iPBX30

User Manual

E2883 / December 2006

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

Congratulations on buying the ASUS iPBX30!

Your Local Area Network (LAN) will now be able to access the Internet using your high-speed broadband connection such as those with ADSL or cable modem. At the same time, you can have a 30-user SIP-based IP PBX functionality.

This User Manual guides you in setting up the iPBX30, and customizing its configuration to get the most out of this product.

1.1 Features

- LAN: 4-port Fast Ethernet switch
- WAN: Dual 10/100Base-T Ethernet ports to provide Internet access for all computers on your LAN
- Firewall, and NAT (Network Address Translation) functions to provide secure Internet access for your LAN
- Automatic network address assignment through DHCP Server
- Services including IP route, DNS and DDNS configuration
- User configurable dual-WAN or WAN plus DMZ support
- USB storage support
- SIP based IP-PBX support allowing up to30 SIP clients registration
- Support SIP trunking to ITSP and SIP gateway routing
- IP-PBX supports voice mail and email notification
- Voice codec support : G.711/G.729
- DTMF method support : In-band, RFC2833, Info
- Configuration program accessible via a web browser, such as Microsoft Internet Explorer 6.0 or newer.

1.2 System Requirements

To use the iPBX30, you must have:

- ADSL or cable modem and the corresponding service up and running, with at least one public Internet address assigned to your WAN

- One or more computers each containing an Ethernet 10Base-T or 100Base-T or 1000Base-T network interface card (NIC)
- (Optional) An Ethernet hub/switch, if you want to connect the router to more than four computers on an Ethernet network.
- For system configuration using the web-based GUI: a web browser such as Internet Explorer 6.0 or later.

1.3 Using this Document

1.3.1 Notational conventions

- Acronyms are defined the first time they appear in the text.
- The iPBX30 is sometimes referred to as the “router” or the ”gateway”.
- The terms LAN and network are used interchangeably to refer to a group of Ethernet-connected computers at one site.
- Sequence of mouse actions is denoted by the “->” character. For instance, **System -> Network Setup** means click the **System menu** and then click the **Network Setup** submenu.

1.3.2 Typographical conventions

- **Boldface** type text is used for items you select from menus and drop-down lists, and text strings you type when prompted by the program.

1.3.3 Special messages

This document uses the following icons:

📝 *Note: Provides clarification or information on the current topic.*

📖 *Definition: Explains terms or acronyms that may be unfamiliar to many readers. These terms are also included in the Glossary.*

⚠ *Warning: Provides messages of high importance, including messages relating to personal safety or system integrity.*

Chapter 2 Getting to Know your iPBX30

2.1 Parts List

Your iPBX30 package include these items:

- iPBX30
- AC adapter
- Ethernet cable (“straight-through” type)

2.2 Hardware Features

Your iPBX30 contains these hardware features:

LAN

- 4-port Fast Ethernet switch
- Auto speed negotiation

WAN

- Dual 10/100M Ethernet ports
- Auto MDI/MDIX

2.3 Software Features

2.3.1 NAT Features

iPBX30 provides Network Address Translation (NAT) to share a single high-speed Internet connection and to save the cost of multiple connections required for the hosts on the LAN segments connected to it. This feature conceals network address and prevents them from becoming public. It maps unregistered IP address of hosts connected to the LAN with valid ones for Internet access. iPBX30 also provides reverse NAT capability, which enables users to host various services such as e-mail servers, web servers, etc. The NAT rules drive the translation mechanism. The following types of NAT are supported by iPBX30.

- **NAPT (Network Address and Port Translation)**

  Also called IP Masquerading or ENAT (Enhanced NAT). Maps many internal hosts to only one globally valid IP address. The mapping usually contains a pool of network ports to be used for translation. Every packet is translated with the globally valid IP address; the port number is translated with a free pool from the pool of network ports.

- **Reverse NAPT**

  Also called inbound mapping, port mapping,or virtual server. Any packet coming to the router can be relayed to an internal host based on the protocol, port number and/or IP Address specified in the rule. This is useful when multiple services are hosted on different internal hosts.

2.3.2 Firewall Features

The firewall as implemented in iPBX30 provides the following features to protect your network from being attacked and to prevent your network from being used as the springboard for attacks.

- Stateful Packet Inspection
- Packet Filtering (ACL)
- Defense against Denial of Service Attacks
- Log

2.3.2.1 Stateful Packet Inspection

The iPBX30 Firewall uses “stateful packet inspection” that extracts state-related information required for the security decision from the packet and maintains this information for evaluating subsequent connection attempts. It has awareness of application and creates dynamic sessions that allow dynamic connections so that no ports need to be opened other than the required ones. This provides a solution which is highly secure and that offers scalability and extensibility.

2.3.2.2 Packet Filtering – ACL (Access Control List)

ACL rule is one of the basic building blocks for network security. Firewall monitors each individual packet, decodes the header information of inbound and outbound traffic and then either blocks the packet from passing or allows it to pass based on the contents of the source address, destination address, source port, destination port, and protocol defined in the ACL rules. ACL is a very appropriate measure for providing isolation of one subnet from another. It can be used as the first line of defense in the network to block inbound packets of specific types from ever reaching the protected network.

The iPBX30 Firewall’s ACL methodology supports:

- Filtering based on destination and source IP address, port number and protocol
- Use of the wild card for composing filter rules
- Filter Rule priorities

2.3.2.3 Defense against DoS Attacks

The iPBX30 Firewall has an Attack Defense Engine that protects internal networks from known types of Internet attacks. It provides automatic protection from Denial of Service (DoS) attacks such as SYN flooding, IP smurfing, LAND, Ping of Death and all re-assembly attacks. For example, the iPBX30 Firewall provides protection from “WinNuke”, a widely used program to remotely crash unprotected Windows systems in the Internet. The iPBX30 Firewall also provides protection from a variety of common Internet attacks such as IP Spoofing, Ping of Death, Land Attack, and Reassembly attacks.

The type of attack protections provided by the iPBX30 is listed in the table below.

Table 2.1. DoS Attacks

Type of Attack	Name of Attacks
Re-assembly Attacks	Bonk, Boink, Teardrop (New Tear), Overdrop, Opentear, Syndrop, Jolt, IP fragmentation overlap
ICMP Attacks	Ping of Death, Smurf, Twinge
Flooders	Logging only for ICMP Flooder, UDP Flooder, SYN Flooder
Port Scans	Logging only for TCP SYN Scan, Attacking packets dropped: TCP XMAS Scan, TCP Null Scan, TCP Stealth Scan
Protection with PF Rules	Echo-Chargen, Ascend Kill
Miscellaneous Attacks	IP Spoofing, LAND, Targa, Winnuke

2.3.2.4 Application Level Gateway (ALG)

Applications such as FTP open connections dynamically based on the respective application parameter. To go through the firewall on the iPBX30, packets pertaining to an application, require a corresponding allow rule. In the absence of such rules, the packets will be dropped by the iPBX30 Firewall. As it is not feasible to create policies for numerous applications dynamically (at the same time without compromising security), intelligence in the form of Application Level Gateways (ALG), is built to parse packets for applications and open dynamic associations. The iPBX30 NAT provides a number of ALGs for popular applications such as FTP, and Netmeeting.

2.3.2.5 Log

Events in the network, that could be attempts to affect its security, are recorded in the iPBX30 system log file.

The log maintains a minimum log details such as, time of packet arrival, description of action taken by Firewall and reason for action.

2.4 Finding Your Way Around

2.4.1 Front Panel

The front panel contains LED indicators that show the status of the unit.

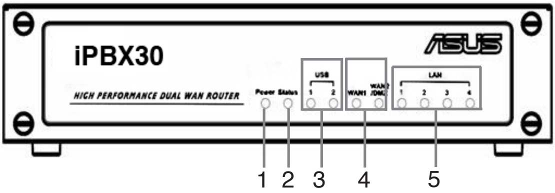


Figure 2.1 Front Panel Label and LEDs

Table 2.2 Front Panel Label and LEDs

	LED	**Color**	**Status**	Indication
1	Power	Green	ON	iPBX30 is powered on.
			OFF	iPBX30 is powered off.
2	Status	Green		
3	USB			Identifies the USB port LEDs.
	1-2	Green	OFF	USB device is not detected.
			ON	USB device is detected.
4	WAN1 and WAN2/DMZ		OFF	No link is detected.
		Green	ON	100Mbps link is detected.
			Blinking	100Mbps activity is detected.
		Amber	ON	10Mbps link is detected.
			Blinking	10Mbps activity is detected.
5	LAN			Identifies the LAN port LEDs.
	1-4		OFF	No link is detected.
		Green	ON	100Mbps link is detected.
			Blinking	100Mbps activity is detected.
		Amber	ON	10Mbps link is detected.
			Blinking	10Mbps activity is detected.

2.4.2 Rear Panel

The rear panel contains the ports for the unit's data and power connections.

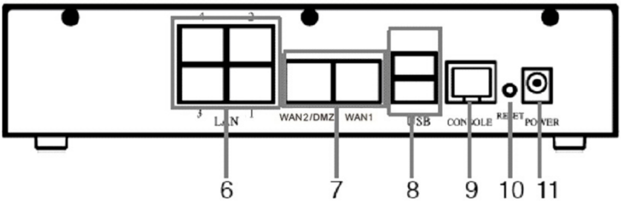
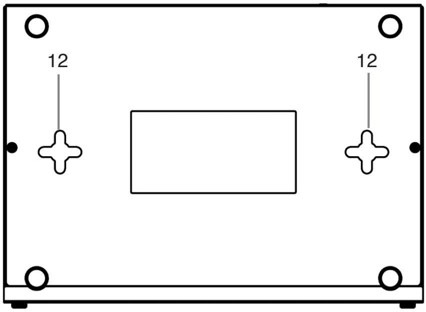


Figure 2.2 Rear Panel Labels and Connectors

Table 2.3 Rear Panel Labels and LEDs

	Connector	Indication
6	1--4	LAN Ports: connect to your PC's Ethernet port, or to the uplink port on your LAN's hub/switch, using the Ethernet cable.
7	WAN1 and WAN2/DMZ	Dual WAN ports or 1 WAN + 1 DMZ: connects to your WAN devices, such as ADSL or cable modem or DMZ network. The DMZ network must be connected to the port labeled as WAN2/DMZ.
8	USB	USB Ports: connect to USB 1.1 OR 2.0 devices
9	Console	Not supported.
10	RESET	Reset Button: 1. Reboot the device 2. Reset the system configuration to factory defaults if pressed for more than 5 seconds.
11	POWER	Power Input Jack: Connect to the supplied AC adapter.

2.4.3 Bottom View



12. Wall Mount Slots: Use these slots to mount iPBX30 on a wall. You can mount the iPBX30 in four orientations: front panel up, rear panel up, left side up or right side up.

2.5 Placement Options

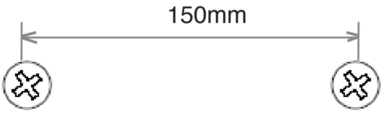
Choose one of the supported placement options for the iPBX30 – desktop placement and wall mount.

