

ZyXEL Prestige 100IH+ (USA)

ZyNOS v2.21(G.01)

Release Note/Manual Supplement

Date: November 18, 1999

First time release.

Supported Platforms

V2.21(G.01) USA F/W supports Prestige models: P100IH+ or P100IH with either U or S/T interface.

Note that if on the back label there is marked "ZyIH01" it indicates the hardware has analog Caller ID support on the POTS ports. (This is the Prestige 100IH+ model).

Features:

More Remote Nodes and IP Static Routes

Version 2.21(G.01) offers 8 IP Static Routes and offers 8 Remote Nodes in Prestige 100IH.

Easy Installation

Most new Prestige owners now need only enter the ISDN phone numbers (supplied by the ISDN provider) in Menu 2, and the phone number, user ID, and password (supplied by the ISP) in Menu 4.

Nailed-up Connection

This new feature allows a dial-up line to emulate a leased line.

Backup and Restore Configuration File via LAN or WAN

PCT (Prestige Configuration Transfer), the stand-alone Java-based utility, allows backup and restoration of the configuration file via LAN or WAN.

Upgrade P100IH Firmware via LAN

PCT can upgrade the Prestige 100IH firmware over the local LAN.

CI Commands

ZyNOS keeps the familiar user interface (SMT, System Management Terminal) although the internal architecture is vastly different. The syntax and semantics of the CI commands remain the same even though some of them are changed.

Here is the brief description about the most frequently used CI commands. The sequence of the following table is based on the v2.20 commands' alphabetic order.

pre-ZyNOS	V2.21	brief description
-----------	-------	-------------------

bridge stat disp	*	statistics on Bridge packets
bridge blt disp	*	Bridge LAN table
bridge brt disp	*	Bridge WAN table
	dev channel disp [bri0 bri1]	show channel information on bri0 or bri1
isdn drop [1 2]	dev channel drop [bri0 bri1]	drop channel bri0 or bri1
isdn dial x	dev dial x	manually dial to remote node x; x is the remote node number here
	ether config	show the current Ethernet configuration
lan cnt disp	ether driver cnt disp	statistics on the Ethernet driver
exit	*	exit from CI mode
ip address	*	LAN IP address
ip ping {IP address}	*	Ping {IP address}
ip route stat	*	IP routing table
ip status	*	statistics on IP packets
ip sua iface [wan0ppp wan1ppp] disp	ip sua iface [wanif0 wanif1] disp	display the SUA table for iface wanif0 or wanif1
ipx route stat	*	IPX routing table
ipx sap stat	*	IPX SAP table
	isdn atring clear [bri0 bri1]	clear the ISDN ring buffer of bri0 or bri1
isdn drv ring [1 2]	isdn atring disp [bri0 bri1]	display the ISDN ring buffer of bri0 or bri1
	isdn config	show the current ISDN configuration
sys epa	isdn fw ana dump	display ISDN trace messages on screen
isdn ana [on off]	isdn fw ana [on off]	enable/disable ISDN trace mechanism
Isdn p128 cnt disp	Isdn fw cnt disp	display ISDN transmission counters
	isdn initstring clear	clear ISDN init string
isdn set initstring {at commands}	isdn initstring set {at commands}	set ISDN init string to {at commands}
isdn init	isdn reset	initialize the ISDN line
ppp lcp acfc [on off]	*	enable/disable PPP LCP ACFC negotiation
ppp lcp bacp [on off]	*	enable/disable PPP LCP BACP negotiation
ppp lcp callback [on off]	*	enable/disable PPP LCP Microsoft callback negotiation
ppp lcp pfc [on off]	*	enable/disable PPP LCP PFC negotiation
sys countrycode	sys countrycode x	set country code
sys event	sys trcl call	show call trace on the screen
sys log disp	*	display the error/warning/information messages in the system log
sys log clear	*	clear the existing contents in system log
sys mbuf pool	*	display the pool of mbuf; mbuf is the buffer pre-allocated for data transmission

sys mbuf status	*	display mbuf status
sys memutil mqueue	*	statistics on pre-allocated system memory cell
sys memutil usage	*	statistics on the memory utilization
sys stdio 0	*	set SMT session timeout value to 0 → never timeout
sys trcd	*	display the packet trace on screen
sys trcl clear	*	clear the existing contents in logic trace log
sys trcl disp	*	display the contents in both of logic and packet trace logs
sys trcl switch [on off]	*	enable/disable logic trace log mechanism
sys trcp chann [in out both enet0]	*	Enable the packet trace mechanism on incoming, outgoing, or both from WAN; or from Ethernet.
sys trcp disp	*	display the contents in packet trace log
sys trcp switch [on off]	*	enable/disable packet trace log mechanism

Notes:

- blank – no corresponding CI command
- * - no change from the previous versions.

