside access (Suppose the Server IP Address is 192.168.1.10):

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	80	80	192.168.1.10
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0

Port numbers for some services

Service	Port Number
FTP	21
Telnet	23
SMTP	25
DNS (Domain Name Server)	53
www-http (Web)	80

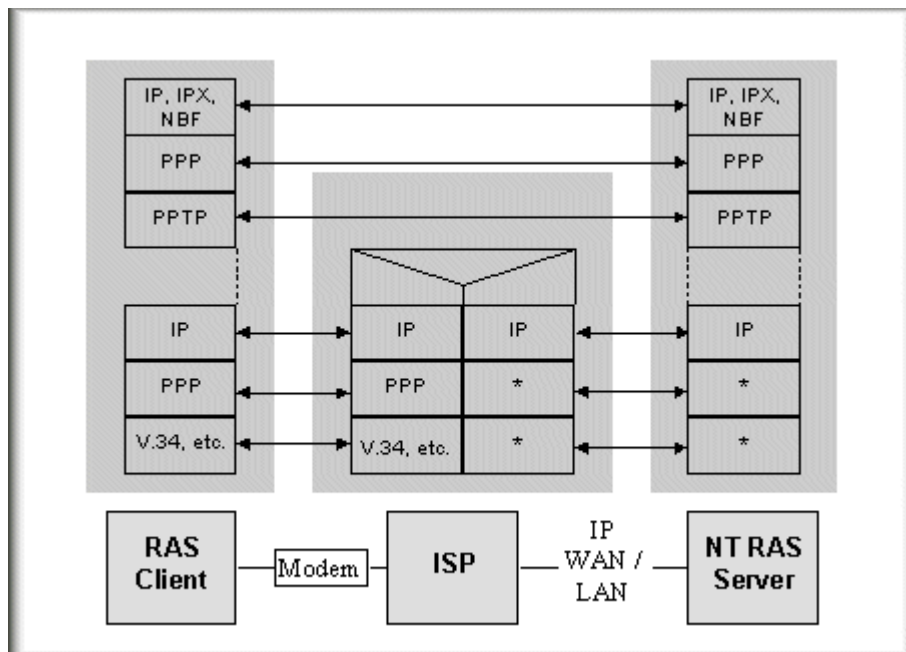
Configure a PPTP server behind SUA

Introduction

PPTP is a tunneling protocol defined by the PPTP forum that allows PPP packets to be encapsulated within Internet Protocol (IP) packets and forwarded over any IP network, including the Internet itself.

In order to run the Windows 9x PPTP client, you must be able to establish an IP connection with a tunnel server such as the Windows NT Server 4.0 Remote Access Server.

Windows Dial-Up Networking uses the Internet standard Point-to-Point (PPP) to provide a secure, optimized multiple-protocol network connection over dial-up telephone lines. All data sent over this connection can be encrypted and compressed, and multiple network level protocols (TCP/IP, NetBEUI and IPX) can be run correctly. Windows NT Domain Login level security is preserved even across the Internet.



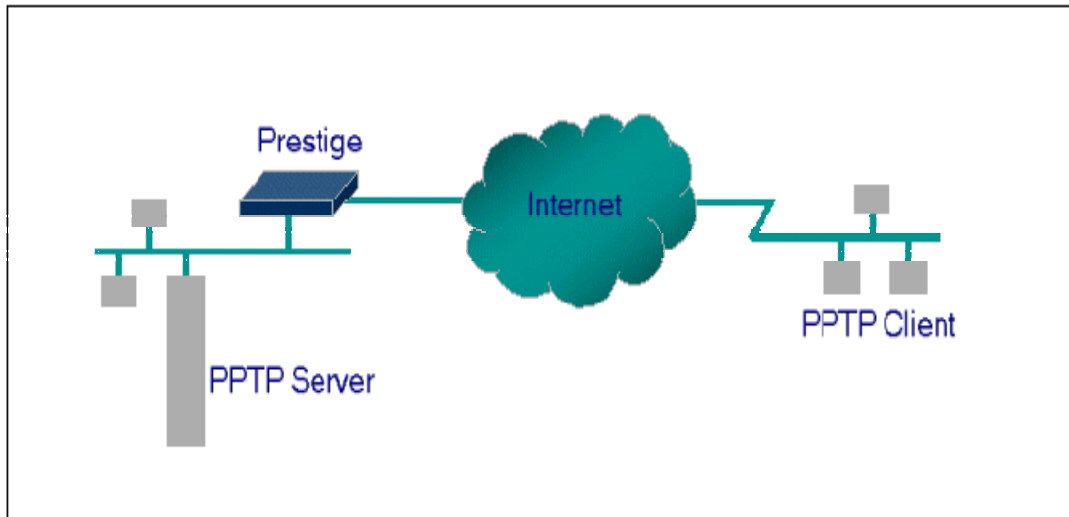
Window98 PPTP Client / Internet / NT RAS Server Protocol Stack

PPTP appears as new modem type (Virtual Private Networking Adapter) that can be selected when setting up a connection in the Dial-Up Networking folder. The VPN Adapter type does not appear elsewhere in the system. Since PPTP encapsulates its data stream in the PPP protocol, the VPN requires a second dial-up adapter. This second dial-up adapter for VPN is added during the installation phase of the Upgrade in addition to the first dial-up adapter that provides PPP support for the analog or ISDN modem.

The PPTP is supported in Windows NT and Windows 98 already. For Windows 95, it needs to be upgraded by the Dial-Up Networking 1.2 upgrade.

Configuration

This application note explains how to establish a PPTP connection with a remote private network in the P-660R-Tx v2 SUA case. In ZyNOS, all PPTP packets can be forwarded to the internal PPTP Server (WinNT server) behind SUA. The port number of the PPTP has to be entered in the Web Configurator, **Advanced Setup -> NAT -> SUA -> Edit Details** for P-660R-Tx v2 to forward to the appropriate private IP address of Windows NT server.



Example

The following example shows how to dial to an ISP via the P-660R-Tx v2 and then establish a tunnel to a private network. There will be three items that you need to set up for PPTP application, these are PPTP server (WinNT), PPTP client (Win9x) and the P-660R-Tx v2.

1. PPTP server setup (WinNT)

- Add the VPN service from Control Panel>Network
- Add an user account for PPTP logged on user
- Enable RAS port
- Select the network protocols from RAS such as IPX, TCP/IP NetBEUI
- Set the Internet gateway to P-660R-Tx v2

2. PPTP client setup (Win9x)

- Add one VPN connection from Dial-Up Networking by entering the correct username & password and the IP address of the P-660R-Tx v2's Internet IP address for logging to NT RAS server.
- Set the Internet gateway to the router that is connecting to ISP

3. P-660R-Tx v2 router setup

- Before making a VPN connection from Win9x to WinNT server, you need to connect P-660R-Tx v2 router to your ISP first.
- Enter the IP address of the PPTP server (WinNT server) and the port number for PPTP as shown below.

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	1723	1723	192.168.1.10
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0

When you have finished the above settings, you can ping to the remote Win9x client from WinNT. This ping command is used to demonstrate that remote the Win9x can be reached across the Internet. If the Internet connection between two LANs is achievable, you can place a VPN call from the remote Win9x client.

For example: C:\ping 203.66.113.2

When a dial-up connection to ISP is established, a default gateway is assigned to the router traffic through that connection. Therefore, the output below shows the default gateway of the Win9x client after the dial-up connection has been established.

Before making a VPN connection from the Win9x client to the NT server, you need to know the exact Internet IP address that the ISP assigns to P-660R-Tx

v2 router in SUA mode and enter this IP address in the VPN dial-up dialog box. You can check this Internet IP address from PNC Monitor or Web Configurator, **Maintenance -> System Status -> WAN Information**. If the Internet IP address is a fixed IP address provided by ISP in SUA mode, then you can always use this IP address for reaching the VPN server.

In the following example, the IP address '140.113.1.225' is dynamically assigned by ISP. You must enter this IP address in the 'VPN Server' dialog box for reaching the PPTP server. After the VPN link is established, you can start the network protocol application such as IP, IPX and NetBEUI.



5. Using Multi-NAT

When P-660R-Tx v2 is in Routing mode, you can select NAT Option as Full Feature in **Winzard Setup -> ISP Parameters for Internet Access**:

Wizard Setup - ISP Parameters for Internet Access

IP Address

Obtain an IP Address Automatically
 Static IP Address
 IP Address
 Subnet Mask
 ENET ENCAP Gateway

Network Address Translation

None
SUA Only
 Full Feature

Key Settings:

Field	Options	Description
Network Address Translation	Full Feature	When you select this option you can select Address Mapping Set Number 1~8 in the pull-down menu on the right.
	None	NAT is disabled when you select this option.
	SUA Only	When you select this option, this remote node will use default SUA Address Mapping Set. You can see it in CLI by command ' ip nat lookup 255 '. It's a read-only sets with two rules: Many-to-One and server mapping. Select Full Feature when you require other mapping types.

Configure NAT

Address Mapping Sets and NAT Server Sets

The P-660R-Tx v2 has 8 remote nodes and so allows you to configure 8 NAT Address Mapping Sets, You must specify which NAT Address Mapping Set (1~8) to use in the remote node when you select **Full Feature NAT**.

You can edit 10 rules for each Address Mapping Set. You can edit the rules for Address Mapping Sets #1 in Web Configurator. The other Address Mapping Sets #2~8 can only be configured in CLI (Command Line Interface).

The NAT Server Set is a list of LAN side servers mapped to external ports. We can configure it in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding**. To use the NAT server sets you've configured, a **Server** rule must be set up inside the NAT Address Mapping set. Please see NAT Server Sets for further information on how to apply it.

When you select **SUA Only**, the P-660R-Tx v2 will use a default SUA Address Mapping set for it. It has two rules: **Many-to-One** and **Server**. You can see it in **CLI** by command 'ip nat lookup 255':

```

c:\ Telnet 192.168.1.1
ras> ip nat lookup 255
NAT Lookup Information on set 255, addr = 0x9456c6f4, timer Period: 1000
rule Internal Start: Internal End: External Start: External End: sz/id/type
1 0.0.0.0 255.255.255.255 0.0.0.0 0.0.0.0 1/ 0/M1
   coneType = Port Restricted Cone (<0>)
2 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 1/ 0/SUR
   coneType = Port Restricted Cone (<0>)

Reference Count For Active Rules
Rule: 1
Rule: 2
ras>
    
```

Please note that the fields in this menu are read-only. However, the settings of the rule set 2 can be modified in Web Configurator, Advanced Setup, **Network -> NAT -> Port Forwarding**. The following table explains the fields in this above screen:

Field	Description	Option/Example
set	This is sequence number for Address Mapping Sets	255 for SUA
Internal Start IP	This is the starting local IP address (ILA).	0.0.0.0 for the Many-to-One type.
Local End IP	This is the starting 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.	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	This is the NAT mapping types.	Many-to-One and Server

Here we'll guide you to configure Address Mapping Sets from **Web Configurator** and **CLI**. (Since in **Web Configurator** we can only edit the rules

for Address Mapping Sets #1. The other Address Mapping Sets #2~8 can only be configured in CLI)

- **Now let's begin with Web Configurator:**

Firstly let's come to Web Configurator, Advanced Setup, **Network -> NAT -> Full Feature -> Edit Details -> Address Mapping Rules:**

NAT - Mode

Network Address Translation

None
 SUA Only [Edit Details](#)
 Full Feature [Edit Details](#)

NAT - Address Mapping Rules

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

This menu is for Address Mapping Set #1, you can edit 10 Address Mapping Rules for Set #1. You can edit or remove a rule by clicking the 'Rule #' in the rule table.

Click the 'Rule1', you can enter the page on which you can edit an individual rule and configure the Mapping Type, Local and Global Start/End IPs:

NAT - Edit Address Mapping Rule 1

Type	One-to-One
Local Start IP	0.0.0.0
Local End IP	N/A
Global Start IP	0.0.0.0
Global End IP	N/A
Server Mapping Set	N/A Edit Details

The following table describes the fields in this screen.

Field	Description	Option/Example
Type	You can select one of the five mapping types from the pull-down menu	1. One-to-One 2. Many-to-One 3. Many-to-Many Overload 4. Many-to-Many No Overload 5. Server
Local IP	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 type. 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 Start IP . 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. 200.1.1.64

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.