2.5.1 Desktop Placement

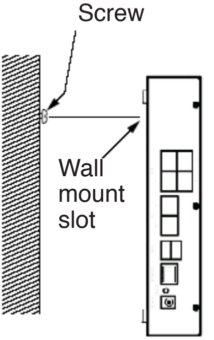
You may place the iPBX30 on any flat surface. The space-saving design of iPBX30 occupies only a small area on your desk.

2.5.2 Wall Mount Instructions:

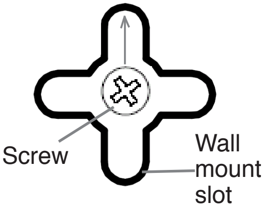
1. Attach two screws on the wall, and with a 150mm distance between the two screws.



2. Align the screws with the wall mount slots as shown below. The wall mount design supports four orientations: rear side up, rear side down, rear side to the left and rear side to the right.



Line up the wall mount slot with both screws.



Maneuver the router so that both screws are inserted into the wall mount slots and then slowly push the router downward as shown in the figure above.

3 Quick Start Guide

This chapter provides basic instructions for connecting the iPBX30 to a computer or a network and to the Internet.

- Part 1 provides instructions to set up the hardware.
- Part 2 describes how to configure Internet properties on your computer(s).
- Part 3 shows you how to configure basic settings on the iPBX30 to get your LAN connected to the Internet.

This chapter assumes that you have already established ADSL or cable modem service with your Internet service provider (ISP). These instructions provide a basic configuration that should be compatible with your home or small office network setup. Refer to the subsequent chapters for additional configuration instructions.

Note: To verify that your setup is working properly, refer to "3.3.2 Testing Your Setup".

3.1 Part 1 — Connecting the Hardware

This section instructs you on how to connect the device to an ADSL or a cable modem (which in turn is connected to a phone jack or a cable outlet), the power outlet, and your computer or network.

Warning: Before you begin, power off all devices, including your computer(s), your LAN hub/ switch (if applicable), and the iPBX30.

Follow the steps that follow for specific instructions.

3.1.1 Step 1. Connecting an ADSL or a cable modem

For the iPBX30: Connect one end of the Ethernet cable to the port labeled WAN on the rear panel of the device. Connect the other end to the Ethernet port on the ADSL or cable modem.

3.1.2 Step 2. Connecting computers or a Network.

If your LAN has no more than four computers, use Ethernet cables to connect computers directly to the built-in switch on the device. You should attach one end of the Ethernet cable to any of the port labeled 1 – 4 on the rear panel of the router and connect the other end to the Ethernet port of a computer.

If your LAN has more than four computers, attach one end of an Ethernet cable to a hub or a switch (probably an uplink port; refer to the hub or switch documentations for instructions) and the other to the Ethernet switch port (labeled 1 – 4) on the iPBX30.

You can use either crossover or straight-through Ethernet cables to connect the built-in switch and computers, hubs or switches as the built-in switch allows connections with either type of cables.

3.1.3 Step 3. Attaching the AC adapter.

Attach the AC adapter to the POWER input jack on the back of the device and plug in the adapter to a wall outlet or a power strip.

3.1.4 Step 4. Powering on iPBX30, the ADSL or cable modem and power up your computers

Plug the AC adapter to the power input jack of iPX30. Turn on your ADSL or cable modem. Turn on and boot up your computer(s) and any LAN devices such as wireless AP, hubs or switches.

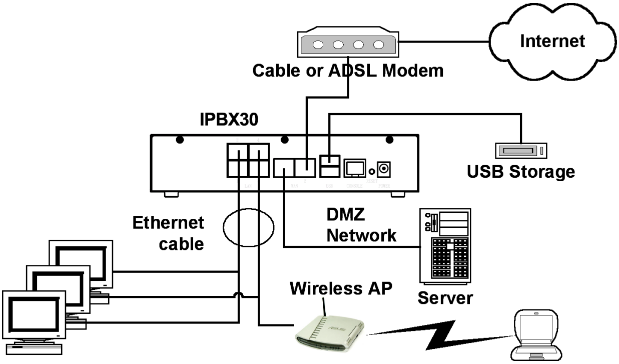


Figure 3.1 Hardware Connections Overview

You should verify the status of the LEDs as indicated in the table below.

Table 3.1 LED Indicators

LED	**Status**
POWER	Solid green indicating that the device is ON. If this light is not on, check if the AC adapter is attached to the iPBX30, and if it is plugged into a power source.
LAN LEDs	Solid green indicating that the device can communicate with your LAN. Flashing when the device is sending or receiving data to or from your LAN computer(s).
WAN	Solid green indicating that the device has successfully established a connection with your ISP. Flashing when the device is sending or receiving data to/from the Internet.

3.2 Part 2 — Configuring Your Computers

This section provides instructions for configuring the network settings on your computers to work with the iPBX30.

3.2.1 Before you begin

By default, the iPBX30 automatically assigns all required network settings (e.g. IP address, DNS server IP address, default gateway IP address) to your PCs. You need only to configure your PCs to accept the network settings provided by the iPBX30.

Note: In some cases, you may want to configure network settings manually to some or all of your computers rather than allow the iPBX30 to do so. See page 18 for instructions.

- If you have connected your PC via Ethernet to the iPBX30, follow the instructions that correspond to the operating system installed on your PC.

3.2.2 Windows® XP PC:

1. In the Windows task bar, click the <**Start**> button, and then click Control Panel.
2. Double-click the **Network** Connections icon.
3. In the LAN or High-Speed Internet window, right-click on icon corresponding to your network interface card (NIC) and select **Properties**. (Often this icon is labeled Local Area Connection).

   The Local Area Connection dialog box displays with a list of currently installed network items.
4. Ensure that the check box to the left of the item labeled Internet Protocol TCP/IP is checked, and click <**Properties**> button.
5. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled **Obtain an IP address automatically**. Also click the radio button labeled **Obtain DNS server address automatically**.
6. Click <**OK**> button twice to confirm your changes, and close the Control Panel.

3.2.3 Windows® 2000 PC:

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the <**Start**> button, point to Settings, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. In the Network and Dial-up Connections window, right-click the **Local Area Connection** icon, and then select **Properties**.

   The Local Area Connection Properties dialog box displays a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip to step 10.
4. If Internet Protocol (TCP/IP) does not display as an installed component, click <**Install**> button.
5. In the Select Network Component Type dialog box, select Protocol, and then click <**Add**> button.

6. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click <**OK**> button.

   You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.

7. If prompted, click <**OK**> button to restart your computer with the new settings.

   Next, configure the PCs to accept IP addresses assigned by the iPBX30:

8. In the Control Panel, double-click the **Network and Dial-up Connections** icon.
9. In Network and Dial-up Connections window, right-click the **Local Area Connection** icon, and then select **Properties**.
10. In the Local Area Connection Properties dialog box, select **Internet Protocol (TCP/IP)**, and then click <**Properties**> button.
11. In the Internet Protocol (TCP/IP) Properties dialog box, click the radio button labeled **Obtain an IP address automatically**. Also click the radio button labeled **Obtain DNS server address automatically**.
12. Click <**OK**> button twice to confirm and save your changes, and then close the Control Panel.

3.2.4 Windows® 95, 98, and ME PC

1. In the Windows task bar, click the <**Start**> button, point to **Settings**, and then click **Control Panel**.
2. Double-click the Network icon.

   In the Network dialog box, look for an entry started with “**TCP/IP ->**” and the name of your network adapter, and then click <**Properties**> button. You may have to scroll down the list to find this entry. If the list includes such an entry, then the TCP/IP protocol has already been enabled. Skip to step 8.

3. If Internet Protocol (TCP/IP) does not display as an installed component, click <**Add**> button.

4. In the Select Network Component Type dialog box, select Protocol, and then click <**Add**> button.
5. Select Microsoft in the Manufacturers list box, and then click TCP/IP in the Network Protocols list, box and then click <**OK**> button.

   You may be prompted to install files from your Windows 95, 98 or Me installation CD or other media. Follow the instructions to install the files.
6. If prompted, click <OK> button to restart your computer with the new settings.

   Next, configure the PCs to accept IP information assigned by the iPBX30:
7. In the Control Panel, double-click the Network icon.
8. In the Network dialog box, select an entry started with "**TCP/IP ->**" and the name of your network adapter, and then click <**Properties**> button.
9. In the TCP/IP Properties dialog box, click the radio button labeled **Obtain an IP address automatically**.
10. In the TCP/IP Properties dialog box, click the "**Default Gateway**" tab. Enter **192.168.1.1** (the default LAN port IP address of the iPBX30) in the "**New gateway**" address field and click <**Add**> button to add the default gateway entry.
11. Click <**OK**> button twice to confirm and save your changes, and then close the Control Panel.
12. If prompted to restart your computer, click <**OK**> button to do so with the new settings.

3.2.5 Windows® NT 4.0 workstation:

First, check for the IP protocol and, if necessary, install it:

1. In the Windows NT task bar, click the <**Start**> button, point to **Settings**, and then click **Control Panel**.
2. In the Control Panel window, double click the **Network** icon.
3. In the Network dialog box, click the **Protocols** tab.

The Protocols tab displays a list of currently installed network protocols. If the list includes TCP/IP Protocol, then the protocol has already been enabled. Skip to step 9.

4. If TCP/IP does not display as an installed component, click <**Add**> button.
5. In the Select Network Protocol dialog box, select TCP/IP, and then click <**OK**> button.

   You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.

   After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.

6. Click <**Yes**> button to continue, and then click <**OK**> button if prompted to restart your computer.

   Next, configure the PCs to accept IP addresses assigned by the iPBX30:

7. Open the **Control Panel** window, and then double-click the **Network** icon.
8. In the Network dialog box, click the **Protocols** tab.
9. In the Protocols tab, select **TCP/IP**, and then click <**Properties**> button.
10. In the Microsoft TCP/IP Properties dialog box, click the radio button labeled **Obtain an IP address from a DHCP server**.
11. Click <**OK**> button twice to confirm and save your changes, and then close the Control Panel.

3.2.6 Assigning static IP addresses to your PC

In some cases, you may want to assign IP addresses to some or all of your PCs directly (often called "statically"), rather than allowing the iPBX30 to assign them. This option may be desirable (but not required) if:

- You have obtained one or more public IP addresses that you want to always associate with specific computers (for example, if you are using a computer as a public web server).

- You maintain different subnets on your LAN.

However, during the first time configuration of your iPBX30, you must assign an IP address in the 192.168.1.0 network for your PC, for example, 192.168.1.2, in order to establish connection between the iPBX30 and your PC as the default LAN IP on iPBX30 is pre-configured as 192.168.1.1. Enter 255.255.255.0 for the subnet mask and 192.168.1.1 for the default gateway. These settings may be changed later to reflect your true network environment.

On each PC to which you want to assign static information, follow the instructions on pages 15 through 18 relating only to checking for and/or installing the IP protocol. Once it is installed, continue to follow the instructions for displaying each of the Internet Protocol (TCP/IP) properties. Instead of enabling dynamic assignment of the IP addresses for the computer, DNS server, and default gateway, click the radio buttons that enable you to enter the information manually.