See Support Tool Manual for detailed information on ZyNOS commands.

Messages to syslogd

Prestige sends two types of messages to **syslogd** if **Syslog IP Address** field is configured. One type is the filter message if the **Log** field in Menu 21.x.y is enabled. In pre-ZyNOS versions, a message will be generated to send to syslogd for each filter rule the incoming/outgoing packet passes. In ZyNOS, there is only one message will be sent to syslogd. The message includes the header of the incoming/outgoing packet and the information about the filter rules it passes.

Another type is the call related information. In ZyNOS, the board information is added to the beginning of pre-ZyNOS messages. Otherwise, there are no other major changes.

Filter Rules

Conceptually, there are two categories of filter rules: *device* and *protocol*. The Generic filter rules belong to the *device* category; they act on the raw data from/to LAN and WAN. The IP and IPX filter rules belong to *protocol* category; they act on the IP and IPX packets.

In pre-ZyNOS versions, device and protocol (IP or IPX) filter rules could be intermixed in a filter set. This is no longer permitted in this release. This design change was provoked by the following dilemma in applying the TCP/IP filtering to SUA (Single User Account) connections:

In pre-ZyNOS versions, Prestige applied the input filter rules to the incoming packets immediately after receiving them from the ISDN line; and applied the call and output filter rules to the outgoing packets immediately prior to sending them out the ISDN port. With

this approach, the call and output filter rules were applied to the output IP packets whose source IP address and port number had already been converted into different values by SUA. Thus, the call and output TCP/IP filter rules did not work for a SUA connection if the filter rules were based on the local network IP address and port number. This same limitation also applied to the input filter rules as well.

Figure 1 shows the pre-ZyNOS logic flow for a packet from LAN to WAN (->), and a packet from WAN to LAN (->). Suppose that the packet from LAN to WAN with source IP address 192.168.1.33 and port number 1023; and the WAN IP address is 203.205.115.6 that could be dynamic or static. But the port number (4034 in this example) generated by SUA is always dynamic and unpredictable. The sequence of the logic flow for the packet from LAN to WAN is:

1. LAN input filter sets.
2. SUA converts the source IP address from 192.168.1.33 to 203.205.115.6 and port number from 1023 to 4034.
3. WAN call and output filter sets. It does not work if the filter rules are based on IP address 192.168.1.33 and port number 1023.

The sequence of the logic flow for the packet from WAN to LAN is:

4. WAN input filter sets. It does not work if the filter rules are based on IP address 192.168.1.33 and port number 1023.
5. SUA converts the destination IP address from 203.205.115.6 to 192.168.1.33 and port number from 4034 to 1023.
6. LAN output filter sets.