- **Configure Address Mapping Sets in CLI**

Setp 1: Telnet to the P-660R-Tx v2. (We suppose the LAN IP Address of P-660R-Tx v2 is 192.168.1.1)

Step 2: Select one Address Mapping Set (#1~#8) by command ‘**ip nat addrmap map [map #] [set name]**’ (set name is optional). Suppose we configure set 2 in the example.

Setp 3: Set NAT address mapping rule for the Address Mapping Set you just configured (Set 2 in this example) by command ‘**ip nat addrmap rule [rule#] [insert | edit] [type] [local start IP] [local end IP] [global start IP] [global end IP] [server set #]**’. Suppose we set a Many-to-One rule for set 2 by command ‘**ip nat addrmap rule 1 edit 1 192.168.1.10 192.168.1.20 172.1.1.1 172.1.1.1**’

Setp 4: Save the configuration by command ‘**ip nat addrmap save**’. You can apply the Address Mapping Set 2 to remote nodes in Web Configurator when you select Full Feature NAT. See the intire process as follows:

```

ras> ip nat addrmap map 2 Test
ras> ip nat addrmap rule 1 edit 1 192.168.1.10 192.168.1.20 172.1.1.1 172.1.1.1
CONFIG NAT Address MAP set:2 rule:1
ras> ip nat addrmap save
ip nat addrmap: save ok
    
```

Set 5: You can lookup the successfully configured Address Mapping Sets by command ‘**ip nat addrmap disp**’

```

ras> ip nat addrmap disp
Set Number: 2
Set Name: dis
  Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
-----
  1.  192.168.1.10    192.168.1.20  172.1.1.1       172.1.1.1     M-1
ras>
    
```

Key Settings:

CI Command	Description
ip nat addrmap map [map#] [set name]	Select NAT address mapping set and set mapping set name, but set name is optional Example: > ip nat addrmap map 2 Test
ip nat addrmap rule [rule#] [insert edit] [type] [local start IP] [local end IP] [global start IP] [global end IP] [server set #]	Set NAT address mapping rule. If the “type” is not “inside-server” then the “type” field will still need a dummy value like “0”. Type is 0 - 4 = one-to-one, many-to-one, many-to-many-overload, many-to-many-non overload, inside-server Example: > ip nat addrmap rule 1 edit 3 192.168.1.10 192.168.1.20 172.1.1.1 172.1.1.1
ip nat addrmap clear [map#] [rule#]	Clear the selected rule of the set
ip nat addrmap freememory	Discard Changes

ip nat addrmap disp	Display nat set information
ip nat addrmap save	Save settings
ip nat server load [set#]	Load the server sets of NAT into buffer
ip nat server disp [1]	“disp 1” means to display the NAT server set in buffer, if parameter “1” is omitted, then it will display all the server sets
ip nat server save	Save the NAT server set buffer into flash
ip nat server clear [set#]	Clear the server set [set#], must use “save” command to let it save into flash
ip nat server edit [rule#] active	Activate the rule [rule#], rule number is 1 to 24, the number 25-36 is for UPNP application
ip nat server edit [rule#] svrport <start port> <end port>	Configure the port range from <start port > to <end port>
ip nat server edit [rule#] remotehost <start IP> <end IP>	Configure the IP address range of remote host (Leave it to be default value if you don't need this command)
ip nat server edit [rule#] leasetime <seconds>	Configure the lease time (Leave it to be default value if you don't want this command)
ip nat server edit [rule#] rulename <string>	Configure the name of the rule (Leave it to be default value if you don't want this command)
ip nat server edit [rule#] forwardip <IP address>	Configure the LAN IP address to be forwarded
ip nat server edit [rule#] protocol <TCP UDP ALL>	Configure the protocol to be used TCP , UDP or ALL (it must be capital)

NAT Server Sets

The NAT Server Set is a list of LAN side servers mapped to external ports (similar to the old SUA menu of before). 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 network appears as a single machine to the outside world. A server 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 a FTP server at 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.

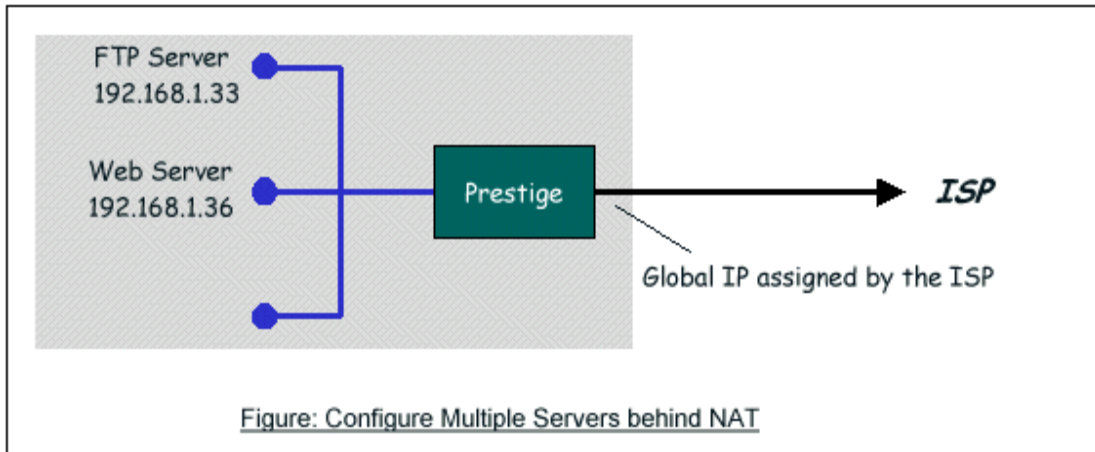


Figure: Configure Multiple Servers behind NAT

Please note that a server can support more than one service, e.g., a server can provide both FTP and Mail service, while another provides only Web service.

The following procedures show how to configure a server behind NAT.

Step 1: Login Web Configurator, Advanced Setup, NAT -> Edit Details -> Port Forwarding.

Step 2: Fill in the service port and Internal Server IP Address in the table, and click button 'Save' to save it.

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	80	80	192.168.1.36
3	20	21	192.168.1.33
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0

Save Cancel

The most often used port numbers are shown in the following table. Please refer RFC 1700 for further information about port numbers.

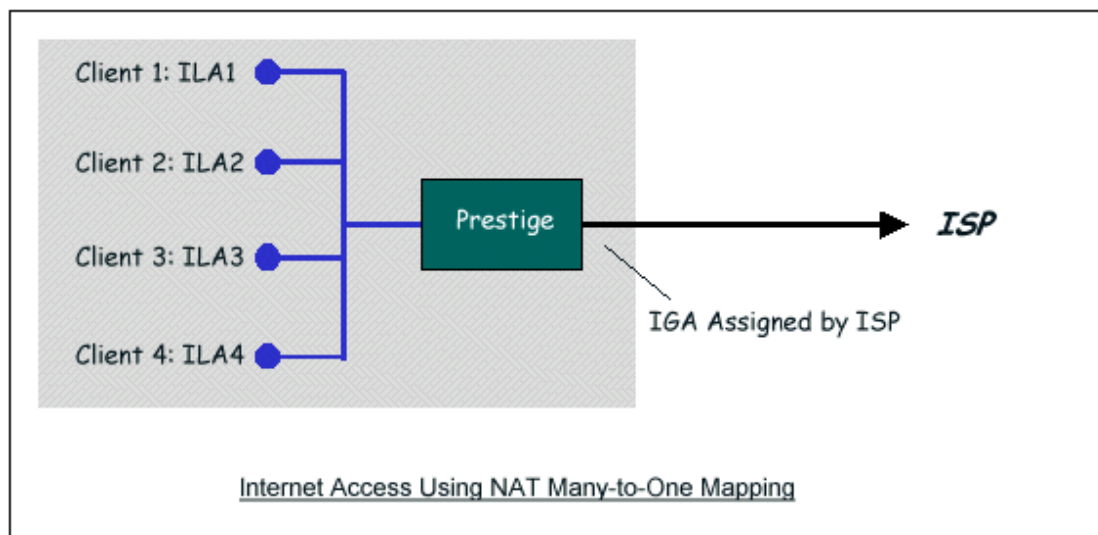
Service	Port Number
FTP	21
Telnet	23
SMTP	25
DNS (Domain Name Server)	53
www-http (Web)	80
PPTP (Point-to-Point Tunneling Protocol)	1723

- **Examples**

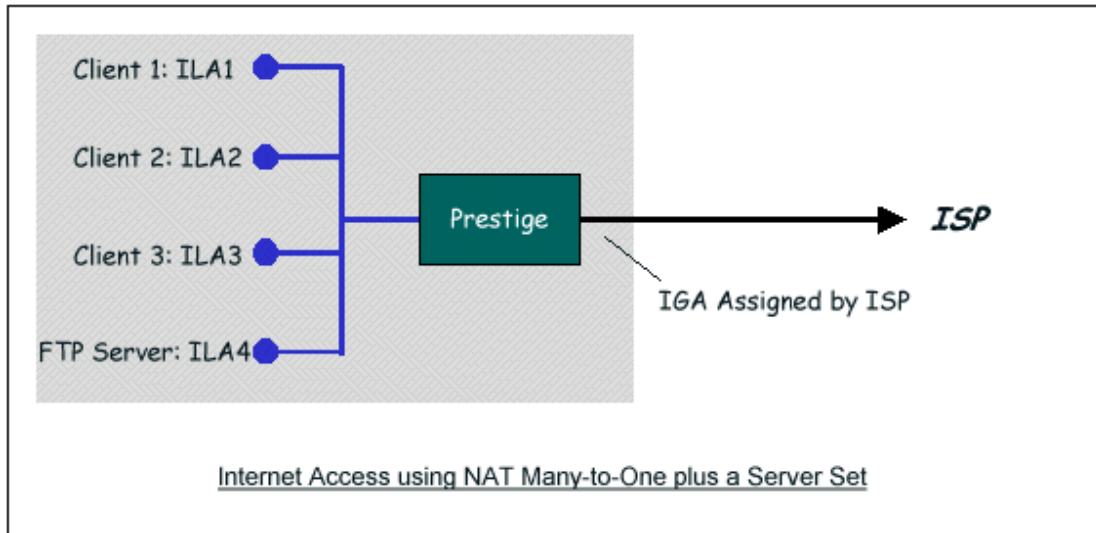
- Internet Access Only
- Internet Access with an Internal Server
- Using Multiple Global IP addresses for clients and servers
- Support Non NAT Friendly Applications

(1) Internet Access Only

In our Internet Access example, we only need one rule where all our ILAs map to one IGA assigned by the ISP. You can just use the default **SUA NAT**, or you could select **Full Feature NAT** and select an Address Mapping Set with a **Many-to-One** Rule. See the following figure.



(2) Internet Access with an Internal Server



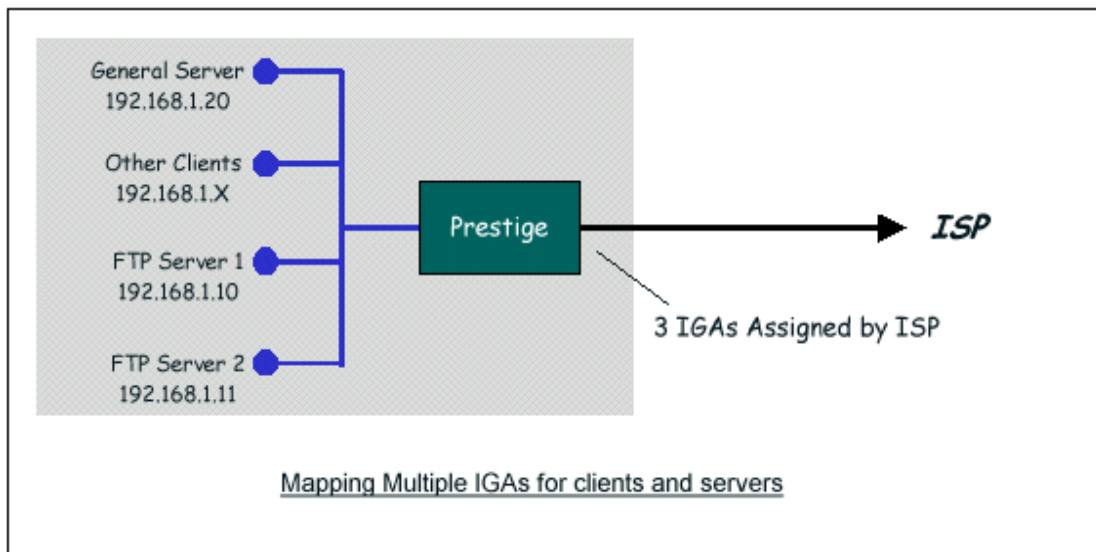
In this case, we do exactly as the figure (use the convenient pre-configured SUA Only set) and also go to Web Configurator, **Network -> NAT -> SUA Only -> Edit Details -> Edit SUA/NAT Server Set** to specify the Internet Server behind the NAT as below:

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	20	21	192.168.1.33
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0

Save Cancel

**(3) Using Multiple Global IP addresses for clients and servers
(One-to-One, Many-to-One, Server Set mapping types are used)**



In this case we have 3 IGAs from the ISP. We have two very busy internal FTP servers and also an internal general server for the web and mail. In this case, we want to assign the 3 IGAs by the following way using 4 NAT rules.