Note: Your PCs must have IP addresses that place them in the same subnet as the iPBX30*'s LAN port. If you manually assign IP information to all your LAN PCs, you can follow the instructions in Chapter 5 to change the LAN port IP address accordingly.*

3.3 Part 3 — Quick Configuration of the iPBX30

In this section, you log into the Web UI Management on the iPBX30 and configure the basic settings for your router. Your ISP should provide you with the necessary information to complete this step. Note the intent here is to quickly get the iPBX30 up and running, instructions are concise. You may refer to corresponding chapters for more details.

3.3.1 Setting Up the iPBX30

Follow these instructions to setup the iPBX30:

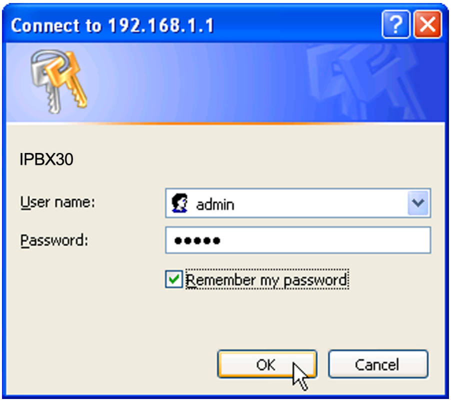
12. Before accessing the Web UI Management in iPBX30, make sure that the HTTP proxy setting is disabled in your browser. In IE, click “Tools” -> “Internet Options...” -> “Connections” tab -> “LAN settings...” and then uncheck “Use proxy server for your

LAN ...”

13. On any PC connected to one of the four LAN ports on the iPBX30, open your Web browser, and type the following URL in the address/location box, and press <Enter>:

http://192.168.1.1

This is the predefined IP address for the LAN port on the iPBX30.



IPBX30

User name: admin

Password: •••••

☑ Remember my password

Figure 3.2 Login Screen

If you encounter problems connecting to the iPBX30, check the following items:

a. Check if your PC is configured to accept IP address assignment from the iPBX30.

b. Set the IP address of your PC to any IP address in the 192.168.1.0 network, such as 192.168.1.2.

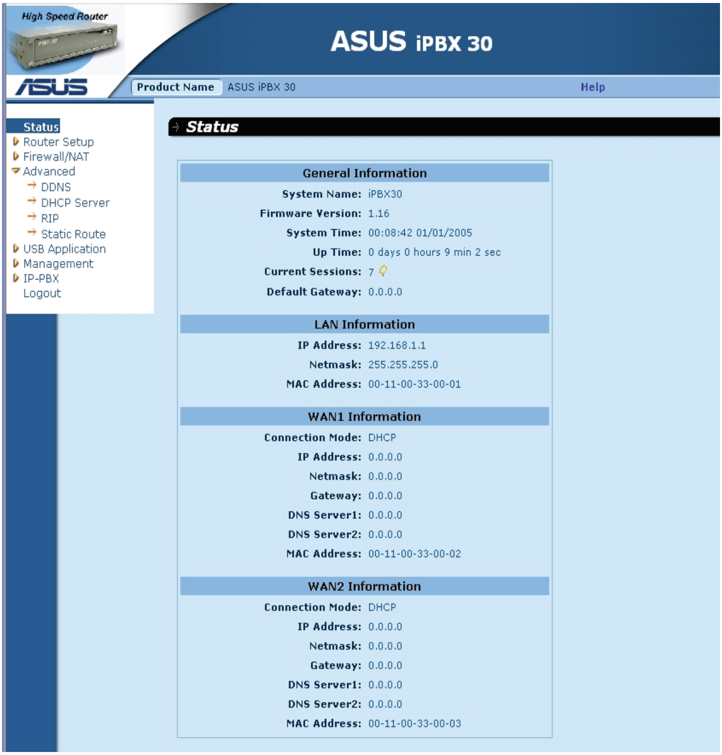
14. Enter your username and password, and then click "OK" to enter the Web UI Management. The first time you log into this program, use these defaults:

Default Username: admin

Default Password: admin

You can change the password at any time (see section 11.2).

The System Information page appears each time you log into the Web UI Management (shown in Figure 3.3).



Status

General Information

System Name: iPBX30
Firmware Version: 1.16
System Time: 00:08:42 01/01/2005
Up Time: 0 days 0 hours 9 min 2 sec
Current Sessions: 7
Default Gateway: 0.0.0.0

LAN Information

IP Address: 192.168.1.1
Netmask: 255.255.255.0
MAC Address: 00-11-00-33-00-01

WAN1 Information

Connection Mode: DHCP
IP Address: 0.0.0.0
Netmask: 0.0.0.0
Gateway: 0.0.0.0
DNS Server1: 0.0.0.0
DNS Server2: 0.0.0.0
MAC Address: 00-11-00-33-00-02

WAN2 Information

Connection Mode: DHCP
IP Address: 0.0.0.0
Netmask: 0.0.0.0
Gateway: 0.0.0.0
DNS Server1: 0.0.0.0
DNS Server2: 0.0.0.0
MAC Address: 00-11-00-33-00-03

Figure 3.3 System Status Page

15. Follow the instructions described in Chapter 5 “Router Setup” to set up the LAN and WAN settings for iPBX30.

After completing the basic configuration for iPBX30, read the following section to determine if you can access the Internet.

3.3.2 Testing Your Setup

At this point, the iPBX30 should enable any computers on your LAN to use the iPBX30’s ADSL or cable modem connection to access the Internet.

To test the Internet connection, open your web browser, and type the URL of any external website (such as *http://www.asus.com*). The LED labeled WAN should be blinking rapidly and may appear solid as the device connects to the site. You should also be able to browse the web site through your web browser.

If the LEDs do not illuminate as expected or the web page is not displayed, see Appendix 12 for troubleshooting suggestions.

3.3.3 Default Router Settings

In addition to handling the DSL connection to your ISP, the iPBX30 can provide a variety of services to your network. The device is pre-configured with default settings for use with a typical home or small office network.

The table below lists some of the most important default settings; these and other features are described fully in the subsequent chapters. If you are familiar with network configuration settings, review them to verify that they meet the needs of your network. Follow the instructions to make changes if necessary. If you are unfamiliar with these settings, try using the device without making any modification, or contact your ISP for assistance.

Before you modifying any settings, review Chapter 4 for general information about accessing and using the Web UI Management program. We strongly recommend that you contact your ISP prior to changing the default configuration.

Table 3.2 Default Settings Summary

Option	Default Setting	Explanation/Instruction
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with the following pool of addresses: 192.168.1.100 through 192.168.1.200	The iPBX30 maintains a pool of private IP addresses for dynamic assignment to your LAN computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in section 3.2. See section 6.1 for an explanation of the DHCP service.
LAN Port IP Address	Static IP address: 192.168.1.1 subnet mask: 255.255.255.0	This is the IP address of the LAN port on the iPBX30. The LAN port connects the device to your Ethernet network. Typically, you will not need to change this address. See section 5.1 for instructions.

4 Using the Web UI Management

The iPBX30 includes the **Web UI Management**, a preinstalled Web-based configuration software. It enables you to configure the device settings to meet the needs of your network. You can access it through your web browser from any PC connected to the iPBX30 via the LAN or the WAN ports.

This chapter describes the general guides in using the Web UI Management.

4.1 Log into the Web UI Management

To access the software, you need the following:

- A computer connected to the LAN or WAN port on the iPBX30 as described in the chapter 3.
- A web browser installed on the computer. The program is designed to work best with Microsoft Internet Explorer® 6.0 or later.

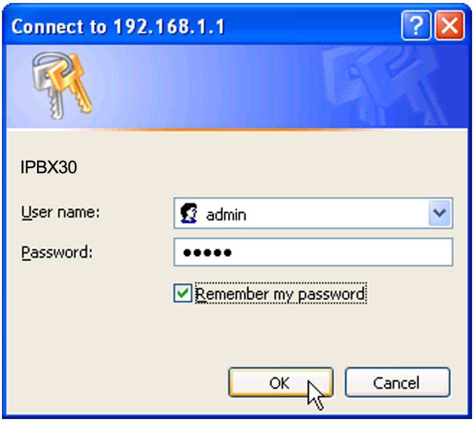
You may access the software from any computer connected to the iPBX30 via the LAN or WAN ports. However, the instructions provided here are for computers connected via the LAN ports.

1. From a LAN computer, open your web browser, type the following in the web address (or location) box, and press <**Enter**>:

http://192.168.1.1

This is the predefined IP address for the LAN port on the iPBX30.

A login screen is shown.



Connect to 192.168.1.1

IPBX30

User name: admin

Password: ●●●●●

☑ Remember my password

Figure 4.1 Login Screen

2. Enter your username and password, and then click **OK**.

The first time you log into the program, use these defaults:

Default Username: admin

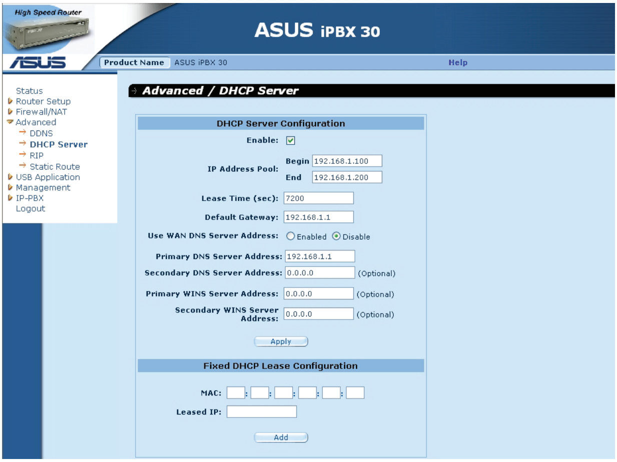
Default Password: admin

Note: You can change the password at any time (see section 11.2).

The System Information page appears every time you log into the software (shown in Figure 3.3).

4.2 Functional Layout

A typical page in the software consists of several elements – banner, menu, menu navigation tips, configuration, and on-line help. You can click on any menu item to expand/contract any menu groups or to access a specific configuration page. The configuration pane is where you interact with the software to configure the settings for iPBX30. Menu navigation tips show how the current configuration can be accessed via the menus.



