

ZyXEL AES-100 V2.03(AS.0)

Release Notes/Manual Supplement

Date: May 22, 2002

Version:

F/W Version: V2.03(AS.0) | 5/22/2002

This version is the same as V2.03(AS.0)b10

Release by Glen Lin

ZyXEL AES-100 V2.03(AS.0)b10

Release Notes/Manual Supplement

Date: May 21, 2002

Version:

F/W Version: V2.03(AS.0)b10 | 5/21/2002

Minior Changes:

1. Add a hidden command "reboot" to reboot system without saving flash
2. Modify HTP task to wait for ADSL chipset initial complete

Release by Glen Lin

ZyXEL AES-100 V2.03(AS.0)b09

Release Notes/Manual Supplement

Date: April 11, 2002

Version:

F/W Version: V2.03(AS.0)b09 | 4/22/2002

Minior Changes:

3. Add a margin (Downstream 50 packets Upstream 500 Cells) while checking PVC to avoid frequent PVC reset

Release by Glen Lin

ZyXEL AES-100 V2.03(AS.0)b08

Release Notes/Manual Supplement

Date: April 11, 2002

Version:

F/W Version: V2.03(AS.0)b08 | 4/11/2002

Minior Changes:

4. Modify xport for close channel error checking
5. Modify TI driver to yield itself before polling to wait TI chipset response
6. Modify reset PVC program flow to prevent frequent reset PVC

Release by Glen Lin

ZyXEL AES-100 V2.03(AS.0)b07

Release Notes/Manual Supplement

Date: March 27, 2002

Version:

F/W Version: V2.03(AS.0)b07 | 3/27/2002

Minior Changes:

7. The original reset pvc mechanism cause the throughput slow down. We modify the pooling interval from 10 to 2 sec but one time only process one port not all ports.
8. Snmp(rose) wait a while for clients (and ip) to send cold start up trap. But the waiting interval is too short (5 sec) to work. I change it to 10 sec.

ZyXEL AES-100 V2.03(AS.0)b06

Release Notes/Manual Supplement

Date: March 15, 2002

Version:

F/W Version: V2.03(AS.0)b06 | 3/15/2002

Minior Changes:

9. Modify the reset pvc mechanism to workaround the packet can not transmit in down stream and up stream direction.

ZyXEL AES-100 V2.03(AS.0)b05

Release Notes/Manual Supplement

Date: March 7, 2002

Version:

F/W Version: V2.03(AS.0)b05 | 3/7/2002

Major Changes:

10. Add the reset pvc mechanism to workaround the packet can not transmit in down stream direction.
 - Add the error log to record it.
2. Fix the console hang on cause by error log mechanism.

ZyXEL AES-100 V2.03(AS.0)b02

Release Notes/Manual Supplement

Date: November 27, 2001

Congratulations on your purchase of AES-100 ADSL-Ethernet Switch. AES-100 is an ADSL (Asymmetrical Digital Subscriber Line) to Ethernet switch. It allows you to multiplex traffic from up to 16 ADSL lines to Ethernet network before it is forwarded to the Internet.

ADSL allows the coexistence of broadband data service and conventional voice service over the same telephone line. When deployed together with ZyXEL's ADSL modems, e.g., P642M, and WAN routers, e.g., P1400, the combination forms an integrated solution for providing broadband services to multiple tenant units such as apartments, hotels, offices and campus buildings.

The AES-100 has two slots for the ADSL to Ethernet multiplexer modules. This design provides the flexibility for you to install as few as a single module for the initial deployment and yet still has room to grow as the demand increases.

Each ADSL to Ethernet multiplexer module aggregates traffic from 8 lines to an Ethernet port.

The integrated splitters eliminate the need to use external splitters to separate voice-band and ADSL signals.

This 10/100 Mbps Ethernet port connects the AES-100 to an Ethernet network. With the Ethernet as the backbone, you can create a network that provides ADSL service to hundreds of subscribers.

This document describes the features in the ZyXEL AES-100 product for its V2.03(AS.0)b02 release. The known problem list section describes problems currently under investigation and enhancement during our internal test.

Version:

F/W Version: V2.03(AS.0)b02 | 11/27/2001

Features:

1. 10/100 Mbps auto-sensing Ethernet port.
2. ADSL ports support G.dmt and G.lite.
3. Support IEEE 802.1d transparent bridge.
4. ADSL ports support RFC 1483 Bridge Mode.
5. Support port-based VLAN.
6. Firmware upgrade and configuration backup/restore.
7. Remote manageable.
8. SNMP manageable.
9. Thermal monitoring to notify over-heat.