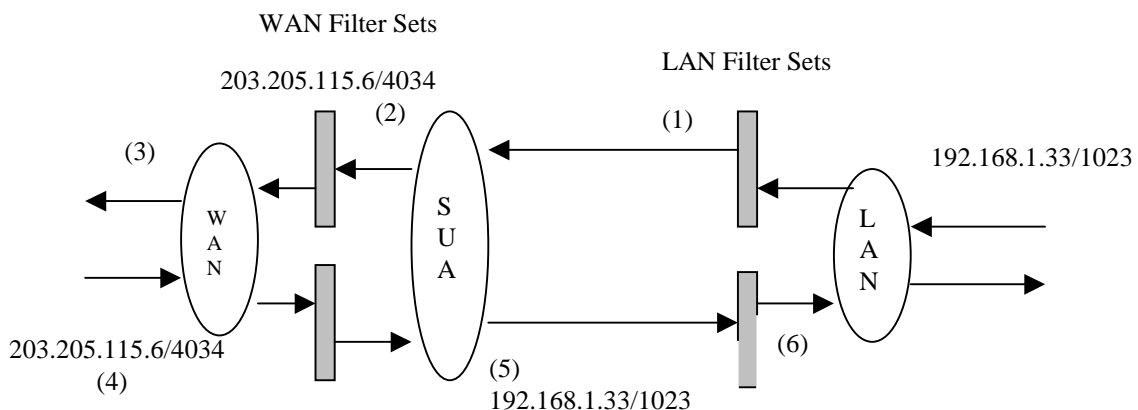


Figure 1. Packet Flow in pre-ZyNOS versions

In order to allowing users to specify the local network IP address and port number in the filter rules with SUA connections, the TCP/IP filter function has to be executed **before** SUA for WAN outgoing packets and **after** the SUA for WAN incoming IP packets. But at the same time, the Generic filter rules must be applied at the point when Prestige is receiving and sending the packets; i.e. the ISDN interface. So, the execution sequence has to be changed. The v2.20 logic flow is shown in Figure 2 and the sequence of the logic flow for the packet from LAN to WAN is:

1. LAN device and protocol input filter sets.
2. WAN protocol call and output filter sets. It works now because SUA does not convert the local IP address and port number to WAN IP address and port number yet.
3. SUA converts the source IP address from 192.168.1.33 to 203.205.115.6 and port number from 1023 to 4034.
4. WAN device output and call filter sets.

The sequence of the logic flow for the packet from WAN to LAN is:

5. WAN device input filter sets.
6. SUA converts the destination IP address from 203.205.115.6 to 192.168.1.33 and port number from 4034 to 1023.
7. WAN protocol input filter sets. It works now because SUA has converted the destination IP address and port number to local IP address and port number.
8. LAN device and protocol output filter sets.

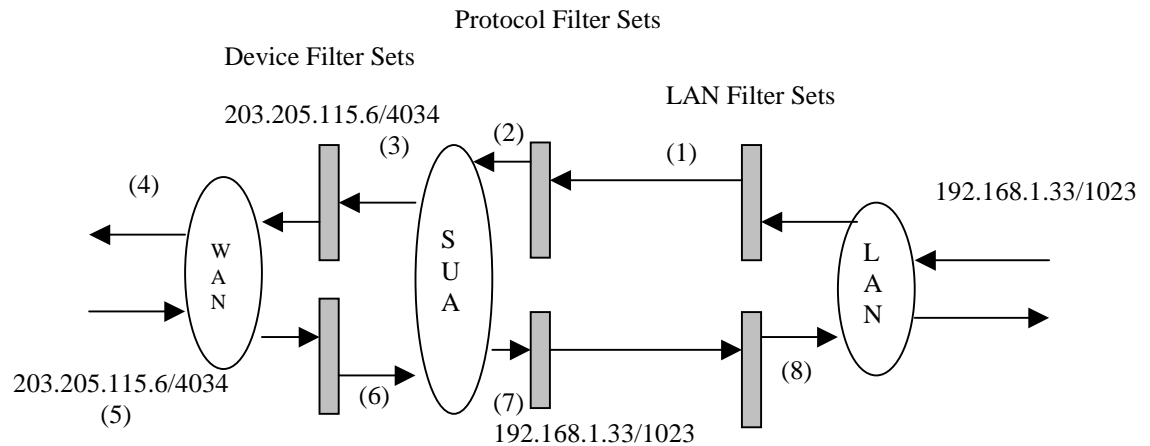


Figure 2. Packet Logic Flow in v2.21

To accommodate the above change, Generic and TCP/IP filter rules must now be in different filter sets. The v2.20 SMT will detect and prevent the mixing of different category rules within any filter set in Menu 21. In the following example, you will receive an error message **"Protocol and device filter rules cannot be active together"** if you try to activate a TCP/IP filter rule in a filter set that has already had one or more active Generic filter rules. You will receive the same error if you try to activate a Generic filter rule in a filter set that has already had one or more active TCP/IP filter rules.