Product Name ASUS iPBX 30

Advanced / DHCP Server

DHCP Server Configuration

Enable: ☑

IP Address Pool: Begin 192.168.1.100

End 192.168.1.200

Lease Time (sec): 7200

Default Gateway: 192.168.1.1

Use WAN DNS Server Address: ○ Enabled ● Disable

Primary DNS Server Address: 192.168.1.1

Secondary DNS Server Address: 0.0.0.0 (Optional)

Primary WINS Server Address: 0.0.0.0 (Optional)

Secondary WINS Server Address: 0.0.0.0 (Optional)

Fixed DHCP Lease Configuration

MAC: _ : _ : _ : _ : _ : _

Leased IP:

Figure 4.2 Typical Web UI Management Page

4.2.1 Menu Navigation

- To expand a group of related menus, double click the menu or the icon: ▶
- To contract a group of related menus, double click the menu or the icon: ▼
- To open a specific configuration page, double click the menu or the icon: →

4.2.2 Commonly Used Buttons and Icons

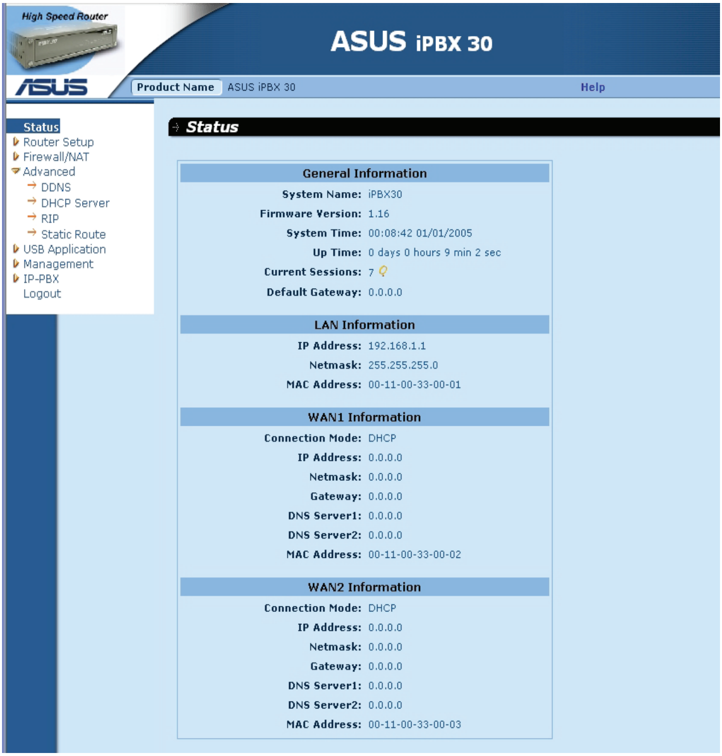
The following buttons or icons are used throughout the application. The following table describes the function for each button or icon.

Table 4.1 Description of Commonly Used Bottons and Icons

Button	Function
Apply	Stores any changes you have made on the current page.
Add	Adds the existing configuration to the system, e.g. a static route or a firewall ACL rule and etc.
Modify	Modifies the existing configuration in the system, e.g. a static route or a firewall ACL rule and etc.
Reload	Redisplays the current page with updated statistics or settings.
✎	Selects the item for editing.
🗑	Deletes the selected item.

4.3 System Configuration Overview

To view the overall system configuration, log into the iPBX30 Web, or click the Status menu if you have already logged on. The figure below shows sample information available in the System Status page.



Status

General Information

System Name: iPBX30
Firmware Version: 1.16
System Time: 00:08:42 01/01/2005
Up Time: 0 days 0 hours 9 min 2 sec
Current Sessions: 7
Default Gateway: 0.0.0.0

LAN Information

IP Address: 192.168.1.1
Netmask: 255.255.255.0
MAC Address: 00-11-00-33-00-01

WAN1 Information

Connection Mode: DHCP
IP Address: 0.0.0.0
Netmask: 0.0.0.0
Gateway: 0.0.0.0
DNS Server1: 0.0.0.0
DNS Server2: 0.0.0.0
MAC Address: 00-11-00-33-00-02

WAN2 Information

Connection Mode: DHCP
IP Address: 0.0.0.0
Netmask: 0.0.0.0
Gateway: 0.0.0.0
DNS Server1: 0.0.0.0
DNS Server2: 0.0.0.0
MAC Address: 00-11-00-33-00-03

Figure 4.3 System Status Page

5 Router Setup

This chapter describes how to configure the basic settings for your router so that the computers on your LAN can communicate with each other and have access to the Internet. The network setup consists of LAN and WAN configurations.

5.1 LAN Configuration

5.1.1 LAN IP Address

If you are using iPBX30 with multiple PCs on your LAN, you must connect your LAN to the Ethernet ports on the built-in Ethernet switch. You must assign a unique IP address to each device residing on your LAN. The LAN IP address that identifies the iPBX30 as a node on your network must be in the same subnet as the PCs on your LAN. The default LAN IP address for the iPBX30 is 192.168.1.1.

Definition: A network node can be thought of as any interface where a device connects to the network, such as the iPBX30*'s LAN port and the network interface cards on your PCs.*

You can change the default IP address to reflect the true IP address that you want to use with your network.

5.1.2 LAN Configuration Parameters

The table below describes the configuration parameters available for LAN IP configuration.

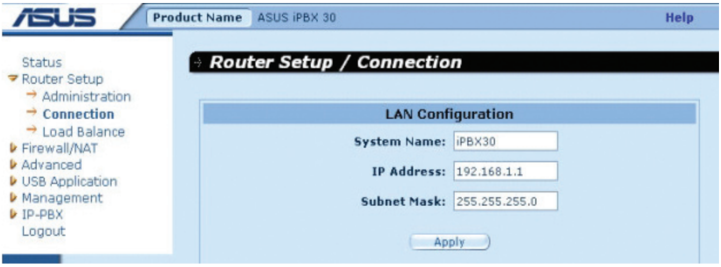
Table 5.1 LAN Configuration Parameters

Settings	Description
Host Name	For identification purpose only.
IP Address	The LAN IP address of the iPBX30. This IP address is used by your computers to identify the iPBX30's LAN port. Note that the public IP address assigned to you by your ISP is not your LAN IP address. The public IP address identifies the WAN port on the iPBX30 to the Internet.
Subnet Mask	The LAN subnet mask identifies which parts of the LAN IP Address refer to your network as a whole and which parts refer specifically to nodes on the network. Your device is preconfigured with a default subnet mask of 255.255.255.0.

5.1.3 Configuring the LAN IP Address

Follow these steps to change the default LAN IP address.

1. Click the **Router Setup -> Connection** menu to open the Connection configuration page.



LAN Configuration

System Name: iPBX30

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Figure 5.1 Network Setup Configuration- LAN Configuration

2. (Optional) Enter the host name for iPBX30. Note that the host name is used for identification purpose only.

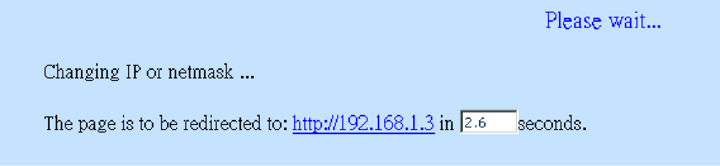
3. Enter the LAN IP address and subnet mask for the iPBX30 in the space provided.

4. Proceed to the WAN Configuration section for instructions on setting up the WAN port if you have not yet done so.

5. Click "**Apply**" to save the settings. If you were using an Ethernet

connection for the current session, and changed the IP address or subnet mask, the connection will be terminated.

6. You will see the following message displayed as shown below.



Please wait...

Changing IP or netmask ...

The page is to be redirected to: http://192.168.1.3 in 2.6 seconds.

7. You will be prompted to log back into the Web UI Management once the timer elapses.

5.2 WAN/DMZ Configuration

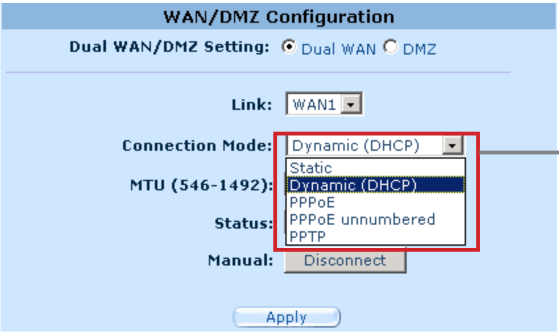
This section describes how to configure WAN/DMZ settings for the WAN interface on the iPBX30 that communicates with your ISP. You'll learn to configure the IP address, DHCP and DNS server for your WAN in this section.

DMZ (short for demilitarized zone) is a host or a small network that sits between a trustful internal network, such as a corporate private LAN, and an untrusted external network, such as the Internet. Typically, the DMZ contains devices accessible to the Internet traffic, such as Web servers, FTP servers, SMTP (e-mail) servers and DNS servers. The DMZ contains no corporate confidential information. In the event that the DMZ is compromised, no other company information will be exposed.

Note: Only static IP connection mode is supported for DMZ.

5.2.1 WAN Connection Mode

The iPBX30 supports five WAN connection modes – static IP, dynamic IP, PPPoE (multi-session), PPPoE unnumbered, and PPTP. You may select one of the WAN connection modes required by your ISP from the Connection Mode drop-down list in the Network Setup Configuration page.



WAN/DMZ Configuration

Dual WAN/DMZ Setting: ● Dual WAN ○ DMZ

Link: WAN1

Connection Mode: Dynamic (DHCP)

MTU (546-1492):

Status:

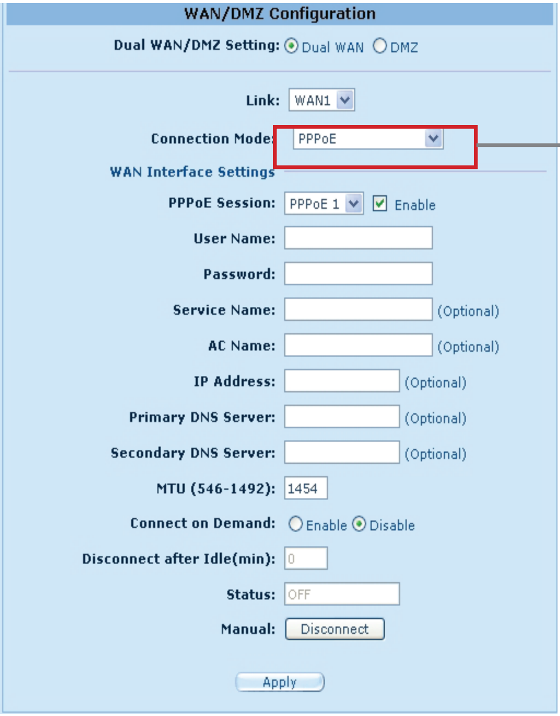
Manual:

Connection Mode drop-down list.

Figure 5.2 Network Setup Configuration Page-WAN Configuration

5.2.2 PPPoE

PPPoE connection is most often used by ADSL service providers.



WAN/DMZ Configuration

Dual WAN/DMZ Setting: ● Dual WAN ○ DMZ

Link: WAN1

Connection Mode: PPPoE

WAN Interface Settings

PPPoE Session: PPPoE 1 ☑ Enable

User Name:

Password:

Service Name: (Optional)

AC Name: (Optional)

IP Address: (Optional)

Primary DNS Server: (Optional)

Secondary DNS Server: (Optional)

MTU (546-1492): 1454

Connect on Demand: ○ Enable ● Disable

Disconnect after Idle(min): 0

Status: OFF

Connection Mode drop-down list.

Figure 5.3. WAN – PPPoE Configuration

5.2.2.1 WAN PPPoE Configuration Parameters

The table below describes the configuration parameters available for the PPPoE connection mode.