10. IGMP snooping.
11. IEEE 802.1Q tagging for subscriber identification.
12. Per port MAC filtering to filter out un-allowed packets.
13. UNIX syslog mechanism to log ADSL link on/down events to remote server.
14. System error log mechanism to log system events locally.
15. Secured access hosts protection.

Wish List:

1. SNMP management objects about ADSL lines (RFC 2662) are not support in this version.
2. Static filtering of IEEE 802.1d is not support in this version.
3. IEEE 802.1Q VLAN is not support in this version.

Know Problem List:

1. When the upstream rate of an ADSL port is over **832** Kbps, the upstream bit error rate may be greater than 10^{-7} .

Major Changes:

11. Contents of some configuration files (listed below) changed
 - initbridge
12. New added configuration files (listed below)
 - syscfg

Minor Changes:

1. Support T1.413 mode in “adsl set port(s)” commands.
2. Display link-up elapsed time in “adsl show port(s)” commands.
3. Support “atve” command in booting to show loader’s information.

New Features:

There are some new features to previous versions in this version. Here lists these features.

1. MAC filtering for packets on individual port.
 - Per port enable/disable
 - Per port 5 filtered MAC addresses
2. Secured access host checking on telnet and FTP sessions.
 - Control the access of telnet and FTP
 - 10 secured hosts
3. System error log. The following events will be logged:

- ADSL link on, (port number + sequence number + rates + noise margins + attainable rates)
 - ADSL link down, (port number + sequence number)
 - Console session begin
 - Console session end
 - Telnet session begin
 - Telnet session end
 - Incorrect telnet password
 - Insecure telnet access, (IP address)
 - FTP session begin
 - FTP session end
 - Incorrect FTP password
 - Insecure FTP access, (IP address)
 - FTP image error, (reason)
 - FTP receive file OK, (file name)
 - Out of packet buffer
 - System reboot
4. UNIX syslog. The following events will be logged:
- ADSL link on, (port number + sequence number + rates)
 - ADSL link down, (port number)

Bugs Fixed:

New CLI Commands to Previous Versions:

There is some new CLI commands in this version. Here lists these commands and the details can be found in AES-100 User' Guide.

1. MAC filtering Configuration Commands Group:

- **bridge macfilter** commands :

Syntax:

macfilter [<port>] - Display the MAC filtering status and the fixed source MAC addresses on a port or on all ports if no port specified.

macfilter enable [<port>] - Enable the MAC filtering feature on a specific port or on all ports if no port specified.

macfilter disable [<port>] - Disable the MAC filtering feature on a specific port or on all ports if no port specified.

macfilter add <port> <mac> - Add a source MAC address fixed on the specified port.

macfilter delete <port> <mac> - Remove a configured source MAC address on the specified port.

where

<port> = bridge port number

<mac> = The source MAC address with "00:a0:c5:12:34:56" format

2. System error log Commands Group:

- **sys errlog** commands :

Syntax:

errlog clear - Clear system error log.

errlog display - Display system error log.

NOTE: System will store current error log in to file "errorlog" when restart. You can use "fm cat errorlog" command to view previous error log.

3. UNIX syslog Commands Group:

- **sys syslog** commands :

Syntax:

syslog - Display current settings.

syslog <mode> - Enable/Disable syslog.

syslog facility <facility> - Set syslog facility.

syslog server <server IP> - Set UNIX syslog server.

where

<mode> = "enable" or "disable"

<facility> = "local1" to "local7"

<server IP> = IP address of syslog server

4. Secured access hosts Commands Group:

- **sys secured host** commands :

Syntax:

secured host - Display current settings.

secured host <mode> - Enable/Disable secured host checking.

secured host add <host IP> - Add a secured host.

secured host delete <host IP> - Delete a secured host.

where

<mode> = "enable" or "disable"

<host IP> = IP address of secured host

SNMP Related Information:

1. OIDs:

- sysObjectID : 1.3.6.1.4.1.890.1.5.9
- mtuSystemCurrentStatus : 1.3.6.1.4.1.890.1.5.1.1.1
- mtuSystemTemperature : 1.3.6.1.4.1.890.1.5.1.1.3
- mtuTraps : 1.3.6.1.4.1.890.1.5.1.2

2. Enterprise Trap IDs:

- overheat trap : 3
- overheatOver trap : 4

3. Support Traps:

- Cold start.
- ADSL ports link up/down.
- Authentication failure.
- Overheat/overheatOver.