Menu 21.1.1:

Menu 21.1.1 - Generic Filter Rule

Filter #: 1,1
Filter Type= Generic Filter Rule
Active= Yes
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Menu 21.1.2:

Menu 21.1.2 - TCP/IP Filter Rule

Filter #: 1,2
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 0 IP Source Route= No
Destination: IP Addr= 0.0.0.0
 IP Mask= 0.0.0.0
 Port #= 0
 Port # Comp= None
Source: IP Addr= 0.0.0.0
 IP Mask= 0.0.0.0
 Port #= 0
 Port # Comp= None
TCP Estab= N/A
More= No Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

Saving to ROM. Please wait...

Protocol and device rule cannot be active together

To separate the device and protocol filter categories; two new menus, Menu 11.5 and Menu 13.1, have been added, as well as some changes made to the Menu 3.1, Menu 11.1, and Menu 13. The changed fields are marked **black** in the following menus:

Menu 3.1:

Menu 3.1 - General Ethernet Setup

Input Filter Sets:
protocol filters= 2
device filters=
Output Filter Sets:
protocol filters=
device filters=

Menu 11.1:

Menu 11.1 - Remote Node Profile

Rem Node Name= abc	Edit PPP Options= No
Active= Yes	Rem IP Addr=
Call Direction= Outgoing	Edit IP= No
Incoming:	Telco Option:
Rem Login= N/A	Transfer Type= 64K
Rem Password= N/A	Allocated Budget(min)= 0
Rem CLID= N/A	Period(hr)= 0
Call Back= N/A	Nailed-Up Connection= No
Outgoing:	Session Options:
My Login= xyxw	Edit Filter Sets= No
My Password= *****	Idle Timeout(sec)= 300
Authen= CHAP/PAP	
Pri Phone #= 140812345678	
Sec Phone #= 140822345678	

Press ENTER to Confirm or ESC to Cancel:

Menu 11.5:

Menu 11.5 - Remote Node Filter

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

Menu 13:

Menu 13 - Default Dial-in Setup

Telco Options:	IP Address Supplied By:
CLID Authen= None	Dial-in User= Yes
	IP Pool= Yes
PPP Options:	IP Start Addr= 123.234.111.163
Recv Authen= CHAP/PAP	IP Count(1,2)= 2
Compression= Yes	
Mutual Authen= No	Session Options:
PAP Login= N/A	Edit Filter Sets= No
PAP Password= N/A	
Multiple Link Options:	
Max Trans Rate(Kbps)= 128	
Callback Budget Management:	
Allocated Budget(min)=	
Period(hr)=	

Menu 13.1:

Menu 13.1 - Default Dial-in Filter

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

SMT will also prevent you entering a protocol filter set configured in Menu 21 to the **device filters** field in Menu 3.1, 11.5, or 13.1, or entering a device filter set to the **protocol filters** field. Even though SMT will prevent the inconsistency from being entered in v2.21, it is unable to resolve the intermixing problems existing in the filter sets that were configured before. Instead, when v2.21 translates the old configuration into the new format, it will verify the filter rules and log the inconsistencies. Please check the system log (Menu 24.3.1) before putting your device into production.

Running the Prestige with wrong filter rules may cause it to keep the ISDN line perpetually active, and/or allow undesired traffic to pass to the outside world, and receive unwanted outside traffic. The first case may incur an enormous ISDN bill; the second may be a data security hazard.

In order to avoid operational problems later, the Prestige will disable its routing/bridging functions if there is an inconsistency among its filter rules.

Proofread your filter rules even if there is no warning message in system log, and observe the router's behavior carefully after upgrading/installation.

P100/P100IH ISDN EPA Mechanism is Moved to PC

The CI (Command Interpreter, menu 24.8) command, "isdn ana display", is disabled in this release. A new CI command "isdn fw ana dump" is added for displaying the ISDN raw trace data. "isdn ana display" could not work with Telnet before, but "isdn fw ana dump" works fine with Telnet. So you do not have to rely on terminal emulator via serial port to capture the ISDN trace any more.