Table 5.2. WAN PPPoE Configuration Parameters

Setting	Description
Link	Select a port to configure. Available options are WAN1, WAN2 or DMZ.
Connection Mode	Select PPPoE from the connection mode drop-down list.
PPPoE Session	Select the PPPoE session ID for this PPPoE session. Note that only two simultaneous PPPoE sessions are supported.
Enable	Check or uncheck this box to activate or de-activate this PPPoE session.
User Name and Password	Enter the username and password you use to log into your ISP. (Note: this is different from the information you used to log into the software application.)
Service Name	Enter the service name provided by your ISP. Service name is optional but may be required by some ISPs.
AC Name	Enter the access concentrator name provided by your ISP. Access concentrator name is optional but may be required by some ISPs.
IP Address	If your ISP allows you to always obtain the same IP address for your WAN, enter it here.
Primary / Secondary DNS Server	IP address of the primary and/or secondary DNS are optional as PPPoE will automatically detect the DNS IP addresses configured at your ISP. However, if there are other DNS servers you would rather use, enter the IP addresses here.
MTU	You may specify the maximum size of the transmitted packet. For PPPoE, the range of MTU is from 546 to 1492. The default value is 1454.
Disconnect after idle (min.)	Enter the inactivity timeout period at which you want to disconnect the Internet connection when there is no traffic. A value of 0 means no activity time out. Note that SNTP service may interfere with this function if there are activities from the service.

Setting	Description
Connect on Demand	Click on the Enable or Disable radio button to enable or disable this option.
Status	On: PPPoE connection is active. Off: No PPPoE connection is active. Connecting: iPBX30 is trying to connect to your ISP using PPPoE connection mode.
Manual Disconnect/ Connect	Click the Disconnect or Connect button to disconnect or connect using the PPPoE connection mode.

5.2.2.2 Configuring PPPoE for WAN

Follow the instructions below to configure PPPoE settings:

1. Click the **Router Setup -> Connection** menu to open the Network Setup configuration page.
2. Select which WAN port (WAN1/WAN2) to configure for PPPoE connection mode.
3. Select **PPPoE** from the WAN Connection Mode drop-down list.
4. Select **PPPoE session ID** from the PPPoE session ID drop-down list. Currently, two sessions are supported for each WAN port.
5. Enter the service name if required by your ISP.
6. (Optional) Enter the service name or AC name, or both, if required by your ISP.
7. (Optional) If your ISP allows you to always obtain the same IP address for your WAN, enter it in the IP Address field; otherwise, skip this step.
8. (Optional) Enter the IP addresses for the primary and/or secondary DNS servers if you want to use your preferred DNS servers; otherwise, skip this step.
9. (Optional) Change the MTU value if necessary. If you do not know what value to enter, leave it as is. For dynamic IP

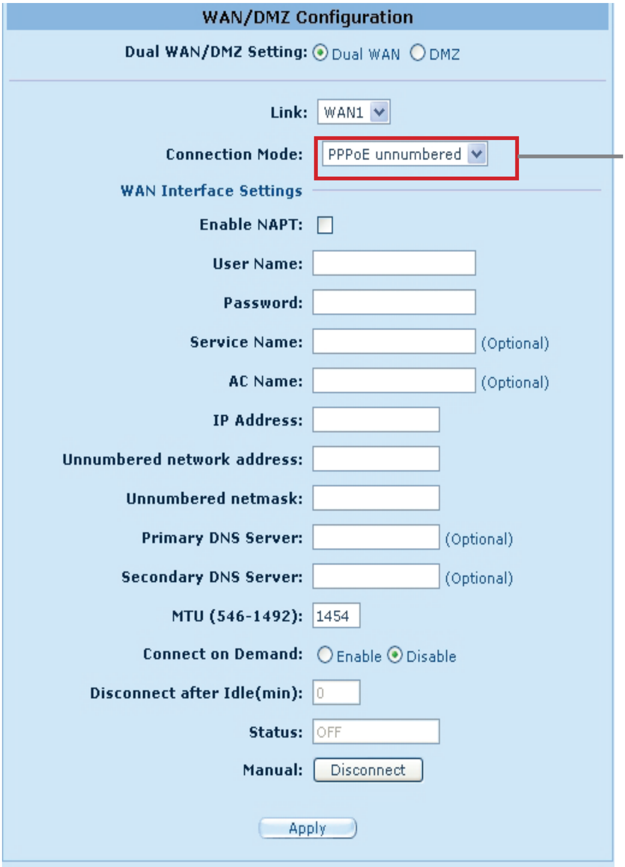
connection mode, the range of MTU is from 546 to 1492. The default value is 1454.

10.Enter the appropriate connection settings for “**Disconnect after Idle (min)**” and “**Connect on Demand**”.

11.Click "**Apply**" to save the settings.

5.2.3 PPPoE Unnumbered

Some of the ADSL service providers may offer PPPoE unnumbered service. Choose this connection mode if your ISP provides such service.



WAN/DMZ Configuration

Dual WAN/DMZ Setting: ● Dual WAN ○ DMZ

Link: WAN1

Connection Mode: PPPoE unnumbered

WAN Interface Settings

Enable NAPT: ☐

User Name:

Password:

Service Name: (Optional)

AC Name: (Optional)

IP Address:

Unnumbered network address:

Unnumbered netmask:

Primary DNS Server: (Optional)

Secondary DNS Server: (Optional)

MTU (546-1492): 1454

Connect on Demand: ○ Enable ● Disable

Disconnect after Idle(min): 0

Status: OFF

Manual:

Connection Mode drop-down list.

Figure 5.4. WAN – PPPoE Unnumbered Configuration

5.2.3.1 WAN PPPoE Unnumbered Configuration Parameters

The table below describes the configuration parameters available for PPPoE Unnumbered connection mode.

Table 5.3. WAN PPPoE Unnumbered Configuration Parameters

Setting	Description
Link	Select a port to configure. Available options are WAN1, WAN2 or DMZ.
Connection Mode	Select PPPoE Unnumbered from the connection mode drop-down list. Traditionally, each network interface must have a unique IP address. However, an unnumbered interface does not have to have a unique IP address. This means that when this option is selected, the WAN and the LAN use the same IP address. Network resources are therefore conserved because fewer network IP addresses are used and routing table is smaller.
Enable NAPT	Check or uncheck this box to enable NAPT for this connection.
User Name and Password	Enter the username and password you use to log into your ISP. (Note: this is different from the information you used to log into Web UI Management.)
Service Name	Enter the service name provided by your ISP. Service name is optional but may be required by some ISPs.
AC Name	Enter the access concentrator name provided by your ISP. Access concentrator name is optional but may be required by some ISPs.
IP Address	Enter a static IP address here for the PPPoE unnumbered connection. This IP address must be provided by your service provider.
Unnumbered Network Address	Enter the network address provided by your ISP.
Primary / Secondary DNS Server	IP address of the primary or secondary DNS are optional as PPPoE will automatically detect the DNS IP addresses configured at your ISP. However, if there are other DNS servers you would rather use, enter the IP addresses here.

Setting	Description
MTU	You may specify the maximum size of the transmitted packet. For PPPoE, the range of MTU is from 546 to 1492. The default value is 1454.
Disconnect after Idle (min.)	Enter the inactivity timeout period at which you want to disconnect the Internet connection when there is no traffic. A value of 0 means no activity time out. Note that SNTP service may interfere with this function if there are activities from the service.
Connect on Demand	Click on the Enable or Disable radio button to enable or disable this option.
Status	On: PPPoE unnumbered connection is active. Off: No PPPoE unnumbered connection is active. Connecting: iPBX30 is trying to connect to your ISP using PPPoE unnumbered connection mode.
Manual Disconnect/ Connect	Click the Disconnect or Connect button to disconnect or connect using the PPPoE unnumbered connection mode.

5.2.3.2 Configuring PPPoE Unnumbered for WAN

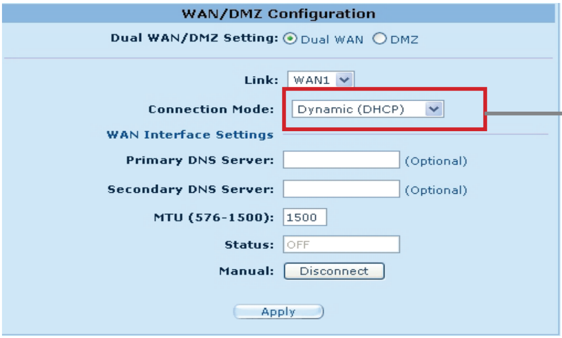
Follow the instructions below to configure PPPoE unnumbered settings:

1. Click the **Router Setup -> Connection** menu to open the Network Setup configuration page.
2. Select which WAN port (WAN1/WAN2) to configure for PPPoE unnumbered connection mode.
3. Select **PPPoE Unnumbered** from the WAN Connection Mode drop-down list.
4. Check **NAPT** box if NAT is to be used for this connection.
5. Enter user name and password provided by your ISP
6. (Optional) Enter the service name and/or AC name if required by your ISP.
7. Enter the IP address, unnumbered network address, and unnumbered netmask provided by your ISP.

8. (Optional) Enter the IP addresses for the primary or secondary DNS servers, or both, if you want to use your preferred DNS servers; otherwise, skip this step.
9. (Optional) Change the MTU value if necessary. If you do not know what value to enter, leave it as is. For dynamic IP connection mode, the range of MTU is from 546 to 1492. The default value is 1454.
10. Enter appropriate connection settings for **Disconnect after Idle (min)** and **Connect on Demand**.
11. Click **Apply** to save the settings.

5.2.4 Dynamic IP

Dynamic IP is most often used by the cable modem service providers.



WAN/DMZ Configuration

Dual WAN/DMZ Setting: ● Dual WAN ○ DMZ

Link: WAN1

Connection Mode: Dynamic (DHCP)

WAN Interface Settings

Primary DNS Server: (Optional)

Secondary DNS Server: (Optional)

MTU (576-1500): 1500

Status: OFF

Manual: Disconnect

Connection Mode drop-down list.

Figure 5.5. WAN – Dynamic IP (DHCP client) Configuration

5.2.4.1 Configuring Dynamic IP for WAN

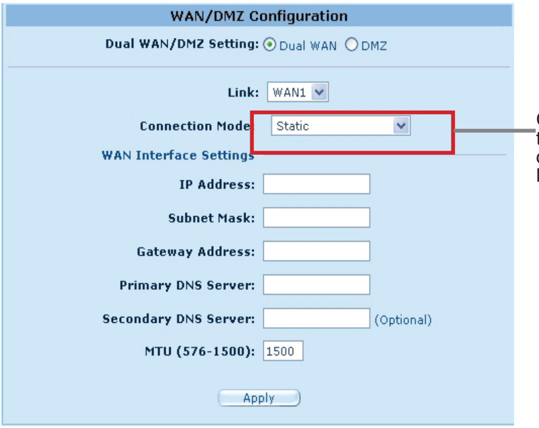
Follow the instructions below to configure dynamic IP settings:

1. Open the **Network Setup** configuration page by clicking the **Router Setup -> Connection** menu.
2. Select which WAN port (WAN1/WAN2) to configure for dynamic connection mode.
3. Select **Dynamic** from the Connection Mode drop-down list. Note that the IP addresses for the primary and/or the secondary DNS servers are automatically assigned by the DHCP server of your

ISP.