Firmware Upgrade

The AES-100 uses FTP to upgrade firmware in run-time through its built-in FTP server. To upgrade the firmware, first download the **firmware** (the file with “**img**” extension name) from the ZyXEL web site and store it on your computer. You can use any FTP client (for example, [ftp.exe](#) in Windows) to upgrade AES-100 firmware. The upgrade procedure is as follows:

On management station:

```
C:\> ftp <AES-100 IP address>
User : <Enter>
Password: 1234
230 Logged in
ftp> put 201AS0b1.img image
ftp> quit
```

Where

- User name : just press <Enter>
- Password : the management password, 1234 by default
- 201AS0b1.img : the name of firmware file you want to upgrade
- image : the internal firmware name in AES-100

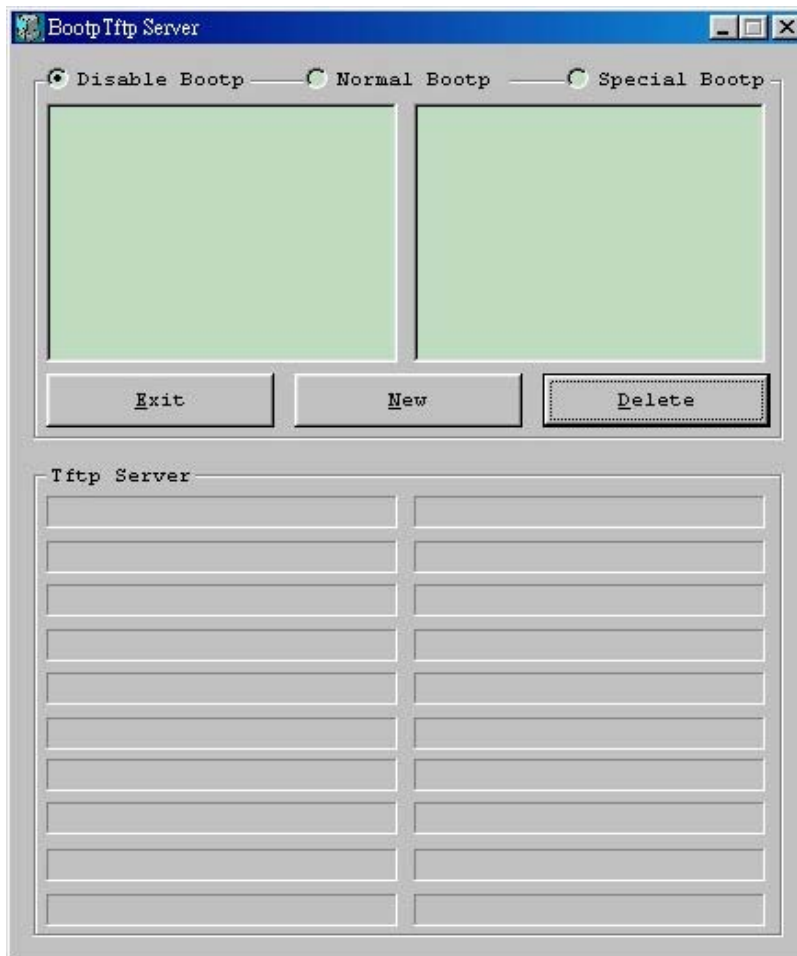
On AES-100:

After management station successfully put firmware and quit the FTP client application, waiting for updating completed and AES-100 will reboot automatically. **Do not power off** AES-100 during updating process is in progress.