A new DOS tool - **epapc**, will be used to decode the ISDN raw trace data into meaningful Q.921 and Q.931 fields. **epapc** is part of this release. If you have difficulties to run **epapc**, please send the raw ISDN trace to ZyXEL support for decoding. The proper steps to take the raw ISDN trace are:

1. issue "isdn fw ana on" to enable ISDN trace function
2. perform the tests for capturing the interested ISDN information
3. issue "isdn fw ana off" to disable ISDN trace function
4. issue "isdn fw ana dump" to dump the ISDN trace information on screen
 - press <Enter> to display all of the ISDN trace information on screen
 - press <space bar> to display the ISDN trace information on screen page by page

Enhancement Details

More Remote Nodes and IP Static Routes

In this release, the number of remote nodes and numbers of IP static routes have been increased as following:

Model	Number of remote nodes	IP static routes
P100IH	8	8

Easy Installation

Factory Default Values

Factory default values are stored in ROMFILE provided by ZyXEL. The factory default values in them have been optimized for Windows Internet connection. Two sets of filter rules have been configured in Menu 21 to prevent NetBIOS traffic from triggering calls. The default filters are shown below:

Menu 21:

Menu 21 - Filter Set Configuration			
Filter Set #	Comments	Filter Set #	Comments
1	NetBIOS_WAN	7	
2	NetBIOS_LAN	8	
3		9	
4		10	
5		11	
6		12	

Menu 21.1 (NetBIOS WAN):

Menu 21.1 - Filter Rules Summary						
#	A	Type	Filter Rules			M m n
1	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137			N D N
2	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138			N D N
3	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139			N D N
4	Y	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137			N D N
5	Y	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138			N D N
6	Y	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139			N D F

Menu 21.2 (NetBIOS LAN):

Menu 21.2 - Filter Rules Summary						
#	A	Type	Filter Rules	M	m	n
1	Y	IP	Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53	N	D	F
2	N					
3	N					
4	N					
5	N					
6	N					

The filter set, NetBIOS_LAN, is inserted in **protocol filters** field under **Input Filter Sets** in Menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.

Menu 3.1:

Menu 3.1 - General Ethernet Setup

Input Filter Sets:
protocol filters= 2
device filters=
Output Filter Sets:
protocol filters=
device filters=

The filter set, NetBIOS_WAN, is inserted in ***protocol filters*** field under ***Call Filter Sets*** in Menu 11.5 to block local NetBIOS traffic from triggering calls to ISP.

Menu 11.5 of ISP remote node:

Menu 11.5 - Remote Node Filter

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

DHCP Server

By default, Prestige is now configured as a DHCP server. The range of IP address pool is from 192.168.1.33 to 192.168.1.64. The DNS Proxy feature is enabled. Please refer to the DNS Proxy sub-section for details.

Menu 3.2:

Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP Setup:

DHCP= **Server**

Client IP Pool Starting Address= **192.168.1.33**

Size of Client IP Pool= **32**

Primary DNS Server= **0.0.0.0**

Secondary DNS Server= 0.0.0.0

TCP/IP Setup:

IP Address= **192.168.1.1**

IP Subnet Mask= **255.255.255.0**

RIP Direction= **Both**

Version= **RIP-1**

SUA and Dynamic IP Address

By default, both SUA and dynamic IP address are enabled. By utilizing the factory default configuration, it will be easy to most of new customers to start to browse the Internet in minutes.

Menu 4:

Menu 4 - Internet Access Setup

ISP's Name= *ChangeMe*

Pri Phone #= 1234

Sec Phone #=

My Login= *ChangeMe*

My Password= *****

Single User Account= **Yes**

IP Addr= **0.0.0.0**

Telco Options:

Transfer Type= 64K

Multilink= Off

Idle Timeout= 300

DNS Proxy

If enabled, DNS Proxy will allow the Prestige to act as the DNS server for the local network. The Prestige will get the IP address of the actual DNS server from the remote site via IPCP negotiation. Note this feature only works if the remote site supports RFC 1877.

I. Configuring the DNS Proxy

DNS Proxy is enabled only if the selection of the **DHCP** field under **DHCP Setup** in Menu 3.2 is **Server** and the **Primary DNS Server** field in Menu 3.2 is set to **0.0.0.0**. (This is factory default). If DNS Proxy is enabled, the Prestige will assign its IP address as the Primary DNS in the responses to DHCP requests on the local network. SMT enforces the consistency between the **Primary DNS server** and **Secondary DNS server** fields in Menu 3.2 by skipping **Secondary DNS Server** field if the IP address of the **Primary DNS Server** field is 0.0.0.0.