- Rule 1 (One-to-One type) to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1 (200.0.0.1).
- Rule 2 (One-to-One type) to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.0.0.2).
- Rule 3 (Many-to-One type) to map the other clients to IGA3 (200.0.0.3).
- Rule 4 (Server type) to map a web server and mail server with ILA3 (192.168.1.20) to IGA3. Type **Server** allows us to specify multiple servers, of different types, to other machines behind NAT on the LAN.

Step 1: In this case, we need to map ILA to more than one IGA, therefore we must choose the **Full Feature** option from the **NAT** field in currently active remote node, and assign IGA3 to P-660R-Tx v2's WAN IP Address.

IP Address

- Obtain an IP Address Automatically
- Static IP Address

IP Address	200.0.0.3
Subnet Mask	255.255.255.0
ENET ENCAP Gateway	200.0.0.254
Zero Configuration	No

Step 2: Go to Web Configurator, Advanced Setup, **NAT -> Full Feature -> Edit Details** to begin configuring Address Mapping Set #1. We can see there are 10 blank rule table that could be configured. See the following setup for the four rules in our case.

Rule 1 Setup: Select **One-to-One** type to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1 (200.0.0.1).

NAT - Edit Address Mapping Rule 1

Type	One-to-One
Local Start IP	192.168.1.10
Local End IP	N/A
Global Start IP	200.0.0.1
Global End IP	N/A
Server Mapping Set	N/A Edit Details

Rule 2 Setup: Selecting **One-to-One** type to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.0.0.2).

NAT - Edit Address Mapping Rule 2

Type	One-to-One
Local Start IP	192.168.1.11
Local End IP	N/A
Global Start IP	200.0.0.2
Global End IP	N/A
Server Mapping Set	N/A Edit Details

Rule 3 Setup: Select **Many-to-One** type to map the other clients to IGA3 (200.0.0.3).

NAT - Edit Address Mapping Rule 3

Type	Many-to-One
Local Start IP	0.0.0.0
Local End IP	255.255.255.255
Global Start IP	200.0.0.3
Global End IP	N/A
Server Mapping Set	N/A Edit Details

Rule 4 Setup: Select **Server** type to map our web server and mail server with ILA3 (192.168.1.20) to IGA3.

NAT - Edit Address Mapping Rule 4

Type	Server
Local Start IP	N/A
Local End IP	N/A
Global Start IP	200.0.0.3
Global End IP	N/A
Server Mapping Set	2 Edit Details

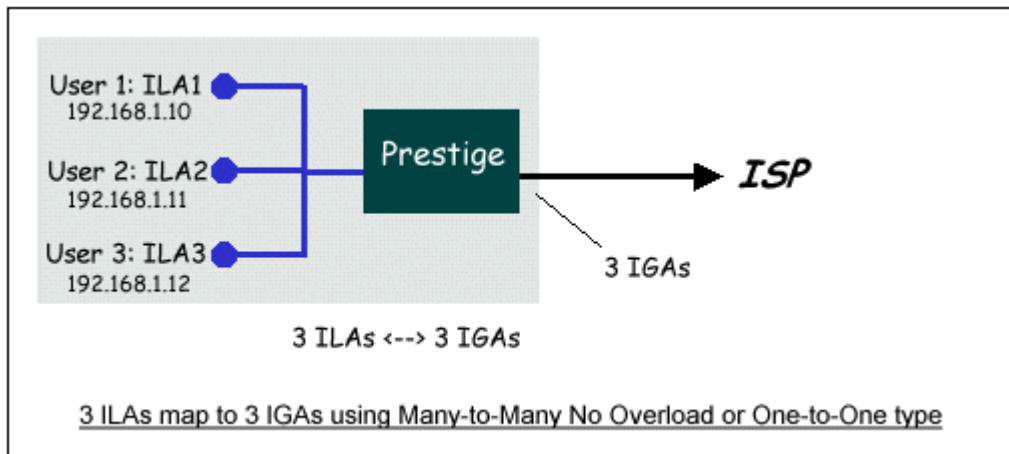
Step 3: Now we configure all other incoming traffic to go to our web server and mail server from Web Configurator, **Advanced Setup -> NAT -> Full Feature -> Rule 4 -> Server Mapping Set -> Edit Details.**

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	80	80	192.168.1.20
3	20	21	192.168.1.20
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0

(4) Support Non NAT Friendly Applications

Some servers providing Internet applications such as some mIRC servers do not allow users to login using the same IP address. In this case it is better to use Many-to-Many No Overload or One-to-One NAT mapping types, thus each user login to the server using a unique global IP address. The following figure illustrates this.



One rule configured for using **Many-to-Many No Overload** mapping type is shown below.

NAT - Edit Address Mapping Rule 5

Type	Many-to-Many No Overload <input type="button" value="v"/>
Local Start IP	192.168.1.10
Local End IP	192.168.1.12
Global Start IP	200.0.0.10
Global End IP	200.0.0.12
Server Mapping Set	N/A <input type="button" value="v"/> Edit Details

We can also do this by configure three **One-to-One** mapping type rules.

6. Using the Dynamic DNS (DDNS)

- What is DDNS?

The DDNS service, an IP Registry provides a public central database where information such as email addresses, hostnames, IPs etc. can be stored and

retrieved. This solves the problems if your DNS server uses an IP associated with dynamic IPs.

Without DDNS, we always tell the users to use the WAN IP of the P-660R-Tx v2 to access the internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the P-660R-Tx v2, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the P-660R-Tx v2.

When the ISP assigns the P-660R-Tx v2 a new IP, the P-660R-Tx v2 must inform the DDNS server the change of this IP so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS name for your web server (i.e., www.zyxel.com.tw) is still usable.

The DDNS servers the P-660R-Tx v2 supports currently is WWW.DYNDNS.ORG where you apply the DNS from and update the WAN IP to.

- Setup the DDNS
 1. Before configuring the DDNS settings in the P-660R-Tx v2, you must register an account from the DDNS server such as WWW.DYNDNS.ORG first. After the registration, you have a hostname for your internal server and a password using to update the IP to the DDNS server.
 2. Login Web Configurator, **Advanced Setup -> Dynamic DNS**, Select **'Active Dynamic DNS'** option:

Dynamic DNS

<input checked="" type="checkbox"/> Active	
Service Provider	WWW.DynDNS.ORG
Host Name	<input type="text"/>
E-mail Address	<input type="text"/>
User	<input type="text"/>
Password	<input type="text"/>
<input type="checkbox"/> Enable Wildcard	

Key Settings:

Option	Description
Service Provider	Enter the DDNS server in this field. Currently, we support WWW.DYNDNS.ORG.
Active	Toggle to 'Yes'.
Host Name	Enter the hostname you subscribe from the above DDNS server. For example, zyxel.com.tw.
User Name	Enter the user name that the DDNS server gives to you.
Password	Enter the password that the DDNS server gives to you.
Enable Wildcard	Enter the hostname for the wildcard function that the WWW.DYNDNS.ORG supports. Note that Wildcard option is available only when the provider is http://www.dyndns.org/ .

7. Network Management Using SNMP

- ZyXEL SNMP Implementation

ZyXEL currently includes SNMP support in some P-660R-Tx v2 routers. It is implemented based on the SNMPv1, so it will be able to communicate with SNMPv1 NMSs. Further, users can also add ZyXEL's private MIB in the NMS to monitor and control additional system variables. The ZyXEL's private MIB tree is shown in figure 3. For SNMPv1 operation, ZyXEL permits one community string so that the router can belong to only one community and allows trap messages to be sent to only one NMS manager.

Some traps are sent to the SNMP manager when anyone of the following events happens:

1. coldStart (defined in RFC-1215) :

If the machine coldstarts, the trap will be sent after booting.

2. warmStart (defined in RFC-1215) :

If the machine warmstarts, the trap will be sent after booting.

3. linkDown (defined in RFC-1215) :

If any link of IDSL or WAN is down, the trap will be sent with the port number . The port number is its interface index under the interface group.

4. linkUp (defined in RFC-1215) :

If any link of IDSL or WAN is up, the trap will be sent with the port number . The port number is its interface index under the interface group.

5. authenticationFailure (defined in RFC-1215) :

When receiving any SNMP get or set requirement with wrong community, this trap is sent to the manager.

6. whyReboot (defined in ZYXEL-MIB) :

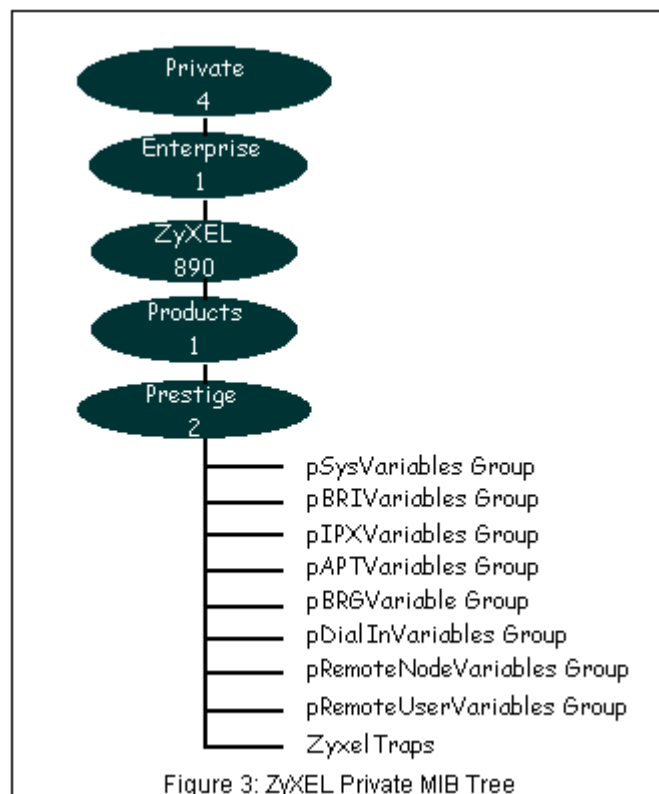
When the system is going to restart (warmstart), the trap will be sent with the reason of restart before rebooting.

(1) For intentional reboot:

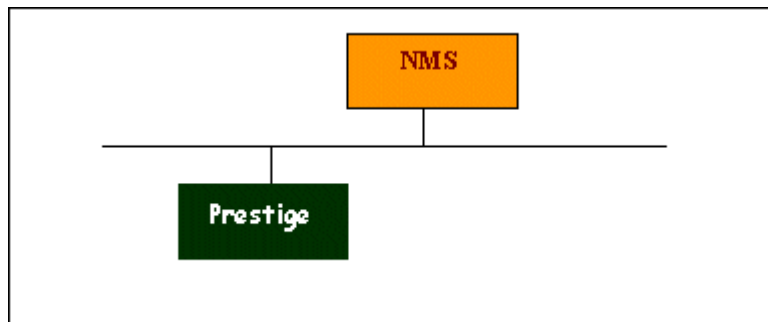
In some cases (download new files, CLI command "sys reboot",), reboot is done intentionally. And traps with the message "System reboot by user !" will be sent.

(2) For fatal error:

System has to reboot for some fatal errors. And traps with the message of the fatal code will be sent.