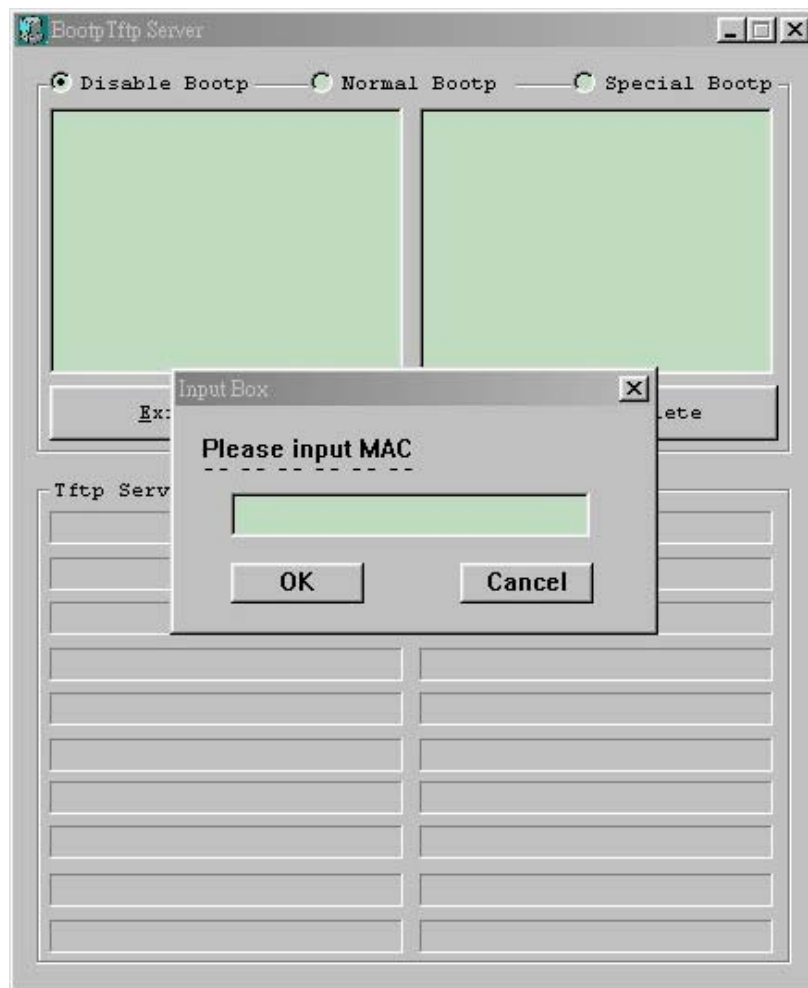
Firmware Recovery

When the firmware in non-volatile memory is damaged, the AES-100 uses BOOTP/TFTP to recover in boot-time through its built-in BOOTP/TFTP client. To recover the firmware, first download the **recovery firmware** (the file with “**bin**” extension name) from the ZyXEL web site and store it on your computer. You can use any BOOTP/TFTP server (for example, BootpTftp.exe) to recover AES-100 firmware. The recovery procedure for server BootpTftp.exe is as follows:

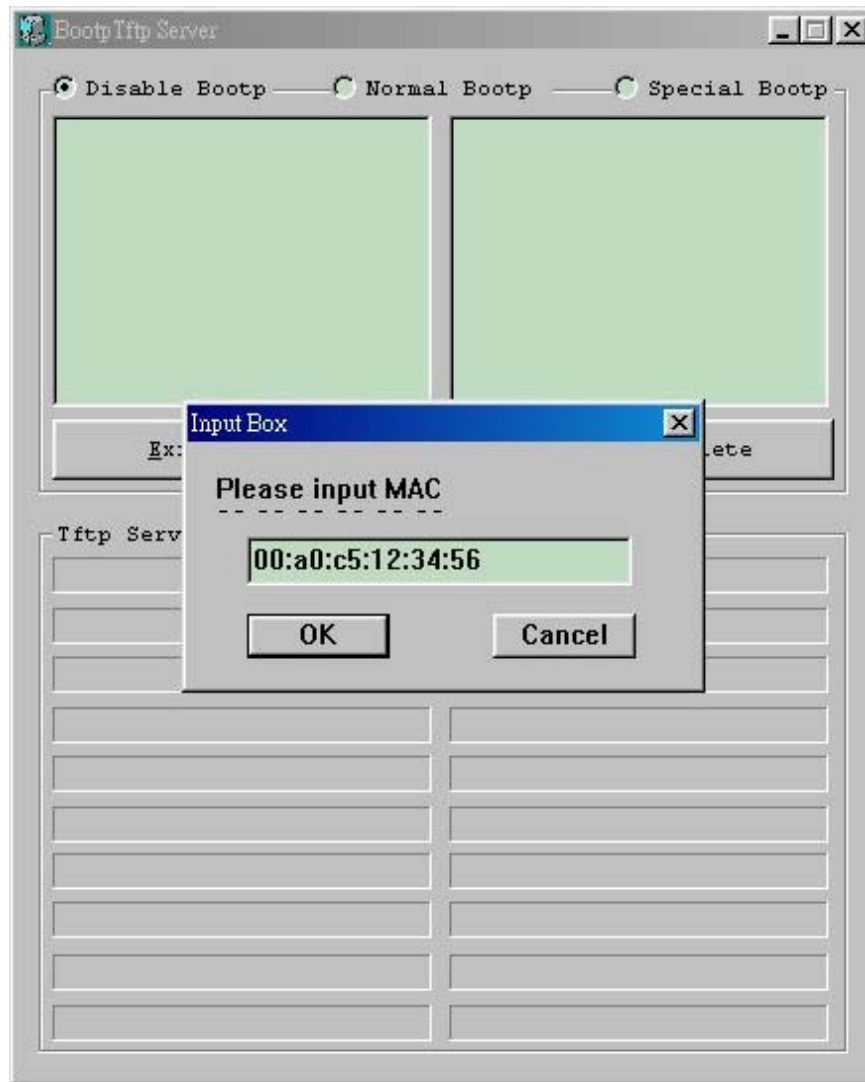
1. Connect your AES-100's LAN port to a PC's LAN port through Ethernet cable.
2. Connect your AES-100's console port to a PC's serial port through RS-232 cable.
3. Run any terminal emulation program, e.g., Windows' built-in HyperTerminal, with the following parameters:
 - VT100 terminal emulation
 - 9600 bps
 - No parity, 8 data bits, 1 stop bit
 - No flow control
4. Run BootpTftp.exe, you will see the following window