If the selection of the **DHCP** field under **DHCP Setup** in Menu 3.2 is **None**, both of DHCP Server and DNS Proxy functions are disabled. Prestige will assign the values entered in **Primary DNS server** and **Secondary DNS server** fields in Menu 3.2 to the responses to the DHCP requests on the local network if DHCP Server function is enabled.

II. DNS Proxy Functional Flows

If DNS Proxy is enabled, Prestige will perform the following functions after receiving a DNS request from local network:

1. If there is no ISP configuration (default remote node), this DNS request packet will be discarded. Otherwise, continue.
2. Save this DNS request in an internal table.
3. If the connection to ISP is not up, Prestige will attempt to bring up the connection and negotiate with the remote site for the DNS server. Otherwise, continue.
4. If there is no DNS server negotiated on the connection to ISP, Prestige will discard this DNS request from the internal table. Otherwise, continue.
5. Replace the source IP address of the DNS request with the Prestige's own WAN IP address and forward this new DNS request to the ISP DNS server.
6. Match the DNS response from the ISP DNS server to the original DNS request in the internal table. Replace the destination IP address of the DNS response with the original client's IP address and forward this new DNS response to the original client.

Menu 11.1:

Menu 11.1 - Remote Node Profile	
Rem Node Name= abc	Edit PPP Options= No
Active= Yes	Rem IP Addr= 0.0.0.0
Call Direction= Outgoing	Edit IP= No
Incoming:	Telco Option:
Rem Login= N/A	Transfer Type= 64K
Rem Password= N/A	Allocated Budget(min)= 0
Rem CLID= N/A	Period(hr)= 0
Call Back= N/A	Nailed-Up Connection= No
Outgoing:	Session Options:
My Login= scci	Edit Filter Sets= No
My Password= *****	Idle Timeout(sec)= 300
Authen= CHAP/PAP	
Pri Phone #= 140812345678	
Sec Phone #= 140822345678	
Press ENTER to Confirm or ESC to Cancel:	

Nailed-up Function Notes:

Because only two B channels are available for the 8/12 remote nodes, the Prestige **always** starts to dial the first two remote nodes with the nailed-up connection requirement.

If it fails to establish a nailed-up connection (i.e. the call does not complete, or the session does not authenticate), the Prestige will keep attempting to connect to the same remote node, until the connection succeeds or exceeds the value set in **Retry Counter** field in Menu 24.9.1. This remote node is still under the budget control set in **Allocated Budget** and **Period** fields under **Telco Option** in Menu 11.1.

A remote node set as a nailed-up connection has no priority over any other remote nodes, except it keeps attempting until the connection succeeds. In other words, it is possible that other remote node connections may be established before the nailed-up connections. (i. e. First come, first serve.)

If a nailed-up connection is manually dropped, or lost from a line interruption, it will redial to reestablish the connection. But as above, it may fail if another other connection has already occupied the channel(s).

No idle timeout applies to nailed-up connections.

MP configuration is allowed to a nailed-up remote node. Each link of the MP will compete for the B-channel resources with other nailed-up or non nailed-up remote node -- again first come, first serve.

Backup and Restore Configuration File via LAN or WAN

With the stand-alone Java based utility, PCT (Prestige Configuration Transfer), you can backup and restore your configuration file via LAN or WAN. Please refer to the PCT release notes for more information.

Upgrade P100IH Firmware via LAN

With PNC, you can upgrade P100IH firmware over the local LAN. (Attempting to upgrade a remote Prestige via the ISDN WAN is **not** recommended, even though it may succeed.) In this release, this feature only applies to P100IH model. Please refer to PCT release notes for more information.

DSS-1 ISDN Supplemental Services

Background

Advanced ISDN Features are supported by Prestige. The relationship among the advanced ISDN features and switch types is:

Table 1. Advanced ISDN features vs. ISDN variances:

Feature:	USA	DSS-1
Incoming Call Bumping (MP)*	y	y
Outgoing Call Bumping (MP)*	y	y
Call Waiting/Call Hold/Call Retrieve	y+	y+
Three Way Calling (Conference/Transfer/Drop)	y+	y
Call Forwarding	y+	y
Reminder Ring	y+	n

Notes:

* - feature supported since v1.3

y+ - feature supported since v1.5

y - feature supported in this release

n - feature not supported

Before You Begin

ISDN Supplemental Services refers to Call Waiting/Call Hold/Call Retrieve, Three Way Calling (Conference/Transfer/ Drop), Call Forwarding, and Reminder Ring on the Prestige POTS ports. There are services on the serving Central Office switch that works in cooperation with the Prestige software must first be enabled. These services usually cost you extra charges in addition to your monthly payment.