- Downloading ZyXEL's private MIB
- Configure the P-660R-Tx v2 for SNMP



The SNMP related settings in P-660R-Tx v2 are configured in **CLI**. The following steps describe a simple setup procedure for configuring all SNMP settings.

(1) Configure the trusted host via command:

sys snmp trusthost <IP Address>

```

c:\ Telnet 192.168.1.1
P-660R-T1> sys snmp trusthost 192.168.1.33
P-660R-T1>

```

(2) Configure the Get community and Set community via command:

sys snmp get <community>

sys snmp set <community>

```

c:\ Telnet 192.168.1.1
P-660R-T1> sys snmp trusthost 192.168.1.33
P-660R-T1> sys snmp get Test
P-660R-T1> sys snmp set Test
P-660R-T1>

```

(3) Configure the Trap community via command:

sys snmp trap community <community>

```

c:\ Telnet 192.168.1.1
P-660R-T1> sys snmp trusthost 192.168.1.33
P-660R-T1> sys snmp get Test
P-660R-T1> sys snmp set Test
P-660R-T1> sys snmp trap community Test
P-660R-T1>

```

(4) Configure the Trap Destination IP via command:

sys snmp trap destination <IP Address>

```

C:\ Telnet 192.168.1.1
P-660R-T1> sys snmp trusthost 192.168.1.33
P-660R-T1> sys snmp get Test
P-660R-T1> sys snmp set Test
P-660R-T1> sys snmp trap community Test
P-660R-T1> sys snmp trap destination 192.168.1.33
P-660R-T1>
    
```

(5) Save the configuration via command:

sys snmp save

```

C:\ Telnet 192.168.1.1
P-660R-T1> sys snmp trusthost 192.168.1.33
P-660R-T1> sys snmp get Test
P-660R-T1> sys snmp set Test
P-660R-T1> sys snmp trap community Test
P-660R-T1> sys snmp trap destination 192.168.1.33
P-660R-T1> sys snmp save
sys snmp: save ok
P-660R-T1> _
    
```

Key Settings:

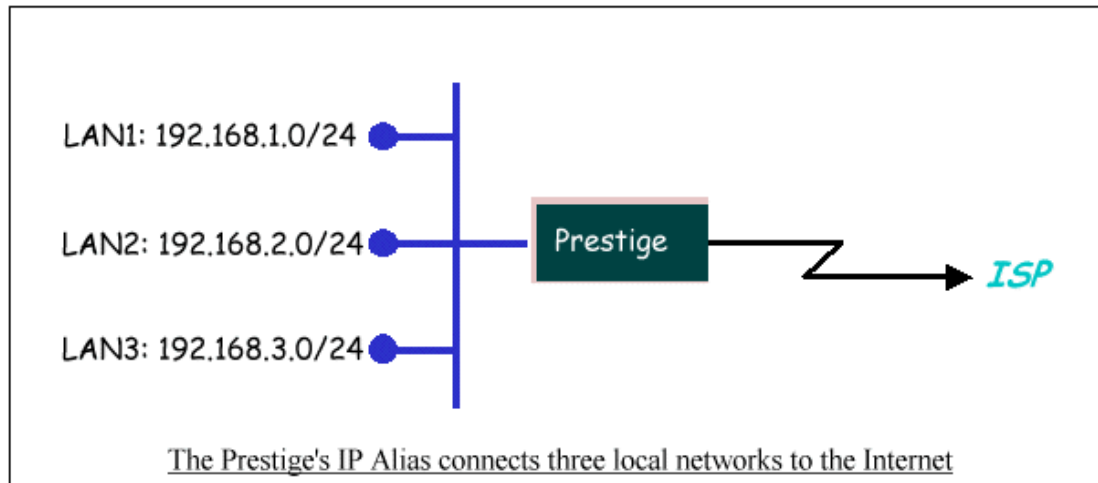
Option	Descriptions
Get Community	Enter the correct Get Community. This Get Community must match the 'Get-' and 'GetNext' community requested from the NMS. The default is 'public'.
Set Community	Enter the correct Set Community. This Set Community must match the 'Set-community requested from the NMS. The default is 'public'.
Trusted Host	Enter the IP address of the NMS. The P-660R-Tx v2 will only respond to SNMP messages coming from this IP address. If 0.0.0.0 is entered, the P-660R-Tx v2 will respond to all NMS managers.
Trap Community	Enter the community name in each sent trap to the NMS. This Trap Community must match what the NMS is expecting. The default is 'public'.
Trap Destination	Enter the IP address of the NMS that you wish to send the traps to. If 0.0.0.0 is entered, the P-660R-Tx v2 will not send trap any NMS manager.

8. Using IP Alias

- What is IP Alias?

In a typical environment, a LAN router is required to connect two local networks. The P-660R-Tx v2 can connect three local networks to the ISP or a remote node, we call this function as '**IP Alias**'. In this case, an internal router is not required. For example, the network manager can divide the local

network into three networks and connect them to the Internet using P-660R-Tx v2's single user account. See the figure below.



The P-660R-Tx v2 supports three virtual LAN interfaces via its single physical Ethernet interface. The first network can be configured in Web Configurator, **Advanced Setup -> LAN -> LAN Setup** as usual. The second and third networks that we call '**IP Alias 1**' and '**IP Alias 2**' can be configured **CLI (Command Line Interface)**.

There are three internal virtual LAN interfaces for the P-660R-Tx v2 to route the packets from/to the three networks correctly. They are **enif0** for the major network, **enif0:0** for the IP alias 1 and **enif0:1** for the IP alias 2. Therefore, three routes are created in the P-660R-Tx v2 as shown below when the three networks are configured. If the P-660R-Tx v2's DHCP is also enabled, the IP pool for the clients can be any of the three networks.

```

Telnet 192.168.1.1
ras> ip ro s
Dest          FF Len Device      Gateway      Metric stat Timer  Use
200.0.0.0    00 24 Idle        200.0.0.3   2    002b 0    0
192.168.1.0  00 24 enet0      192.168.1.1 1    041b 0    93
192.168.2.0  00 24 enet0      192.168.2.1 1    041b 0    0
192.168.3.0  00 24 enet0      192.168.3.1 1    041b 0    0
ras> ip if
enif0: mtu 1500
  inet 192.168.1.1, netmask 0xfffff00, broadcast 192.168.1.255
  RIP RX:None, TX:None,
  [InOctets      505058] [InUnicast      2339] [InMulticast    3220]
  [InDiscards    0] [InErrors        0] [InUnknownProtos 0]
  [OutOctets     1062338] [OutUnicast     2609] [OutMulticast   218]
  [OutDiscards   0] [OutErrors        0]
enif0:0: mtu 1500
  inet 192.168.2.1, netmask 0xfffff00, broadcast 192.168.2.255
  RIP RX:None, TX:None,
  [InOctets      0] [InUnicast      0] [InMulticast    0]
  [InDiscards    0] [InErrors        0] [InUnknownProtos 0]
  [OutOctets     0] [OutUnicast     0] [OutMulticast   0]
  [OutDiscards   0] [OutErrors        0]
enif0:1: mtu 1500
  inet 192.168.3.1, netmask 0xfffff00, broadcast 192.168.3.255
  RIP RX:None, TX:None,
  [InOctets      0] [InUnicast      0] [InMulticast    0]
  [InDiscards    0] [InErrors        0] [InUnknownProtos 0]

```

You can edit filter rule to accept or deny LAN packets from/to the IP alias 1/2 go through the P-660R-Tx v2 by command in **CLI**:

lan index [index number]

Usage: index number = 1 main LAN

2 IP Alias#1

3 IP Alias#2

lan filter <incoming|outgoing> <tcpip|generic> [set#]

Usage: set# = the corresponding filter set number you've configured

lan save

Don't forget to save the configuration.

- IP Alias Setup

(1) Telnet to access the **CLI** of the P-660R-Tx v2, select an IP Alias interface to begin via command:

lan index [index number]

Usage: index number = 2 IP Alias#1

3 IP Alias#2

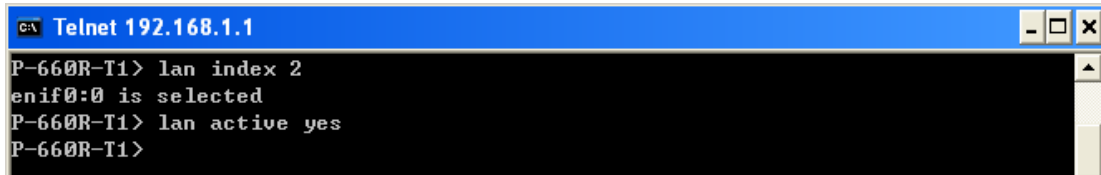
```

Telnet 192.168.1.1
P-660R-T1> lan index 2
enif0:0 is selected
P-660R-T1> _

```

(2) Active this IP Alias Interface via command:

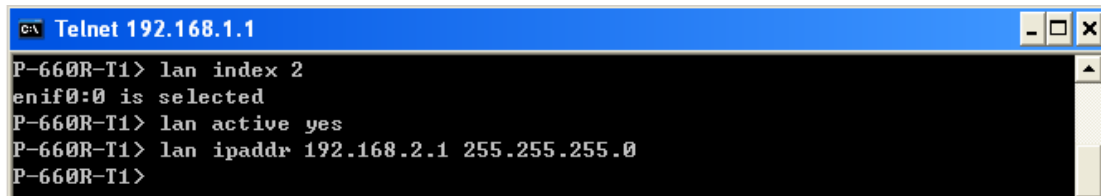
lan active yes



```
C:\ Telnet 192.168.1.1
P-660R-T1> lan index 2
enif0:0 is selected
P-660R-T1> lan active yes
P-660R-T1>
```

(3) Setup the Alias Interface IP Address vis command:

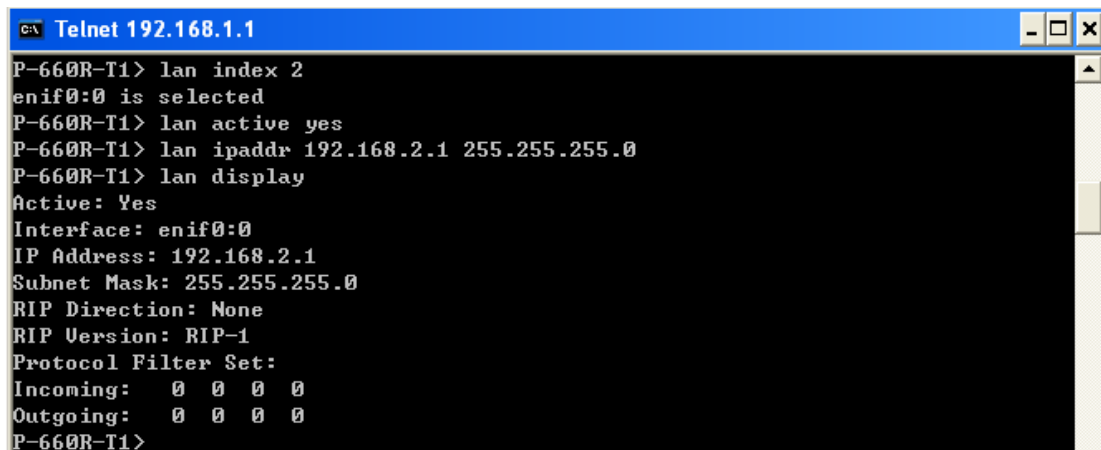
lan ipaddr <IP Addr> <Mask>



```
C:\ Telnet 192.168.1.1
P-660R-T1> lan index 2
enif0:0 is selected
P-660R-T1> lan active yes
P-660R-T1> lan ipaddr 192.168.2.1 255.255.255.0
P-660R-T1>
```

(4) Check the current configuration via command:

lan display



```
C:\ Telnet 192.168.1.1
P-660R-T1> lan index 2
enif0:0 is selected
P-660R-T1> lan active yes
P-660R-T1> lan ipaddr 192.168.2.1 255.255.255.0
P-660R-T1> lan display
Active: Yes
Interface: enif0:0
IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0
RIP Direction: None
RIP Version: RIP-1
Protocol Filter Set:
Incoming:  0 0 0 0
Outgoing:  0 0 0 0
P-660R-T1>
```