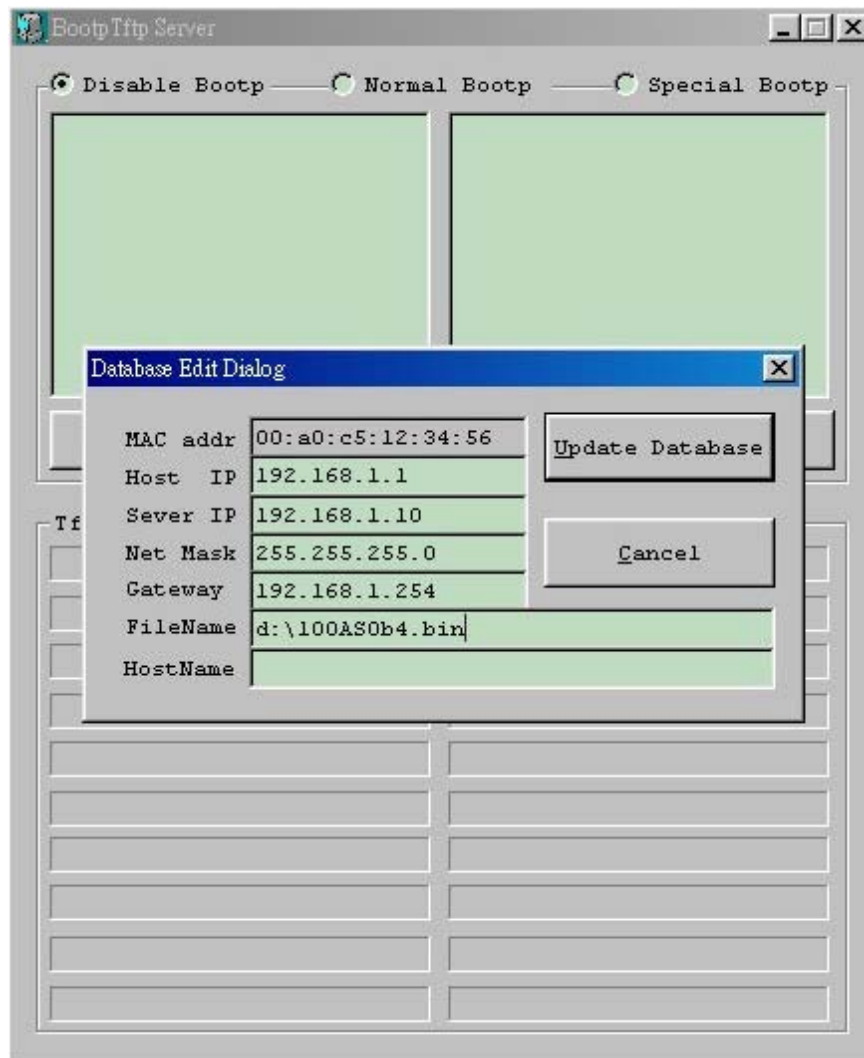
5. Click the “New” button to create a MAC address entry. The “Input Box” will pop up.