4. (Optional) Change the MTU value if necessary. If you do not know what value to enter, leave it as is. For dynamic IP connection mode, the range of MTU is from 576 to 1500. The default value is 1500.
5. Click **Apply** to save the settings.

5.2.5 Static IP



WAN/DMZ Configuration

Dual WAN/DMZ Setting: ● Dual WAN ○ DMZ

Link: WAN1

Connection Mode: Static

WAN Interface Settings

IP Address:

Subnet Mask:

Gateway Address:

Primary DNS Server:

Secondary DNS Server: (Optional)

MTU (576-1500): 1500

Connection Mode drop-down list.

Figure 5.6. WAN – Static IP Configuration

5.2.5.1 WAN or DMZ Static IP Configuration Parameters

The table below describes the configuration parameters available for static IP connection mode.

Table 5.4. WAN Static IP Configuration Parameters

Setting	Description
Link	Select a port to configure. Available options are WAN1/ WAN2 or WAN/DMZ.
Connection Mode	Select Static from the connection mode drop-down list.
IP Address	WAN/DMZ IP address. Please note that WAN IP address is a public IP address provided by your ISP while DMZ IP address is a private IP address.

Setting	Description
Subnet Mask	WAN/DMZ subnet mask. Typically, it is set as 255.255.255.0.
Gateway Address	Gateway IP address provided by your ISP. It must be in the same subnet as the WAN on the iPBX30.
Primary/ Secondary DNS Server	You must at least enter the IP address of the primary DNS server. Secondary DNS server is optional
MTU	You may specify the maximum size of the transmitted packet. For static IP connection, the range of MTU is from 576 to 1500. The default value is 1500.

5.2.5.2 Configuring Static IP for WAN or DMZ

Follow the instructions below to configure static IP settings:

1. Click the **Router Setup -> Connection** menu to open the **Network Setup** configuration page.
2. Select which WAN port (WAN1/WAN2) or DMZ port to configure for the static connection mode.
3. Select **Static** from the Connection Mode drop-down list.
4. Enter WAN IP address in the IP Address field. This information should be provided by your ISP.
5. Enter Subnet Mask for the WAN. This information should be provided by your ISP. Typically, it is 255.255.255.0.
6. Enter gateway address provided by your ISP in the space provided.
7. Enter the IP address of the primary DNS server. This information should be provided by your ISP. Secondary and third DNS servers are optional.
8. (Optional) Change the MTU value if necessary. If you do not know what value to enter, leave it as it is. For static IP connection mode, the range of MTU is from 576 to 1500. The default value is 1500.
9. Click **Apply** to save the settings

5.2.6 PPTP

Some service providers require user to login using PPTP connection.

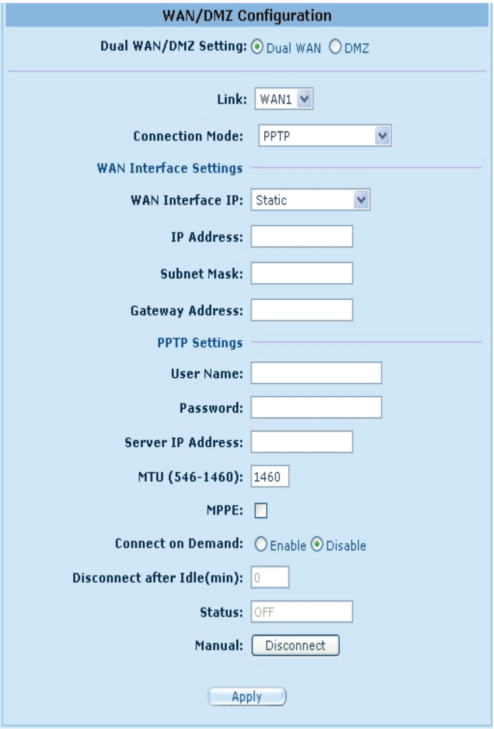
5.2.6.1 WAN PPTP Configuration Parameters

The table below describes the configuration parameters available for PPTP connection mode.

Table 5.5. WAN PPTP Configuration Parameters

Setting	Description
Link	Select a port to configure. Available options are WAN1, WAN2 or DMZ.
Connection Mode	Select PPTP from the connection mode drop-down list.
WAN Interface IP	Select how WAN IP address is to be configured – static (manually set the IP address) or dynamic (obtained automatically from the DHCP server).
Static	Choose this connection mode if the WAN IP is a fixed IP provided by your ISP.
IP Address	Enter the WAN IP address provided by your ISP.
Subnet Mask	Enter the subnet mask for the WAN IP provided by your ISP.
Gateway Address	Enter the gateway IP address for the WAN provided by your ISP.
Dynamic (DHCP)	Select this connection mode if your WAN IP address is obtained automatically from your ISP's DHCP server.
User Name and Password	Enter the username and password you use to log into your ISP. (Note: this is different from the information you used to log into the software application.)
Server IP Address	Enter the PPTP server IP address provided by your ISP.
MTU	You may specify the maximum size of the transmitted packet. For PPTP, the range of MTU is from 546 to 1460. The default value is 1460.
Connect on Demand	Click on the Enable or Disable radio button to enable or disable this option.

Setting	**Description**
Disconnect after Idle (min)	Enter the inactivity timeout period at which you want to disconnect the Internet connection when there is no traffic. A value of 0 means no activity time out. The SNTP service may interfere with this function if there are activities from the service.
Status	On: PPTP connection is active. Off: No PPTP connection is active. Connecting: iPBX30 is trying to connect to your ISP using PPTP connection mode.
Manual Disconnect/ Connect	Click the Disconnect or Connect button to disconnect or connect using the PPTP connection mode.



WAN/DMZ Configuration

Dual WAN/DMZ Setting: ● Dual WAN ○ DMZ

Link: WAN1

Connection Mode: PPTP

WAN Interface Settings

WAN Interface IP: Static

IP Address:

Subnet Mask:

Gateway Address:

PPTP Settings

User Name:

Password:

Server IP Address:

MTU (546-1460): 1460

MPPE: ☐

Connect on Demand: ○ Enable ● Disable

Disconnect after Idle(min): 0

Status: OFF

Manual: Disconnect

Apply

Figure 5.7. WAN – PPTP Configuration

5.2.6.2 Configuring PPTP for WAN

Follow the instructions below to configure the PPTP settings:

1. Click the **Router Setup ->Connection** menu to open the Network Setup configuration page.
2. Select which WAN port (WAN1/WAN2) to configure for PPTP connection mode.
3. Select **PPTP** from the **WAN Connection Mode** drop-down list.
4. Select how WAN IP is to be obtained – static or dynamic. If your ISP provides a fixed IP address, select **Static** in the WAN Interface IP drop-down list. Consult with your ISP if you have no idea.
5. Enter IP address, subnet mask and gateway IP address for your WAN if your WAN IP is to be set manually.
6. Enter user name and password provided by your ISP.
7. Enter PPTP server IP address provided by your ISP.
8. (Optional) Change the MTU value if necessary. If you do not know what value to enter, leave it as is. For PPTP connection mode, the range of MTU is from 546 to 1460. The default value is 1460.
9. Check MPPE box if the packet is to be encrypted with this protocol.
10. Enter the appropriate connection settings for **Disconnect after Idle (min)** and **Connect on Demand**.
11. Click **Apply** to save the settings.

5.3 WAN Load Balancing and Line Back Up

iPBX30 supports load balancing and line back up on the WAN connection. This function is available only when “**Dual-WAN**” is selected in the Router Connection configuration page (accessible by clicking the **Router Setup ->Connection** menu).

WAN load balancing distributes communication activities across the two WANs on iPBX30 based on the preconfigured bandwidth requirement on the WANs. Another feature supported is fail-over for the WAN ports. If one of the WAN links is down, iPBX30 will direct the traffic destined for the downed WAN port to the still active WAN port.

The line back up function is another feature supported to ensure uninterrupted Internet access. When the primary WAN link is down, the Internet access is automatically switched to the backup WAN link.

5.3.1 WAN Load Balancing and Line Back Up Configuration Parameters

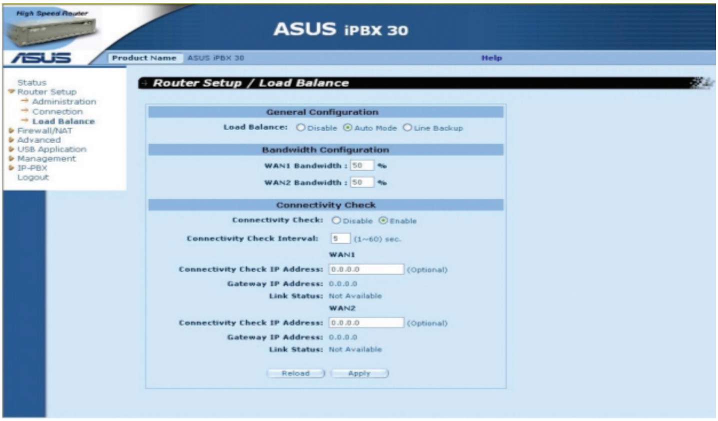
The table below describes the configuration parameters available for WAN load balancing and line back up.

Table 5.6. WAN Load Balancing and Line Back Up Configuration Parameters

Setting	Description
Load Balance	Select one of the three available options: Disable: disable both the WAN load balancing and line back up functionalities. Auto Mode: select this option if load balancing is desired. The algorithm used for the load balancing is weighted round robin. This option includes the functionality off line backup. It is recommended that this option be selected. Line Backup: select this option if line backup is needed. In the existing implementation, the primary link is always set to WAN1 and the backup link is always set to WAN2.
WAN1/WAN2 Bandwidth	Enter the ratio of the traffic amount that you want to distribute between the WANs. The number should be between 0 to 100%. For example, 80% for WAN1 and 20% for WAN2 means 80% of the traffic is directed to WAN1 and 20% of the traffic is directed to WAN2.
Connectivity Check	Click Enable or Disable radio button to enable or disable this feature. Connectivity check is used to monitor the link status for the WAN ports. If this option is disabled, iPBX30 will not perform fail-over; this means that if one of the WAN links is down, the traffic directed to the downed link will not be re-directed to the active link. It is recommended that you keep this option enabled. However, if the gateway or the specific network device that will be checked for connectivity does not respond to ping, you

Setting	Description
Connectivity Check (Cont.)	will need to disable this feature. Otherwise, iPBX30 will make incorrect judgment regarding the WAN link status and thus affect the behavior of the load balancing or line back up.
Connectivity Check Interval	The interval that iPBX30 will check for the WAN link status. The allowable value is 1 to 60 seconds.
Connectivity Check IP Address (WAN1)	Enter the IP address of the specific network device that the traffic will pass through. This field is optional. Normally, you don't need to provide any IP address here, unless you know the traffic must pass a specific network device.
Connectivity Check IP Address (WAN2)	Enter the IP address of the specific network device that the traffic will pass through. This field is optional. Normally, you don't need to provide any IP address here, unless you know the traffic must pass a specific network device.