(5) Save the configuration via command:

lan save

```

Telnet 192.168.1.1
P-660R-T1> lan index 2
enif0:0 is selected
P-660R-T1> lan active yes
P-660R-T1> lan ipaddr 192.168.2.1 255.255.255.0
P-660R-T1> lan display
Active: Yes
Interface: enif0:0
IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0
RIP Direction: None
RIP Version: RIP-1
Protocol Filter Set:
Incoming:  0 0 0 0
Outgoing:  0 0 0 0
P-660R-T1> lan save
lan: save ok
P-660R-T1>

```

(6) When we finished the configure we could see an route entry for Alias Interface has been added to route table. We can check via command:

ip route status

We can also see the iface information via command:

ip ifconfig

```

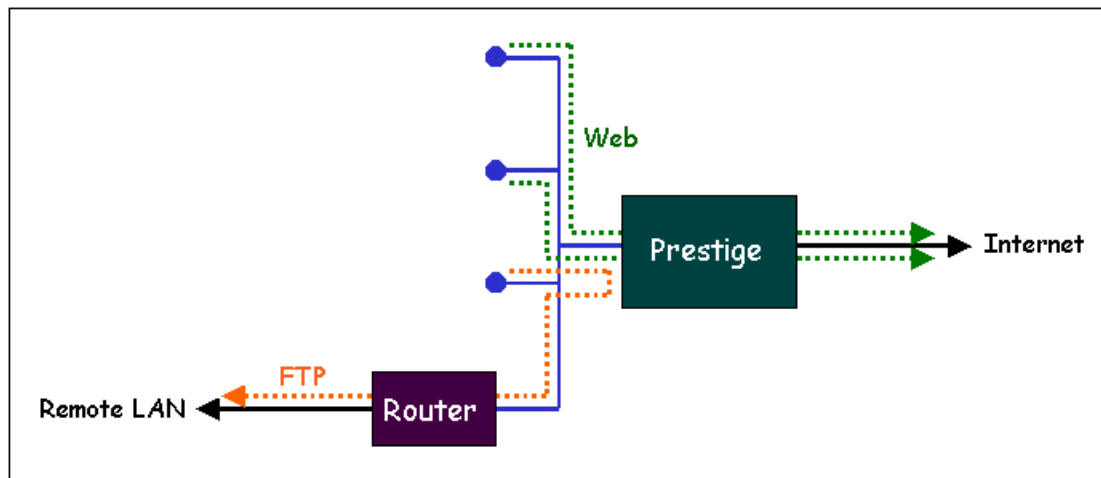
Telnet 192.168.1.1
P-660R-T1> ip route status
Dest          FF Len Device      Gateway      Metric stat Timer  Use
192.168.1.0   00 24 enet0       192.168.1.1  1   041b 0   1413
192.168.2.0   00 24 enet0       192.168.2.1  1   041b 0    0
default      00 0  Idle       MyISP        2   002b 0   649
P-660R-T1> ip ifconfig
enif0: mtu 1500
inet 192.168.1.1, netmask 0xfffff00, broadcast 192.168.1.255
RIP RX:Ver 1 & 2, TX:Ver 1 compatible,
[[InOctets      75008] [InUnicast     1298] [InMulticast    66]
[[InDiscards    0] [InErrors      0] [InUnknownProtos 0]
[OutOctets     79297] [OutUnicast    1441] [OutMulticast   19]
[OutDiscards   3] [OutErrors     0]
enif0:0: mtu 1500
inet 192.168.2.1, netmask 0xfffff00, broadcast 192.168.2.255
RIP RX:None, TX:None,
[[InOctets      0] [InUnicast     0] [InMulticast    0]
[[InDiscards    0] [InErrors      0] [InUnknownProtos 0]
[OutOctets     0] [OutUnicast    0] [OutMulticast   0]
[OutDiscards   0] [OutErrors     0]
enif0:1: mtu 1500
inet 0.0.0.0, netmask 0x00000000, broadcast 0.0.0.0
RIP RX:None, TX:None,
[[InOctets      0] [InUnicast     0] [InMulticast    0]
[[InDiscards    0] [InErrors      0] [InUnknownProtos 0]
[OutOctets     0] [OutUnicast    0] [OutMulticast   0]
[OutDiscards   0] [OutErrors     0]
P-660R-T1>

```

9. Using IP Policy Routing

- What is IP Policy Routing (IPPR)?

Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Network administrators can use IPPR to distribute traffic among multiple paths. For example, if a network has both the Internet and remote node connections, we can route the Web packets to the Internet using one policy and route the FTP packets to the remote LAN using another policy. See the figure below.



Use IPPR to distribute traffic among multiple paths

- Benefits

Source-Based Routing - Network administrators can use policy-based routing to direct traffic from different users through different connections.

Quality of Service (QoS)- Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.

Cost Savings- IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost path while using low-path for batch traffic.

Load Sharing- Network administrators can use IPPR to distribute traffic among multiple paths.

- How does the IPPR work?

A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The

criteria include the source address and port, IP protocol (ICMP, UDP, TCP, etc), destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, e.g., Telnet, tend to have short packets, while bulk traffic, e.g., file transfer, tends to have large packets.

The actions that can be taken include routing the packet to a different gateway (and hence the outgoing interface) and the TOS and precedence fields in the IP header. IPPR follows the existing packet filtering facility of ZyNOS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with 6 policies in each set.

- Setup the IP Policy Routing

Step 1: Set the index of IP routing policy set rule by command '**ip policyrouting set index [set#] [rule#]**'. Suppose set#=1, rule#=1 in this example.

Step 2: Suppose we'd like to edit the rule like this:

```

Policy Set Name=Test
Active= Yes
Criteria:
IP Protocol    = 6
Type of Service= Don't Care    Packet length= 0
Precedence    = Don't Care    Len Comp= N/A
Source:
  addr start= 192.168.1.2      end= 192.168.1.20
  port start= 0                end= N/A
Destination:
  addr start= 0.0.0.0          end= N/A
  port start= 80               end= 80
Action= Matched
Gateway addr   = 192.168.1.254  Log= No
Type of Service= No Change
Precedence    = No Change
  
```

This policy example forces the Web packets originated from the clients with IP addresses from 192.168.1.2 to 192.168.1.20 be routed to the remote LAN via the gateway 192.168.1.254.

To implement this, we need to invoke the following command one by one:

ip policyrouting set name Test

(Set the name as Test of IP routing policy rule)

ip policyrouting set active yes

(Enable the rule)

ip policyrouting set criteria protocol 6

(Set the protocol ID as 6(TCP) for the rule)

ip policyrouting set criteria serviceType 0

(Set the criteria type of service as don't care for this rule)

ip policyrouting set criteria precedence 8

(Set the precedence as don't care for this rule)

ip policyrouting set criteria packetlength 0

(Set the packet length as 0 for the rule)

ip policyrouting set criteria srcip 192.168.1.2 192.168.1.20

(Set the source IP address for the rule: Start=192.168.1.2, end=192.168.1.20)

ip policyrouting set criteria srcport 0

(Set the source port for the rule: Start=0)

ip policyrouting set criteria destip 0.0.0.0

(Set the destination port for the rule: Start=0.0.0.0)

ip policyrouting set criteria destport 80 80

(Set the destination port for the rule: Start=80, end=80)

ip policyrouting set action actmatched

(Set the action for the rule: Matched)

ip policyrouting set action gatewaytype 0

(Set gateway type for the rule: Gateway Address)

ip policyrouting set action gatewayaddr 192.168.1.254

(Set the gateway address for the rule: 192.168.1.254)

ip policyrouting set criteria serviceType 0

(Set the action type of service as don't care for this rule)

ip policyrouting set criteria precedence 8

(Set the action precedence as don't care for this rule)

ip policyrouting set action log no

(Set log option for the rule: no log)

ip polictrouting set save

(Save the rule)

Step 3: Apply the IP policy routing. There are two interfaces to apply the policy set, they are the LAN interface and WAN interface. It depends where the gateway specified in the policy rule is located. If the gateway you specified is located on the local LAN you apply the policy set in LAN interface. If the gateway you specified is located on the remote WAN site you apply the policy set in WAN interface.

Apply to WAN Interface (Suppose we apply it to remote node 1 in the example):

wan node index 1
wan node ippolicy 1

Apply to LAN Interface (Suppose we apply it to remote node 1 in the example):

lan index 1
Usage: index <1: main LAN| 2: IP Alias#1|3: IP Alias#2>
lan ippolicy 1
lan save

10. Using Call Scheduling

- What is Call Scheduling?

Call scheduling enables the mechanism for the P-660R-Tx v2 to run the remote node connection according to the pre-defined schedule. This feature is just like the scheduler in a video recorder which records the program according to the specified time. Users can apply at most 4 schedule sets in Remote Node. The remote node configured with the schedule set could be "Forced On", "Forced Down", "Enable Dial-On-Demand", or "Disable Dial-On-Demand" on specified date and time.

- How to configure a Call Scheduling?

You can configure a call scheduling in CLI

Suppose we want to edit a call schedule set like this:

```
Call Schedule Set #=1
Set name=Test
Active= Yes
Start Date(yyyy-mm-dd)= 2005 - 12 - 27
How Often= Once
Once:
Date(yyyy-mm-dd)= 2005 -12 -27
Start Time(hh:mm)= 12 : 00
Duration(hh:mm)= 16 : 00
Action= Enable Dial-on-demand
```

This schedule example permits a demand call on the line on 12:00 a.m., 2005-12-27. The maximum length of time this connection is allowed is 16 hours.

To implement this, we need to invoke the following command one by one:

wan callsch index 1

(Set call schedule index #= 1. You must apply this command first before you begin to configure call schedule)

wan callsch name Test

(Set the schedule name as Test)

wan callsch active Yes

(Enable schedule)

wan callsch startdate 2005 12 27

(Set schedule start date as 2005-12-27)

wan callsch oncedate 2005 12 27

(Set the schedule used just once, it works on 2005-12-27)

wan callsch starttime 12 00

(Set the schedule start time as 12:00)

wan callsch duration 16 00

(Set schedule duration time as 16 hours)

wan callsch action 2

(Set action as dial-on-demand)

wan callsch save

(Save the current call schedule set)

Key Settings:

Start Date	Start date of this schedule rule. It can be unmatched with weekday setting. For example, if Start Date is 2000/10/02(Monday), but Monday setting in weekday can be No.
Forced On	The node will always keep up during the setting period. It is equivalent to disable the idel timeout.
Forced Down	The node will always keep doen during the setting period. The connected remote node will be dropped.
Enable Dial-On-Demand	The remote node accepts Dial-on-demand during this period.
Disable Dial-On-Demand	The remote node denies any demand dial during the period. For the existing connected nodes, it will be dropped after idle timeout and no triggered up.
Start Time/Duration	Start Time and Duration of this schedule.

- Apply the schedule to the Remote node

Multiple scheduling rules can program in a Remote node, and they have priority. For example, if we program the sets as 1,2,3,4 in remote node, then the set 1 will override set 2,3,4. set 2 will override 3,4, and so on.

We can apply the schedule to the remote node in **CLI** by the commands:

wan node index []index#]

wan node callsch [index#]

wan node save

For example, if we want to apply the call schedule set 1 to remote node 1, we could use the commands:

wan node index 1

wan node callsch 1

wan node save

- Time Service in P-660R-Tx v2

There is no RTC (Real-Time Clock) chip so the P-660R-Tx v2 should launch a mechanism to get current time and date from external server in boot time.

Time service is implemented by the **Daytime protocol(RFC-867)**, **Time protocol(RFC-868)**, and **NTP protocol(RFC-1305)**. You have to assign an IP address of a time server and then, the P-660R-Tx v2 will get the date, time, and time-zone information from this server. You can configure it in Web Configurator, **Advanced Setup -> Time and Date**.

Time and Date

Time Server			
Use Protocol when Bootup	Daytime (RFC-867) ▾		
IP Address or URL	202.132.154.1		
Time and Date	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London ▾		
<input type="checkbox"/> Daylight Savings			
Start Date	1	month	1
End Date	1	month	1
<input type="checkbox"/> Synchronize system clock with Time Server now. (This may take up to 60 seconds.)			
Date			
Current Date	2006	-01-	22
New Date (yyy-mm-dd)	2006	-01-	22
Time			
Current Time	15	:05:	00
New Time	15	:05:	00

11. Using IP Multicast

- What is 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 P-660R-Tx v2 queries all directly connected networks to gather group membership.