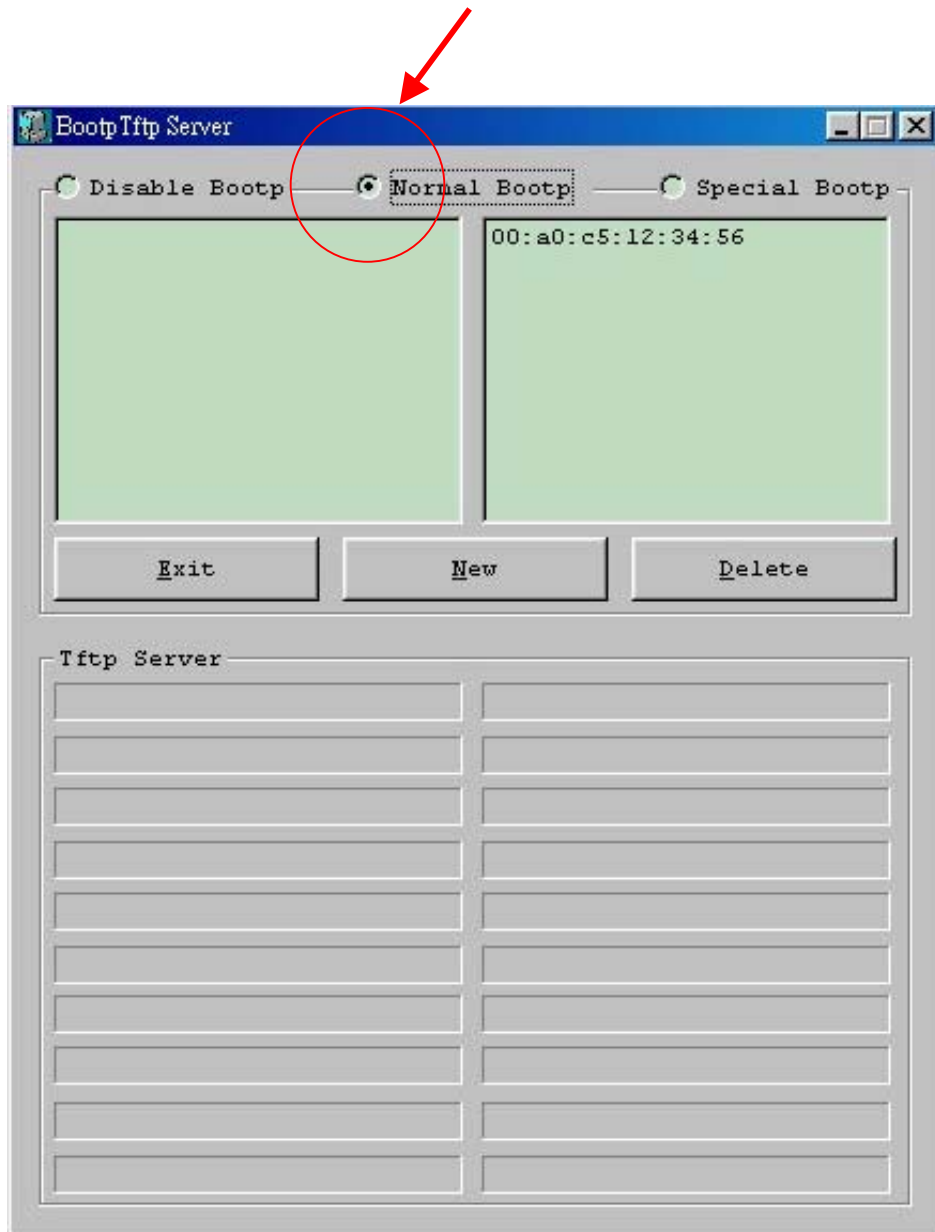
6. Input MAC address of AES-100 and then click "OK". You can find the MAC address of AES-100 on boot console of AES-100.