Additional Call Offering (ACO) (in Europe the same service is better known as Call Waiting? is required to be subscribed on your ISDN line in order to utilizing the Call Waiting/Call Hold/Call Retrieve feature. Flexible Calling is required on your ISDN line in order to using the Three Way Calling (Conference/Transfer/ Drop) feature. You may want to check with your PTT to confirm if these services are available to you.

Call Waiting/Call Hold/ Call Retrieve

ISDN Call Waiting/Call Hold/ Call Retrieve allows user to place an active voice call on hold, switch to another call, and retrieve the original call.

Menu 2.1 -- ISDN Advanced Setup

Phone 1 Call Waiting= Enable/Disable
Phone 2 Call Waiting= Enable/Disable
Calling Line Indication = Enable/Disable

By toggling the **Phone 1 Call Waiting** and **Phone 2 Call Waiting** fields, user can enable and disable the Call Waiting/Call Hold/ Call Retrieve feature on the POTS ports. The default value is enable to this feature.

The **Calling Line Indication**, or Caller ID, governs whether the other party can see your number when you call. If set to **Enable**, the Prestige sends the caller ID and the party you call can see your number. If it is set to **Disable**, the caller ID is blocked ID and the party you call can not see your number.

How to use Call Waiting/Call Hold/ Call Retrieve feature:

Put your current call on hold and answer the incoming call - after hearing the call waiting indicator tone, press and immediately release the flash hook button on your telephone.

Put your current call on hold and switch to another call - press and immediately release the flash hook button on your telephone.

Hang up your current call before answering the incoming call hang up the phone and wait for the phone to ring. Then answer the incoming call.

Hang up on the current active call and switch back to the other call ?hang up the phone and wait for the phone to ring. Then pick up the phone to return to the other call.

Why Call Waiting does not work as expected:

1. An incoming caller will receive a busy signal if:
you have two calls (one active and one on hold; or both actives by using Three Way Calling) on the Directory (Phone) number the incoming caller is attempting to reach.
you are dialing out by using the Directory (Phone) number the incoming caller is attempting to reach, but have not yet established a connection.
2. If no action is taken (call waiting indicator tone is ignored) to pickup the call, the call waiting tones will disappear after about 20 seconds.

Three Way Calling (Conference/Transfer/Drop)

The Three Way Calling feature allows you to add the third party to an existing call. This service must be subscribed from your PTT.

How to Add the Third Party to the Existing Call

If you wish to add the third party to an existing call, the steps are:

1. Press the flash hook button and immediately release it to put the existing call on hold and receive a dial tone.
2. Dial the third party.
3. Inform the third party about the conference.
4. When you are ready to conference the call, press the flash hook button and immediately release it to establish a Three Way Conference Call.

If you wish to cancel your attempt for some reason (the third part line is busy, or no one answer), just hang up the phone and pick it back up after the phone ringing.

How to Remove a Party from the Three Way Calling

If you wish to drop the last one added to the Three way calling call, just press the flash key. The last call that was added to the conference will be dropped.

If you wish to drop yourself from the conference call, but allow the other two callers to remain connected. Just hang up your phone. If the other two remain on the line, your drop will not impact their connection.

Call Transfer

Call Transfer is a variance of Three Way and allows you to transfer an active call to a third party. If you wish to transfer an active call to a third party and inform him about the transferred call, the steps are:

1. Press flash to immediately put the existing call on hold and receive a dial tone.
2. Dial the third party.
3. Inform the third party about the transfer call.
4. Press the flash hook button and immediately release it to establish a Three Way Conference
5. Call.
6. Hang up the phone to complete the transfer.
7. If you wish to do a blind transfer to the third party, the steps are:
8. Press flash to immediately put the existing call on hold and receive a dial tone.
9. Dial the third party.
10. Before the third party picks up the call, you can transfer the call by pressing the flash and
11. hanging up. The call will be automatically transferred.