After that, the P-660R-Tx v2 updates the information by periodic queries. The P-660R-Tx v2 implementation of IGMP is also compatible with version 1. The multicast setting can be turned on or off on Ethernet and remote nodes.

- IP Multicast Setup

(1) Enable IGMP in P-660R-Tx v2's LAN in Web Configurator, Advanced Setup, -> **LAN** -> **LAN Setup**.

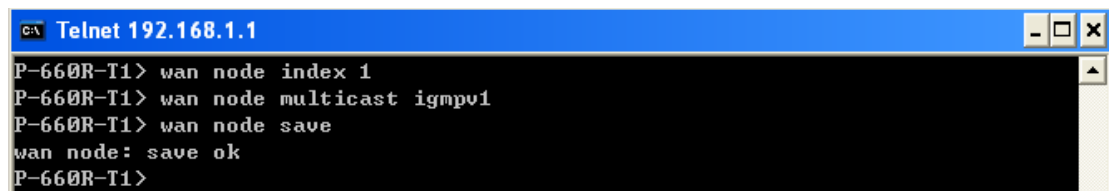
(2) Enable IGMP in P-660R-Tx v2's remote node via command:

wan node index <node#>

Usage: node#= 1~8

wan node multicast < none | igmpv1 | igmpv2 >

wan node save



```

c:\ Telnet 192.168.1.1
P-660R-T1> wan node index 1
P-660R-T1> wan node multicast igmpv1
P-660R-T1> wan node save
wan node: save ok
P-660R-T1>
  
```

Key Settings:

Multicast	IGMP-v1 for IGMP version 1, IGMP-v2 for IGMP version 2.
------------------	---

12. Using Zero-Configuration

- Zero-Configuration and VC auto-hunting

Zero-Configure feature can help customer to reduce the burden of setting efforts. Whenever system ADSL links up system will send out some probing patterns, system will analyze the packets returned from ISP, and decide which services the ISP may provide. Because ADSL is based on a ATM network, so system have to pre-configured a VPI/VCI hunting pool before Auto-Configure function begins to work.

The Zero-Configuration feature can hunt the encapsulation and VPI/VCI value, and system will automatically configure itself if the hunting result is successfully. This feature has two constraints:

1. It supports the ISP provides one kind of service (PPPoE/PPPoA..etc.) only, otherwise the hunting will get confusing and failed.
2. VC auto-hunting only supports dynamic WAN IP address. If the router is set a static WAN IP address. VC auto-hunting function will be disabled.

The entry of hunting pool must also contain the VPI, VCI, and which kinds of hunting patterns you wish to send. Whenever system send out all the probing patterns with specific VPI/VCI, system will wait for 5~10 seconds and get the response from ISP, the response patterns will decide which kinds of ADSL services of the line will be. After that, system will save back the correct VPI, VCI and also services (encapsulation) type into profile of WAN interface.

- Configure the VC auto-hunting preconfigured table.

(1) Display auto-haunting preconfigured table via command:

wan atm vchunt disp

```

Telnet 192.168.1.1
P-660R-T1> wan atm vchunt display
<1> Configure Buffer
<2> RemoteNode <Read Only>
  RN UPI    UCI | RN UPI    UCI | RN UPI    UCI | RN UPI    UCI |
-----|-----|-----|-----|
  1  8    35 | 2  0     0 | 3  0     0 | 4  0     0 |
  5  0     0 | 6  0     0 | 7  0     0 | 8  0     0 |
<3> UC Hunt Table: <User setting>
Flags: Active<1>
  RN UPI    UCI serv | RN UPI    UCI serv | RN UPI    UCI serv | RN UPI    UCI serv
-----|-----|-----|-----|
  1  0  33   3fH | 1  0  35   3fH | 1  1  35   3fH | 1  8  32   3fH |
  1  0 101   3fH | 1  0  50   3fH | 1  0  32   3fH | 1 14  24   3fH |
  0  0   0   0H | 0  0   0   0H |
<4> WebRedirect: Enable
P-660R-T1>
    
```

(2) Add items to the auto-haunting preconfigured table by using CI commands:

```
wan atm vchunt add <remoteNodeIndex> <vpi> <vci> <service
bit(hex)>
```

```
wan atm vchunt save
```

Note: <remote node> : input the remote node index 1-8

<vpi> : vpi value

<vci> : vci value

<service>: it's a hex value, bit0:PPPoE/VC (1), bit1:PPPoE/LLC (2) , bit2:PPPoA/VC (4), bit3:PPPoA/LLC (8), bit4:Enet/VC (16), bit5 :Enet/LLC (32)

For examples:

If you need service PPPoE/LLC and Enet/LLC then the service bits will be 2+32 = 34 (decimal) = 22 (hex), you must input 22

If you want to enable all service for VC hunting, the service bits will be 1+2+4+8+16+32=63(decimal)= 3f (hex), you must input 3f

Need to perform save after this by command '**wan atm vchunt save**'

```
ras> wan atm vchunt add 1 8 36 3f
ras> wan atm vchunt save
ras> wan atm vchunt display
(1) Configure Buffer
(2) RemoteNode (Read Only)
RN VPI   VCI | RN VPI   VCI | RN VPI   VCI | RN VPI   VCI |
-----|-----|-----|-----|
 1  0   33 | 2  0     0 | 3  0     0 | 4  0     0 |
 5  0     0 | 6  0     0 | 7  0     0 | 8  0     0 |
(3) VC Hunt Table: (User setting)
Flags: Active(1)
RN VPI   VCI serv| RN VPI   VCI serv| RN VPI   VCI serv| RN VPI   VCI serv
-----|-----|-----|-----|
 1  8   35 400H| 1  0   35  3fH| 1  1   35  3fH| 1  8   32  3fH|
 1  0  101  3fH| 1  0   50  3fH| 1  0   32  3fH| 1  14  24  3fH|
 1  8   36  3fH| 0  0     0   0H|
```

(3) Delete items from the auto-haunting preconfigured table via command:

```
wan atm vchunt remove <remote node> <vpi> <vci>
```

```
ras> wan atm vchunt remove 1 8 36
ras> wan atm vchunt display
(1) Configure Buffer
(2) RemoteNode (Read Only)
RN VPI   VCI | RN VPI   VCI | RN VPI   VCI | RN VPI   VCI |
-----|-----|-----|-----|
 1  0   33 | 2  0     0 | 3  0     0 | 4  0     0 |
 5  0     0 | 6  0     0 | 7  0     0 | 8  0     0 |
(3) VC Hunt Table: (User setting)
Flags: Active(1)
RN VPI   VCI serv| RN VPI   VCI serv| RN VPI   VCI serv| RN VPI   VCI serv
-----|-----|-----|-----|
 1  8   35 400H| 1  0   35  3fH| 1  1   35  3fH| 1  8   32  3fH|
 1  0  101  3fH| 1  0   50  3fH| 1  0   32  3fH| 1  14  24  3fH|
 0  0     0   0H| 0  0     0   0H|
```

- Using Zero configuration.

(1) After configure the auto-haunting preconfigured table. You just need a PC connected to the device LAN Ethernet port with the DSL sync up.

(2) Open your web browser to access a Web site. It should prompt and request for your username password of your ISP account, if your ISP provide PPPoE or PPPoA service.

(3) After key-in the correct info, it will than test the connection. If it is successful it will than close the browser and you can open a new browser to surf the Internet. If the connection test fail, it will go back to the page ask for user name and password.

The user name or password are incorrect. You need to keyin again to retry.

(4) Basically the zero configuration only work on the VC that was preconfigured in the auto-haunting preconfigured table.



Enter the username and password exactly as your ISP assigned them.

System Password	••••
User Name	85111279@hinet.net
Password	••••••••

Save Settings

Support Tool

1. LAN/WAN Packet Trace

The Prestige packet trace records and analyzes packets running on LAN and WAN interfaces. It is designed for users with technical backgrounds who are interested in the details of the packet flow on LAN or WAN end of Prestige. It is also very helpful for diagnostics if you have compatibility problems with your ISP or if you want to know the details of a packet for configuring a filter rule.

The format of the display is as following:

Packet:

```
0 02:10:02.390 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
```

[index] [timer/second][channel-receive/transmit][length] [protocol]
[sourceIP/port] [destIP/port]

There are two ways to dump the trace:

Online Trace--display the trace real time on screen

Offline Trace--capture the trace first and display later

The details for capturing the trace in CLI as follows:

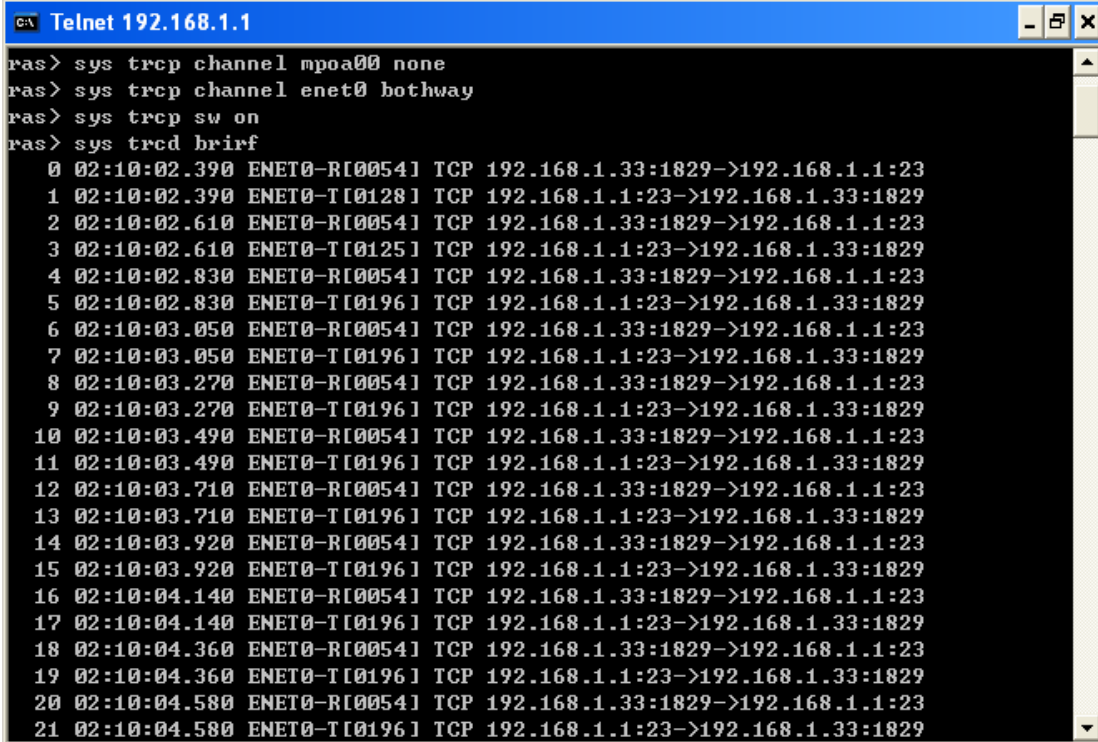
First of all, you need to telnet to the P-660HW-D firstly. The password is Administrator passwords, 'admin' by default.