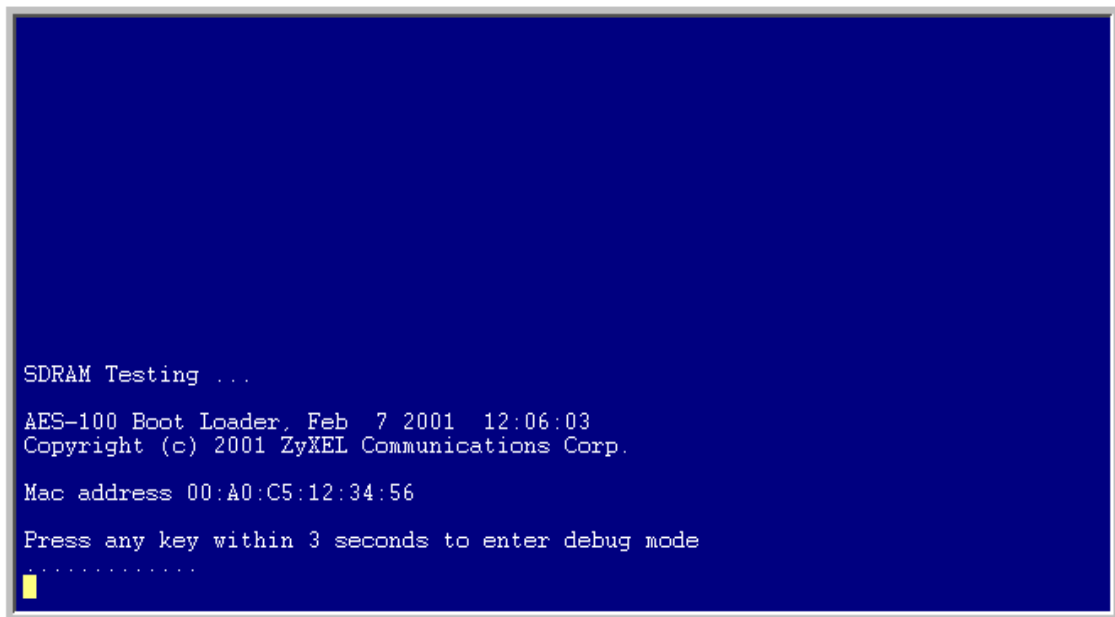
7. Set up host address (the IP address you want to assign to AES-100), server address (the IP address of this PC), net mask, gateway and filename (the new firmware name). And then click "Update Database".



8. Choose "Normal Bootp" to enable normal BOOTP/TFTP function.



9. Power on AES-100 and press any key within 3 seconds. You will see the following in console window:



```
SDRAM Testing ...  
AES-100 Boot Loader, Feb  7 2001 12:06:03  
Copyright (c) 2001 ZyXEL Communications Corp.  
Mac address 00:A0:C5:12:34:56  
Press any key within 3 seconds to enter debug mode  
.....  
█
```

10. Type “**atnb**” and then press Enter key on AES-100 boot console.
11. Wait for firmware upload to complete.
12. Use the following command sequence on AES-100 to write new firmware to flash memory.
 - 192.168.1.1> **flashfs**
 - 192.168.1.1 flashfs> **update**
13. Wait for the update to complete and then restart AES-100.

Configuration Backup/Restore

The AES-100 uses FTP to backup/restore configuration through its built-in FTP server. You can use any FTP client (for example, [ftp.exe](#) in Windows) to backup/restore AES-100 configuration. The procedure is as follows:

On management station:

```
C:\> ftp <AES-100 IP address>
User : <Enter>
Password: 1234
230 Logged in
ftp> get initadsl
ftp> put resolve
ftp> quit
```

Where

- User name : just press <Enter>
- Password : the management password, 1234 by default
- initadsl : the internal name of ADSL configuration in AES-100
- resolve : the internal name of IP configuration in AES-100

On AES-100:

If configuration restore is performed, after management station successfully put configuration and quit the FTP client application, waiting for updating completed and AES-100 will reboot automatically. **Do not power off** AES-100 during updating process is in progress.

Configuration Files of the AES-100 :

The AES-100 uses configuration files to store the user's settings, so they can be applied the next time the AES-100 is booted. The AES-100 has the following eight important configuration files:

initadsl =	The configuration file for ADSL ports.
resolve =	The configuration file for IP parameters.
initbridge =	The configuration file for bridge settings.
password =	The configuration file for the console and Telnet password.
services =	The configuration file for IP services.
initether =	The configuration file for Ethernet port settings.
snmpinit =	The configuration file for SNMP settings.
snmp.dat =	The configuration file for system related information.

Forget Your Management Password

The AES-100 requires users input the management password during console or telnet login. To manage the AES-100, the system administrator must remember the management password. If the password is forgotten, please contact ZyXEL.