Call Forwarding

The Call Forwarding feature is supported by ISDN switch directly. The Call Forwarding feature of the POTS port can be activated and deactivated by using the phone set. The Call Forwarding is a telephone feature and will not impact incoming data call. Please request your PTT for the instruction activate or deactivate the Call Forwarding feature.

This document describes the enhancements in the ZyXEL Prestige product line since the last manual printing.

Bug fixes

This list describes the bug fixed since version 2.20 beta version.

1. Make DOVBS/56K MP connection, the outgoing second call is always 64K.
2. The second phone number assigned is always phone 1 # when BAP start negotiation.
3. Get the wrong CLID. If the CLID authentication is required, the call will be rejected.
4. The idle timeout field of SMT menu 4 should be not available if nailed-up connection is enabled.
5. Fix only CLID number can be displayed problem.
6. Change timeout waiting for layer 1 activation from 20 seconds to 40 seconds.
7. There could be no busy tone after silent timer timeout for answering machine. User may define the silent time by adding initial string in CI command "isdn ini set s78.5=nS78.6=m", then reboot system to function, which n=0, m=0 is default, n=1, m=0 is 5 seconds, n=0, m=1 is 10 seconds, and n=1, m=1 is 15 seconds.
8. Enable nailed-up connection in SMT menu 11, the idle timeout field should be not available.
9. Fix MP connection may fail after loopback test.
10. Enhance "sys trcl call" display.
11. Fix wrong connect speed "64K" display when connect DOVBS and 56K.
12. Fix tracelog bug when CLID matched.
13. Fix flash key detection bug which can't place call forwarding connect.
14. Off hook could cause router to crash in PNC system maintenance status menu.
15. Fix the hang-up problem of transferring ftp big files or a lot of small files.
16. AT&T NI-1 CLID display problem in menu 24.1.
17. Can't link up with AT&T p-2-p switch.
18. Power up system with no Menu 2 configuration, but Menu 24.1 shows 'idle'.

19. Sometimes, ISDN of USA version will report redundant information and cause initialize fail.
20. Enhance leased line connection for USA version. User can't manually drop leased connection
21. From SMT menu 24.1, 24.4 or CI command ("device channel drop bri0 | bri1 | all").
22. The prompt size '>' in CI mode will disappear if there are dots trail of system name.
23. Dial a null phone number will cause router crash.

Known Problem List

1. For Northern American version, the Prestige may drop both data channels if both of the POTS port telephones are off hook simultaneously while an MP call is in progress.
2. For DSS-1 version, Prestige may stop placing outgoing data calls after Call Waiting/Call
3. Hold/ Call Retrieve scenario if both of POTS ports are assigned the identical phone number. When it happens, the B-channel status shown on Menu 24.1 is wrong.
4. For the Northern American version, it may have problems to place voice call to far-end (hear busy tone) via second POTS ports even though it works by using the first POTS port.
5. Prestige performance will be degraded if there exists a telnet session in Menu 24.1 via LAN at the same time.
6. For old P100ih models with 0.5M DRAM, you may have difficulties to backup configuration due to system unable to allocate enough memory to perform the function. The workaround is to use ZyXEL's Prestige Configuration Tool (PCT) or ZyXEL's Prestige Network Commander (PNC) to perform backup function in this case.
7. Incompatible DHCP leased time with Linux machine.
8. The supplemental service blind transfer feature may have problem to work.

To Upgrade Prestige

Get the files from ZyXEL anonymous FTP server (ftp.zyxel.com). Upgrade your Prestige by following the instructions for your model:

P100IH

Versions:

RAS S/W Version - V2.21(G.01) | 11/18/99
 ISDN F/W Version - USA : V 09C

RAS and ISDN firmware files:

p100ihpa.bin (for Northern America)

Commands:

ATBAx: Where x = baud rate

options available are:

1= 38.4K

2= 19.2K

3= 9.6K

4= 57.6K

5= 115.2K

ATUR: Upload Firmware file via XMODEM

Romfile: p100ihpa.rom (for Northern America)

Commands:

ATUR3: Upload Romfile and reset configuration to factory default.