5.3.2 Setting Up WAN Load Balancing and Line Back Up



Router Setup / Load Balance

General Configuration

Load Balance: ○ Disable ● Auto Mode ○ Line Backup

Bandwidth Configuration

WAN1 Bandwidth : 50 %

WAN2 Bandwidth : 50 %

Connectivity Check

Connectivity Check: ○ Disable ● Enable

Connectivity Check Interval: 5 (1~60) sec.

WAN1

Connectivity Check IP Address: 0.0.0.0 (Optional)

Gateway IP Address: 0.0.0.0

Link Status: Not Available

WAN2

Connectivity Check IP Address: 0.0.0.0 (Optional)

Gateway IP Address: 0.0.0.0

Link Status: Not Available

Figure 5.8. Load Balancing Configuration

Follow the instructions below to set up WAN load balancing:

1. Click the **Router Setup ->Load Balance** menu to open the Load Balancing configuration page.
2. Select **Auto Mode** in the Load Balance field.
3. Enter the ratio of the traffic amount that you want to distribute between the two WANs. The allowable value is from 0 to 100%. The sum of the two numbers is 100%.
4. Select whether you need to enable or disable connectivity check. If this option is enabled, please also enter the following:

a) Enter the connectivity check interval.

b) (Optional) Enter the connectivity check IP address for WAN1 and/or WAN2.

5. Click **Apply** to save the settings.

5.3.3 Setting Up WAN Line Back Up

Follow the instructions below to set up line backup:

1. Click the **Router Setup ->Load Balance** menu to open the Load Balancing configuration page.
2. Select “**Line Backup**” in the Load Balance field.
3. Select whether you need to enable or disable connectivity check. If this option is enabled, please also enter the following:
   a) Enter the connectivity check interval.
   b) (Optional) Enter the connectivity check IP address for WAN1 and/or WAN2.
4. Click **Apply** to save the settings.

6 DHCP Server Configuration

6.1 Dynamic Host Control Protocol (DHCP)

6.1.1 What is DHCP?

DHCP is a protocol that enables network administrators to centrally manage the assignment and distribution of IP information to computers on a network.

When you enable DHCP on a network, you allow a device — such as the iPBX30 — to assign temporary IP addresses to your computers whenever they connect to your network. The assigning device is called a DHCP server, and the receiving device is a DHCP client.

Note: If you followed the instructions in chapter 3, you either configured each LAN PC with an IP address, or you specified that it will receive IP information dynamically (automatically). If you chose to have the information assigned dynamically, then you configured your PCs as DHCP clients that will accept IP addresses assigned from a DCHP server such as the iPBX30*.*

The DHCP server draws from a defined pool of IP addresses and “leases” them for a specified amount of time to your computers when they request an Internet session. It monitors, collects, and redistributes the addresses as needed.

On a DHCP-enabled network, the IP information is assigned dynamically rather than statically. A DHCP client can be assigned a different address from the pool each time it reconnects to the network.

6.1.2 Why use DHCP?

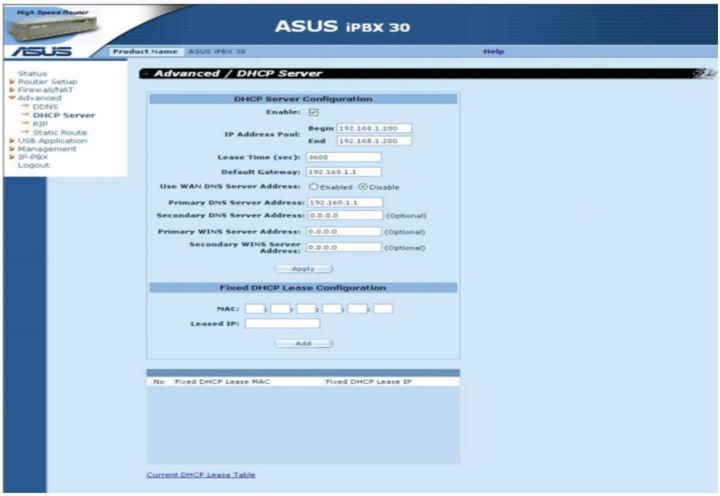
DHCP allows you to manage and distribute IP addresses throughout your network from the iPBX30. Without DHCP, you would have to configure each computer separately with IP address and related information. DHCP is commonly used with large networks and those that are frequently expanded or otherwise updated.

6.1.3 Configuring DHCP Server

Note: By default, the iPBX30 is configured as a DHCP server on the LAN side, with a predefined IP address pool of 192.168.1.100 through 192.168.1.149 (subnet mask 255.255.255.0). To change this range of addresses, follow the procedures described in this section.

First, you must configure your PCs to accept DHCP information assigned by a DHCP server:

1. Click **Advanced -> DHCP Server** menu to open the DHCP Server Configuration page.



Enable: ☑
IP Address Pool: Begin 192.168.1.100
End 192.168.1.200
Lease Time (sec): 3600
Default Gateway: 192.168.1.1
Use WAN DNS Server Address: ○ Enabled ● Disable
Primary DNS Server Address: 192.168.1.1
Secondary DNS Server Address: 0.0.0.0 (Optional)
Primary WINS Server Address: 0.0.0.0 (Optional)
Secondary WINS Server Address: 0.0.0.0 (Optional)

MAC: __ : __ : __ : __ : __ : __
Leased IP:

No	Fixed DHCP Lease MAC	Fixed DHCP Lease IP

Figure 6.1. DHCP Server Configuration Page

2. Enter the information for the IP Address Pool (Begin/End Address), Subnet Mask, Lease Time and Default Gateway IP Address, fields; others, such as Primary/Secondary DNS Server IP Address and Primary/Secondary WINS Server IP Address are optional. However, it is recommended that you enter the primary DNS server IP address in the space provided. You may enter the LAN IP or your ISP's DNS IP in the primary DNS Server IP Address field. The table below describes the DHCP configuration parameters in detail.

Table 6.1. DHCP Configuration Parameters

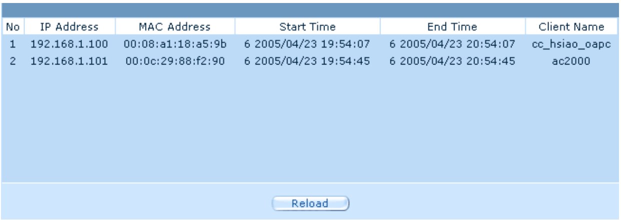
Field	Description
Enable	Check or uncheck this box to enable or disable the DHCP server service for your LAN.
IP Address Pool Begin/End	Specify the lowest and highest addresses in the DHCP address pool.
Lease Time	The amount of time in seconds the assigned address will be used by a device connected on the LAN.
Default Gateway IP Address	The address of the default gateway for computers that receive IP addresses from this pool. The default gateway is the device that the DHCP client computers first contacted to communicate with the Internet. Typically, it is the iPBX30's LAN port IP address.
Primary/ Secondary DNS Server IP Address	The IP address of the Domain Name System server to be used by computers that receive IP addresses from this pool. The DNS server translates common Internet names that you type into your web browser into their equivalent numeric IP addresses. Typically, the server(s) are located with your ISP. However, you may enter LAN IP address of the iPBX30 as it will serve as DNS proxy for the LAN computers and forward the DNS request from the LAN to DNS servers and relay the results back to the LAN computers. Note that both the primary and secondary DNS servers are optional.
Primary/ Secondary WINS Server IP Address (optional)	The IP address of the WINS servers to be used by computers that receive IP addresses from the DHCP IP address pool. You don't need to enter this information unless your network has WINS servers.

3. Click **Apply** to save the DHCP server configurations.

6.1.4 Viewing Current DHCP Address Assignments

When the iPBX30 functions as a DHCP server for your LAN, it keeps a record of any addresses it has leased to your computers. To view a table of all current IP address assignments, just open the DHCP Server Configuration page and click on the link “Current DHCP Lease Table” located at the bottom of the configuration page.

The DHCP lease table lists any IP addresses leased and the corresponding MAC addresses.



No	IP Address	MAC Address	Start Time	End Time	Client Name
1	192.168.1.100	00:08:a1:18:a5:9b	6 2005/04/23 19:54:07	6 2005/04/23 20:54:07	cc_hsiao_oapc
2	192.168.1.101	00:0c:29:88:f2:90	6 2005/04/23 19:54:45	6 2005/04/23 20:54:45	ac2000

Figure 6.2. DHCP Lease Table

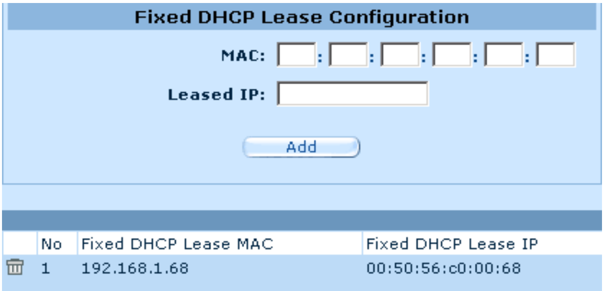
6.1.5 Fixed DHCP Lease

Fixed DHCP lease is used in situations when a fixed DHCP address is desired for a host that gets IP from the DHCP server. First, you should configure your PCs to accept DHCP information assigned by a DHCP server:

6.1.5.1 Access Fixed DHCP Configuration Page – (Advanced ->DHCP Server)

Click **Advanced ->DHCP Server** menu to open the Fixed DHCP Lease configuration page.

When you open the Fixed DHCP Lease configuration page, a list of existing lease is also displayed at the bottom half of the configuration page.



	No	Fixed DHCP Lease MAC	Fixed DHCP Lease IP
🗑	1	192.168.1.68	00:50:56:c0:00:68

Figure 6.3. Fixed DHCP Lease Configuration Page

6.1.5.2 Add a Fixed DHCP Lease

To add a fixed DHCP lease, follow the instructions below:

1. Click **Advanced ->DHCP Server** menu to open the Fixed DHCP Lease configuration page.
2. Enter the MAC address and the desired IP address of the host requiring a fixed IP address. The table below describes the fixed DHCP lease configuration parameters in detail.

Table 6.2. Fixed DHCP Lease Configuration Parameters

Field	**Description**
Fixed DHCP Lease MAC	A hardware ID of the device that needs a fixed IP address from the DHCP server.
Fixed DHCP Lease IP	The IP address leased from the DHCP server. It is recommended that this IP address be outside of the DHCP IP pool.

3. Click on the **Add** button to add the new fixed DHCP lease entry.

6.1.5.3 Delete a Fixed DHCP Lease

To delete a fixed DHCP lease, click on the 🗑 in front of the specific fixed DHCP lease to be deleted.

6.1.5.4 Viewing Fixed DHCP Lease Table

To see existing inbound fixed DHCP lease, just open the Fixed DHCP Lease configuration page by clicking **Advanced ->DHCP Server** menu.