Online Trace

(1) Trace LAN packet

- Disable to capture the WAN packet by entering: **sys trcp channel mpoa00 none**
- Enable to capture the LAN packet by entering: **sys trcp channel enet0 bothway**
- Enable the trace log by entering: **sys trcp sw on & sys trcl sw on**
- Display the brief trace online by entering: **sys trcd brief**
- Display the detailed trace online by entering: **sys trcd parse**

Example:



```

C:\ Telnet 192.168.1.1
ras> sys trcp channel mpoa00 none
ras> sys trcp channel enet0 bothway
ras> sys trcp sw on
ras> sys trcd brif
0 02:10:02.390 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
1 02:10:02.390 ENET0-T[0128] TCP 192.168.1.1:23->192.168.1.33:1829
2 02:10:02.610 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
3 02:10:02.610 ENET0-T[0125] TCP 192.168.1.1:23->192.168.1.33:1829
4 02:10:02.830 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
5 02:10:02.830 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
6 02:10:03.050 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
7 02:10:03.050 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
8 02:10:03.270 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
9 02:10:03.270 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
10 02:10:03.490 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
11 02:10:03.490 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
12 02:10:03.710 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
13 02:10:03.710 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
14 02:10:03.920 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
15 02:10:03.920 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
16 02:10:04.140 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
17 02:10:04.140 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
18 02:10:04.360 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
19 02:10:04.360 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829
20 02:10:04.580 ENET0-R[0054] TCP 192.168.1.33:1829->192.168.1.1:23
21 02:10:04.580 ENET0-T[0196] TCP 192.168.1.1:23->192.168.1.33:1829

```

(2) Trace WAN packet

- Disable the capture of the LAN packet by entering: **sys trcp channel enet0 none**
- Enable to capture the WAN packet by entering: **sys trcp channel mpoa00 bothway**
- Enable the trace log by entering: **sys trcp sw on** & **sys trcl sw on**
- Display the brief trace online by entering: **sys trcd brief**
- Display the detailed trace online by entering: **sys trcd parse**

Example:

```

Telnet 192.168.1.1
ras> sys trcp channel enet0 none
ras> sys trcp channel mpoa00 bothway
ras> sys trcp sw on
ras> sys trcd parse
-----<0000>-----
MPOA Frame: MPOA00-RECU  Size: 60/ 60  Time: 02:20:24.510
Frame Type: Ethernet Packet

Ethernet Header:
  Destination MAC Addr  = 001349000001
  Source MAC Addr      = 000480EF2E78

Network Type          = 0x0800 <TCP/IP>
IP Header:
  IP Version           = 4
  Header Length        = 20
  Type of Service      = 0x00 <0>
  Total Length         = 0x0028 <40>
  Identification       = 0x3F0F <16143>
  Flags                = 0x02
  Fragment Offset      = 0x00
  Time to Live         = 0x71 <113>
  Protocol              = 0x06 <TCP>
  Header Checksum      = 0x9FCD <40909>
  Source IP            = 0xDEAC8AF3 <222.172.138.243>
  Destination IP       = 0xAC19153A <172.25.21.58>

TCP Header:
  Source Port          = 0x0F28 <3880>
  Destination Port     = 0x2966 <10598>
  Sequence Number      = 0x326B4309 <845890313>
  Ack Number           = 0xAD825B3A <2911001402>
  Header Length        = 20
  Flags                = 0x10 <..A....>
  Window Size         = 0x2BE6 <11238>
  Checksum             = 0xA23B <41531>
  Urgent Ptr           = 0x0000 <0>

TCP Data: <Length=6, Captured=6>
0000: 00 00 00 00 00 00  .....

RAW DATA:

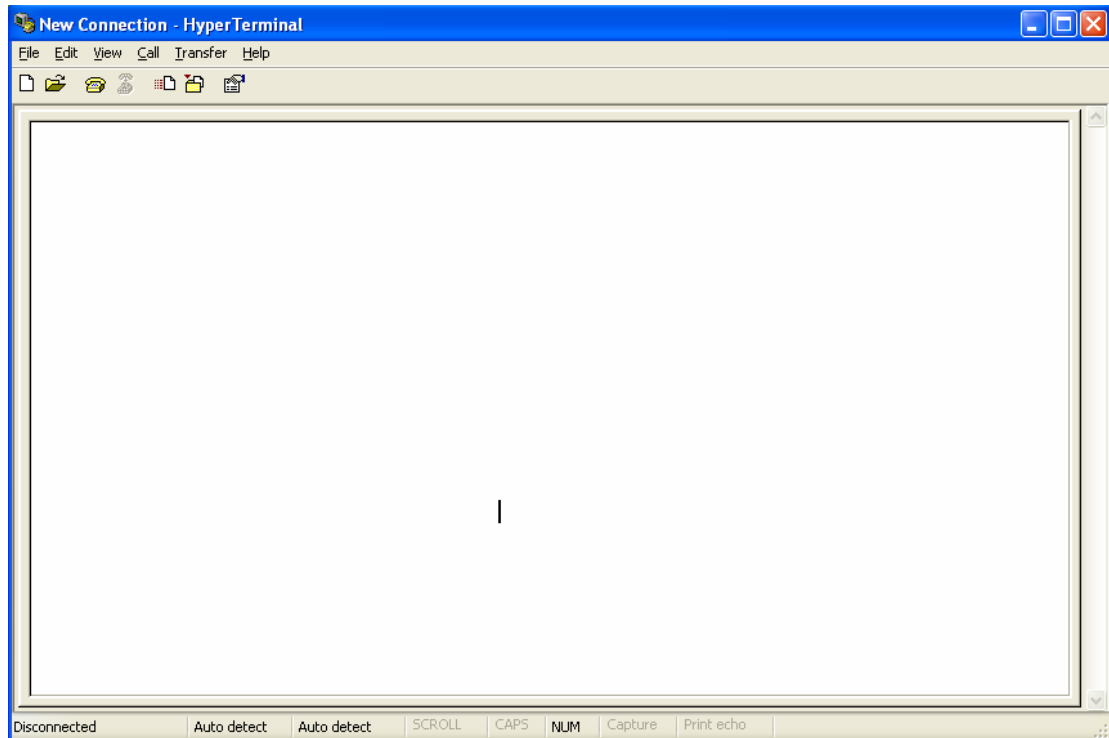
```

Offline Trace

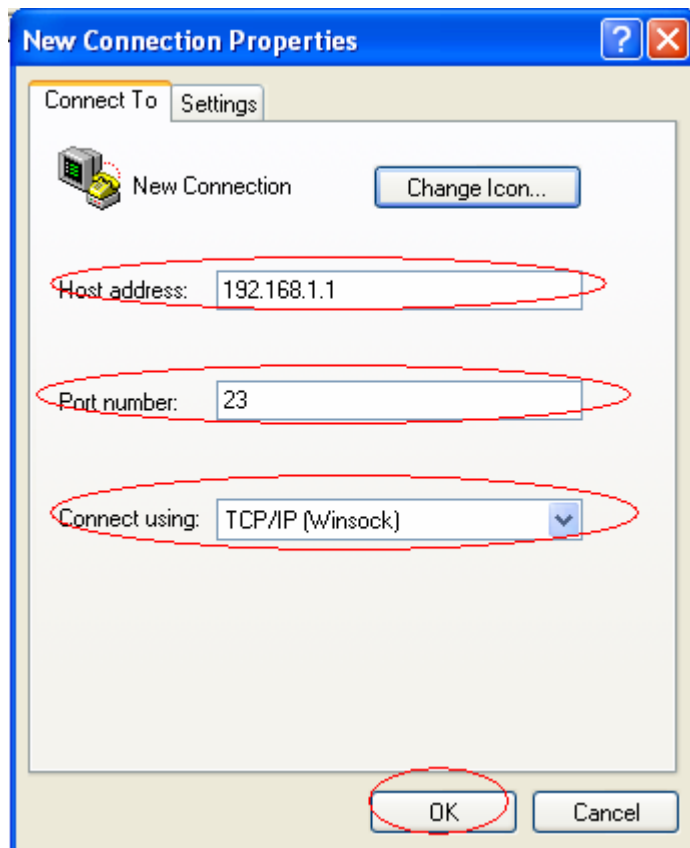
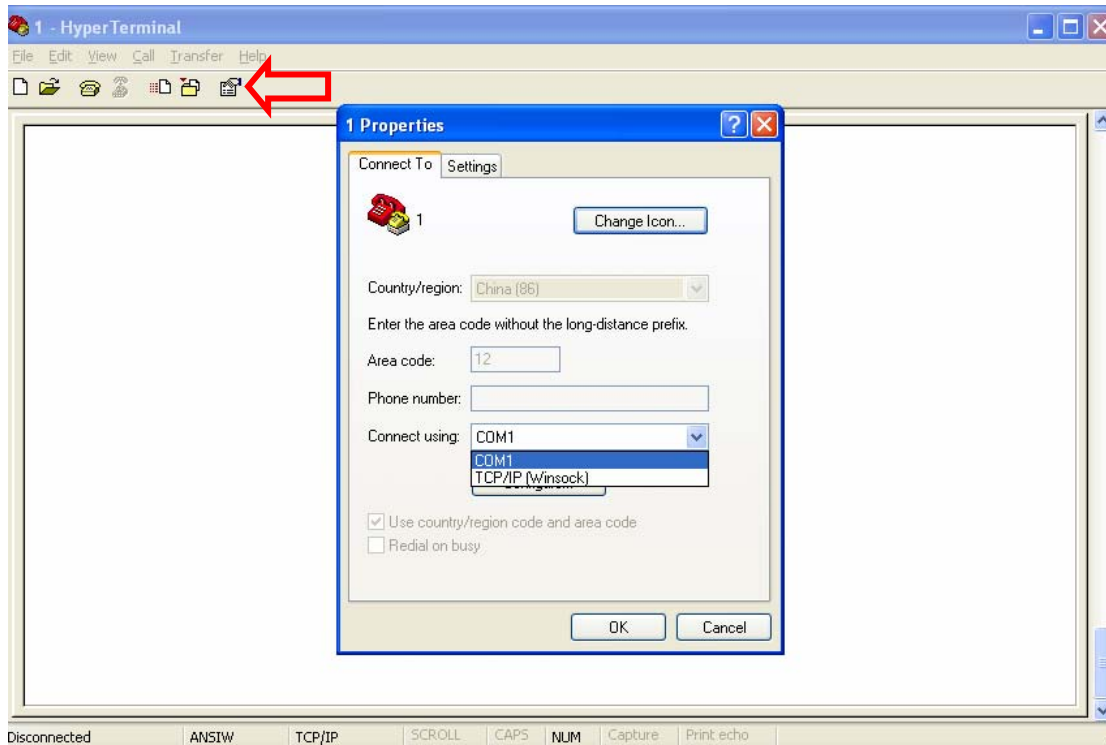
- Disable the capture of the WAN packet by entering: **sys trcp channel mpoa00 none**
- Enable the capture of the LAN packet by entering: **sys trcp channel enet0 bothway**
- Enable the trace log by entering: **sys trcp sw on & sys trcl sw on**
- Wait for packet passing through the Prestige over LAN
- Disable the trace log by entering: **sys trcp sw off & sys trcl sw off**
- Display the trace briefly by entering: **sys trcp brief**
- Display specific packets by using: **sys trcp parse <from_index> <to_index>**

- **Capture the detailed logs by Hyper Terminal**

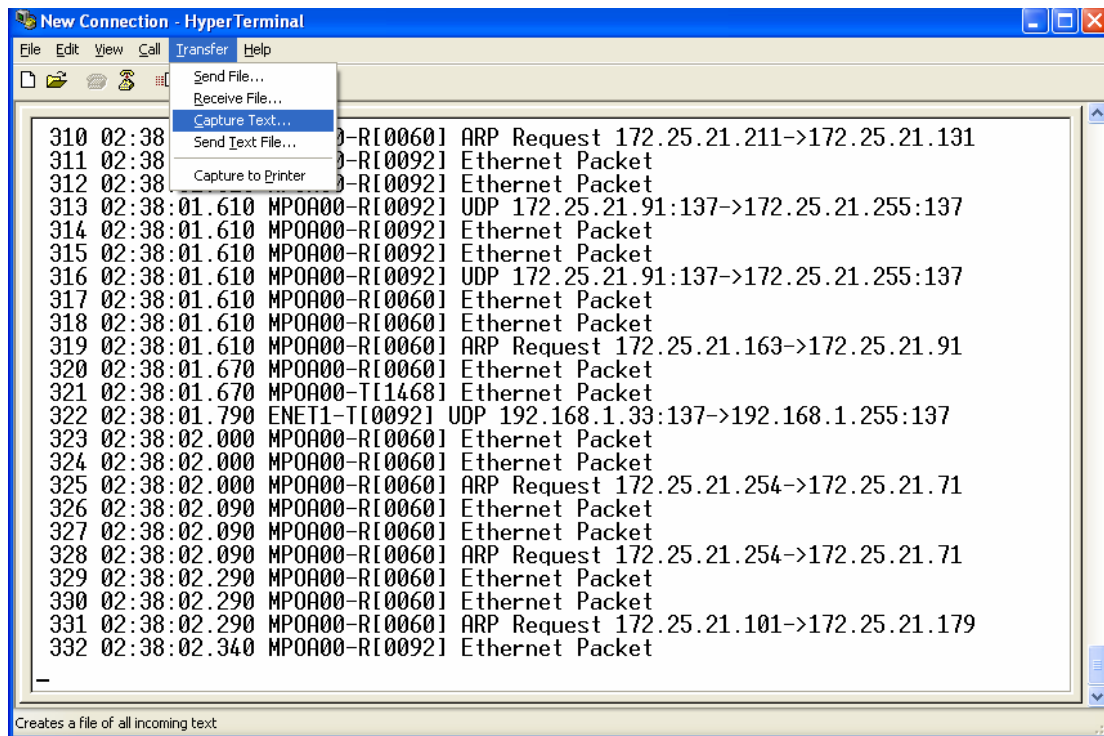
Step 1: Initiate a hyper terminal connection from your PC(suppose you connected to the LAN port of P-660R-Tx v2)



Step 2: Click the 'properties' to configure parameters to telnet to the P-660R-Tx v2.



Step 3: So that after you invoke the relevant commands, you could save the logs you've captured.



2. Firmware/Configurations Uploading and Downloading using TFTP

- Using TFTP client software

- Upload/download ZyNOS via LAN
- Upload/download Prestige configurations via LAN

(1) Using TFTP to upload/download ZyNOS via LAN

Step 1: TELNET to your Prestige first before running the TFTP software

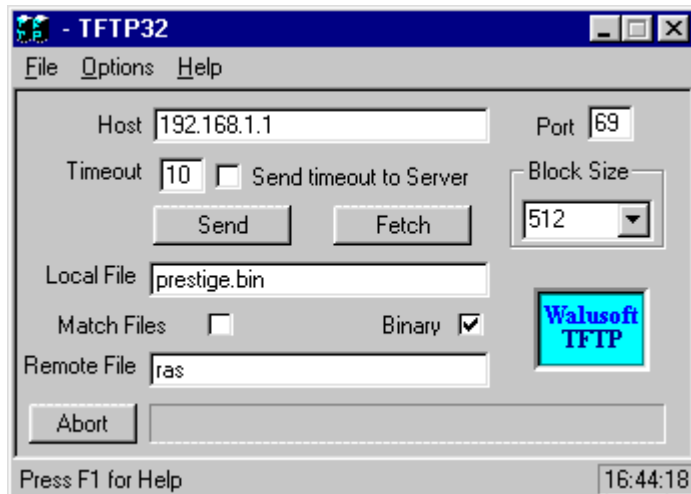
Step 2: Type the CLI command '**sys studio 0**' to disable console idle timeout in **Command Line Interface (CLI)**

Step 3: Run the TFTP client software

Step 4: Enter the IP address of the Prestige

Step 5: To upload the firmware, please save the remote file as '**ras**' to Prestige. After the transfer is complete, the Prestige will program the upgraded firmware into FLASH ROM and reboot itself.

An example:



The 192.168.1.1 is the IP address of the Prestige. The local file is the source file of the ZyNOS firmware that is available in your hard disk. The remote file is the file name that will be saved in Prestige. Check the port number 69 and 512-Octet blocks for TFTP. Check **'Binary'** mode for file transferring.

(2) Using TFTP to upload/download SMT configurations via LAN

Step 1: TELNET to your Prestige first before running the TFTP software

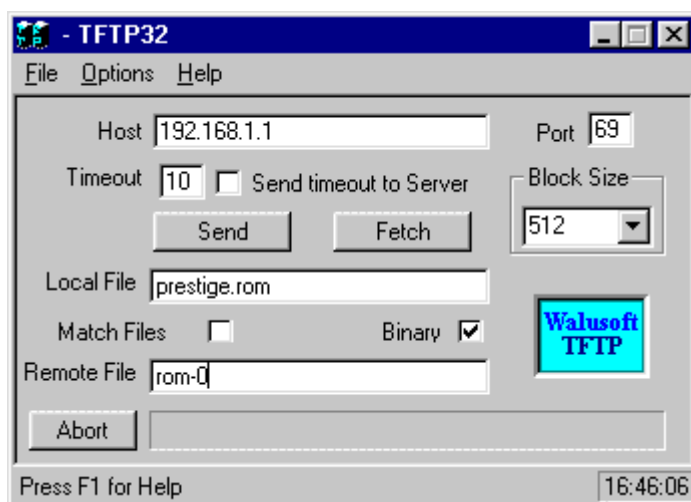
Step 2: Type the command **'sys studio 0'** to disable console idle timeout in **Command Line Interface (CLI)**.

Step 3: Run the TFTP client software

Step 4: To download the P-660R-Tx v2 configuration, please get the remote file **'rom-0'** from the Prestige.

Step 5: To upload the P-660R-Tx v2 configuration, please save the remote file as **'rom-0'** in the Prestige.

An example:



- The 192.168.1.1 is the IP address of the Prestige.
- The local file is the source file of your configuration file that is available in your hard disk.
- The remote file is the file name that will be saved in Prestige.
- Check the port number 69 and 512-Octet blocks for TFTP.
- Check 'Binary' mode for file transferring.

- **Using TFTP command on Windows NT**

Step 1: TELNET to your Prestige first before using TFTP command

Step 2: Type the CLI command '**sys stdio 0**' to disable console idle timeout in **Command Line Interface (CLI)**.

Step 3: Download ZynOS via LAN : **c:\tftp -i [PrestigeIP] get ras [localfile]**

Step 4: Upload P-660HW-D configurations via LAN: **c:\tftp -i [PrestigeIP] put [localfile] rom-0**

Step 5: Download P-660R-Tx v2 configurations via LAN: **c:\tftp -i [PrestigeIP] get rom-0 [localfile]**

- **Using TFTP command on UNIX**

Before you begin:

1. TELNET to your Prestige first before using TFTP command
2. Type the CLI command '**sys stdio 0**' to disable console idle timeout in **Command Line Interface (CLI)**

Example:

```
[cppwu@faelinux cppwu]$ telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^'.
Password: ****
ras> sys stdio 0
(Open a new window)
[cppwu@faelinux cppwu]$ tftp -l 192.168.1.1 get rom-0 [local-rom] <- change to binary mode
<- download configurations

[cppwu@faelinux cppwu]$ tftp -l 192.168.1.1 put [local-rom] rom-0 <- upload configurations

[cppwu@faelinux cppwu]$ tftp -l 192.168.1.1 get ras [local-ras ] <- download firmware
```



```
[cppwu@faelinux cppwu]$ tftp -l 192.168.1.1 put [local-ras] ras <- upload firmware
```

3. Using FTP to Upload the Firmware and Configuration Files

In addition to upload the firmware and configuration file via the console port and TFTP client, you can also upload the firmware and configuration files to the Prestige using FTP.

To use this feature, your workstation must have a FTP client software. See the example shown below.

- **Using FTP client software**

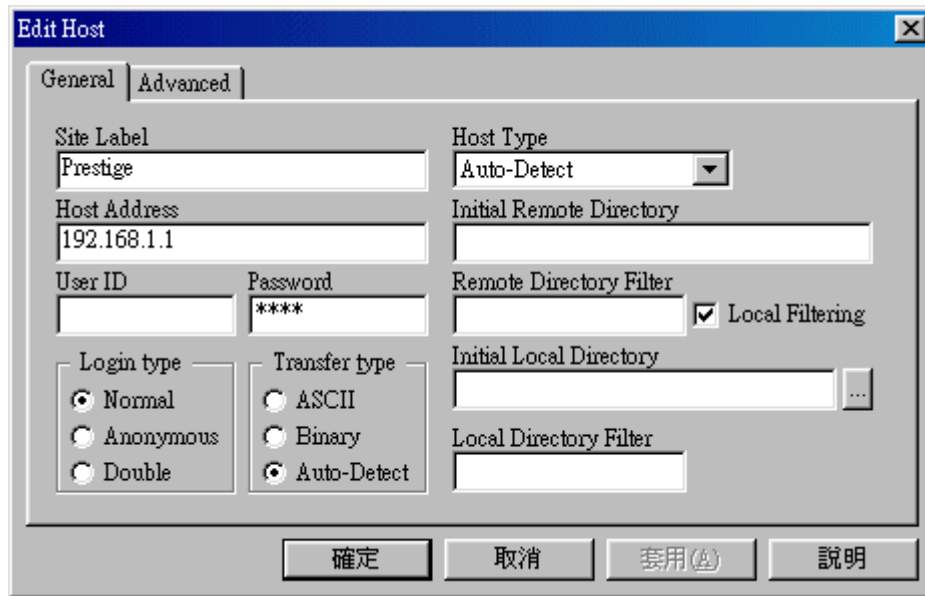
Note: The remote file name for the firmware is '**ras**' and the configuration file is '**rom-0**'.

Step 1	Use FTP client from your workstation to connect to the Prestige by entering the IP address of the Prestige.
Step2	Press ' Enter ' key to ignore the username, because the Prestige does not check the username.
Step 3	Enter the CLI password as the FTP login password, the default is ' admin '.
Step 4	Enter command ' bin ' to set the transfer type to binary.
Step 5	Use ' put ' command to transfer the file to the Prestige.

Example:

Step 1: Connect to the Prestige by entering the Prestige's IP and Administrator password in the FTP software. Set the transfer type to '**Auto-Detect**' or

'Binary'.

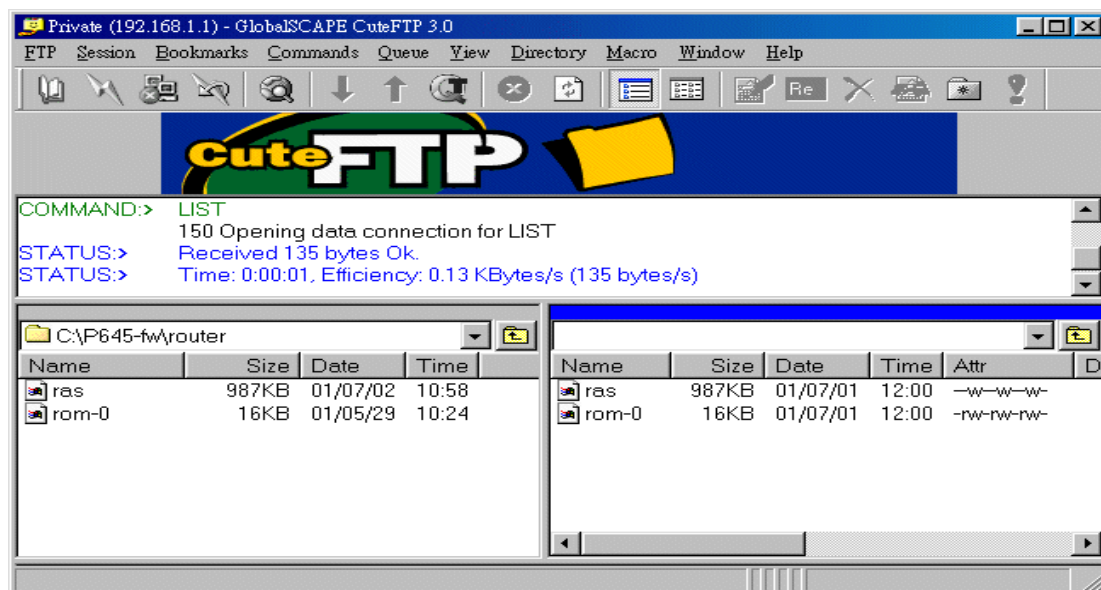


Step 2: Press 'OK' to ignore the 'Username' prompt.



Step 3: To upload the firmware file, we transfer the local 'ras' file to overwrite the remote 'ras' file.

To upload the configuration file, we transfer the local 'rom-0' to overwrite the remote 'rom-0' file.



Step 4: The Prestige reboots automatically after the uploading is finished.
Please do not power off the router at this moment.

CI Command Reference

Command Syntax and General User Interface

CI has the following command syntax:

command <*iface* | *device* > **subcommand** [*param*]

command subcommand [*param*]

command ? | **help**

command subcommand ? | **help**

General user interface:

1. ?	Shows the following commands and all major (sub)commands
2. exit	Returns to SMT

To get the latest CI Command list

The latest CI Command list is available in release note of every ZyXEL firmware release. Please goto ZyXEL public WEB site http://www.zyxel.com/support/download_index.php to download firmware package (*.zip), you should unzip the package to get the release note in PDF format.