6.2 DNS

6.2.1 About DNS

Domain Name System (DNS) servers map the user-friendly domain names that users type into their Web browsers (e.g., “yahoo.com”) to the equivalent numerical IP addresses that are used for Internet routing.

When a PC user types a domain name into a browser, the PC must first send a request to a DNS server to obtain the equivalent IP address. The DNS server will attempt to look up the domain name in its own database, and will communicate with higher-level DNS servers when the name cannot be found locally. When the address is found, it is sent back to the requesting PC and is referenced in IP packets for the remainder of the communication.

6.2.2 Assigning DNS Addresses

Multiple DNS addresses are useful to provide alternatives when one of the servers is down or is encountering heavy traffic. ISPs typically provide primary and secondary DNS addresses, and may provide additional addresses. Your LAN PCs learn these DNS addresses in one of the following ways:

- Statically: If your ISP provides you with their DNS server addresses, you can assign them to each PC by modifying the PCs’ IP properties.
- Dynamically from a DHCP Server: You can configure the DNS addresses in the DHCP server in the iPBX30 and allow the DHCP server to distribute the DNS addresses to the PCs. Refer to the section 6.1.3 “Configuring DHCP Server” for instructions on configuring DHCP server.

In either case, you can specify the actual addresses of the ISP’s DNS servers (on the PC or in the DHCP Server configuration page), or you can specify the address of the LAN port on the iPBX30 (e.g., 192.168.1.1). When you specify the LAN port IP address, the device performs DNS relay, as described in the following section.

Note: If you specify the actual DNS addresses on the PCs or in the DHCP pool, the DNS relay feature is not used.

6.2.3 Configuring DNS Relay

When you specify the device’s LAN port IP address as the DNS address, then the Internet Security Router automatically performs “DNS relay”; i.e., because the device itself is not a DNS server, it forwards domain name lookup requests from the LAN PCs to a DNS server at the ISP. It then relays the DNS server’s response to the PC.

When performing DNS relay, the iPBX30 must maintain the IP addresses of the DNS servers it contacts. It can learn these addresses in either or both of the following ways:

- Learned through PPPoE or Dynamic IP Connection: If the iPBX30 uses a PPPoE (see section 5.2.2 PPPoE or 5.2.3 PPPoE or Dynamic IP (see section 5.2.4 Dynamic IP) connection to the ISP, the primary and secondary DNS addresses can be learned via the PPPoE protocol. Using this option provides the advantage that you will not need to reconfigure the PCs or the iPBX30 if the ISP changes their DNS addresses.
- Configured on the iPBX30: You can also specify the ISP’s DNS addresses in the WAN configuration page.

Follow these steps to configure DNS relay:

1. Enter LAN IP in the DNS Server IP Address field in DHCP configuration page.
2. Configure the LAN PCs to use the IP addresses assigned by the DHCP server on the Internet Security Router, or enter the Internet Security Router’s LAN IP address as their DNS server address manually for each PC on your LAN.

Note: DNS addresses that are assigned to LAN PCs prior to enabling DNS relay will remain in effect until the PC is rebooted. DNS relay will only take effect when a PC’s DNS address is the LAN IP address.

Similarly, if after enabling DNS relay, you specify a DNS address (other than the LAN IP address) in a DHCP pool or statically on a PC, then that address will be used instead of the DNS relay address.

7 Routing

You can use the software application specific routes for your Internet and network data communication.

This chapter describes basic routing concepts and provides instructions for creating static routes. Note that most users do not need to define static routes.

7.1 Overview of IP Routes

The essential challenge of a router is: when it receives data intended for a particular destination, which next device should it send that data to? When you define IP routes, you provide the rules that the iPBX30 uses to make these decisions.

7.1.1 Do I need to define static routes?

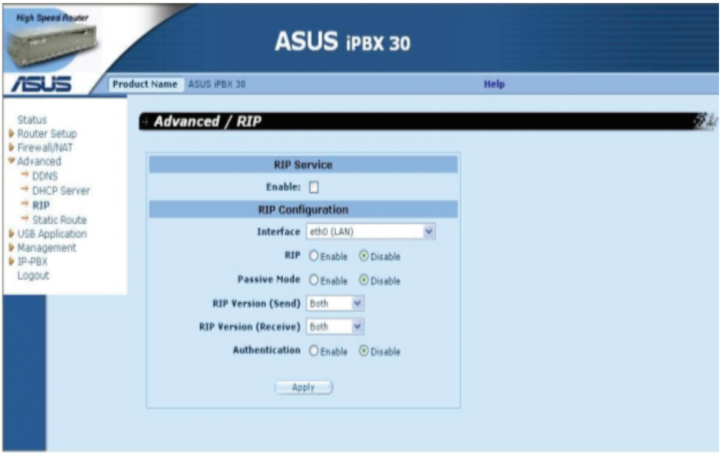
Most users do not need to define static routes. On a typical small home or office network, the existing routes that set up the default gateways for your LAN computers and for the iPBX30 provide the most appropriate path for all your Internet traffic.

- On your LAN computers, a default gateway directs all Internet traffic to the LAN port on the iPBX30. Your LAN computers know their default gateway either because you assigned it to them when you modified their TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet. (Each of these processes is described in section 3.2.)
- On the iPBX30 itself, a default gateway is defined to direct all outbound Internet traffic to a router at your ISP. This default gateway is assigned automatically by your ISP whenever the device negotiates an Internet connection. (The process for adding a default route is described in section 7.3.2.)

You may need to define static routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.

7.2 Dynamic Routing using RIP (Routing Information Protocol)

RIP enables routing information exchange between routers; thus, routes are updated automatically without human intervention. It is recommended that you enable RIP in the System Services Configuration Page.



Enable: ☐

Interface: eth0 (LAN)

RIP: ○ Enable ● Disable

Passive Mode: ○ Enable ● Disable

RIP Version (Send): Both

RIP Version (Receive): Both

Authentication: ○ Enable ● Disable

Figure 7.1. RIP Configuration Page

7.2.1 RIP Configuration Parameters

The following table defines the available configuration parameters for static routing configuration.

Table 7.1. Static Route Configuration Parameters

Field	Description
Interface	Select an interface through which the routing information is exchanged. Available options are LAN, WAN1, WAN2, PPPoE1, PPPoE2, PPPoE3 and PPPoE4.
RIP	Click the “Enable” or “Disable” radio button to enable or disable “RIP” for the interface selected. Note that you must enable RIP service first in the Management / System Services configuration page first.

Field	Description
Passive Mode	Enable this mode if RIP configured for this interface will only receive routing information from other routers and not send routing information to other routers. Disable this mode if you want this interface to send and receive routing information to/from other routers.
RIP Version (Send)	Select the RIP version for sending the routing information. Three options are available: Version 1. Version 2 and Both.
RIP Version (Receive)	Select the RIP version for receiving the routing information. Three options are available: Version 1. Version 2 and Both.
Authentication	Click on “Enable” or “Disable” radio button to enable/ disable authentication for exchanging the routing information. Note that all the routers exchanging routing information must use the same authentication key.
Authentication Mode	Select RIP authentication mode from the drop down list. Two modes are supported - Clear Text and MD5.
Authentication Key	Enter the authentication key shared by all the routers exchanging the routing information.

7.2.2 Configuring RIP

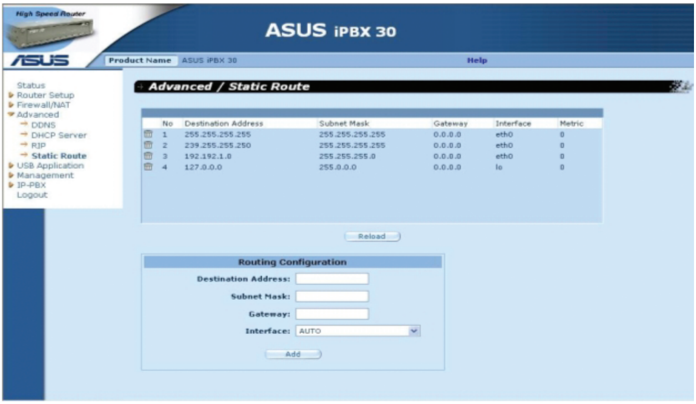
Follow these instructions to enable or disable RIP:

1. In the **System Services Configuration** page, click the **Enable** or **Disable** radio button depending on whether you want to enable or disable RIP.
2. Select an interface from the drop-down list for routing information exchange.
3. Click the **Enable** radio button to enable RIP for the particular interface selected.
4. Decide whether the RIP is operated in passive mode or not by clicking the **Enable** or **Disable** radio button.
5. Choose RIP version for sending and receiving the routing information. Available options are Version 1, Version 2 and Both.
6. Choose whether authentication is required by clicking the

Enable or **Disable** radio button.

7. (Optional) If authentication is enabled, you must also select authentication mode and the desired authentication key.
8. Click **Apply** to save the settings.

7.3 Static Route



No	Destination Address	Subnet Mask	Gateway	Interface	Metric
1	255.255.255.255	255.255.255.255	0.0.0.0	eth0	0
2	239.255.255.250	255.255.255.255	0.0.0.0	eth0	0
3	192.192.1.0	255.255.255.0	0.0.0.0	eth0	0
4	127.0.0.0	255.0.0.0	0.0.0.0	lo	0

Destination Address:
Subnet Mask:
Gateway:
Interface: AUTO

Figure 7.2. Static Route Configuration Page

7.3.1 Static Route Configuration Parameters

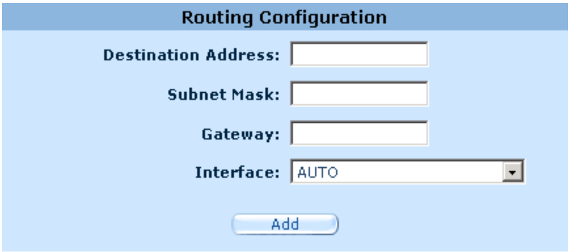
The following table defines the available configuration parameters for static routing configuration.

Table 7.2. Static Route Configuration Parameters

Field	Description
Destination Address	Specifies the IP address of the destination computer or an entire destination network. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway). Note that destination IP must be a network ID. The default route uses a destination IP of 0.0.0.0. Refer to Appendix 11 for an explanation of network ID.

Field	Description
Subnet Mask	Indicates which parts of the destination address refer to the network and which parts refer to a computer on the network. Refer to Appendix 11 for an explanation of network masks. The default route uses a 0.0.0.0 for subnet mask.
Gateway	Gateway IP address
Interface	Available option include AUTO, Eth0 (LAN), Eth1 (WAN), PPPoE:0 (unnumbered), PPPoE:1 (1st PPPoE session), PPPoE:2 (2nd PPPoE session). These options are selectable from the drop-down list. If AUTO is selected, the router will automatically assign an interface to route the packets based on the gateway IP address.

7.3.2 Adding Static Routes


Routing Configuration

Destination Address:

Subnet Mask:

Gateway:

Interface: AUTO

Figure 7.3. Static Route Configuration

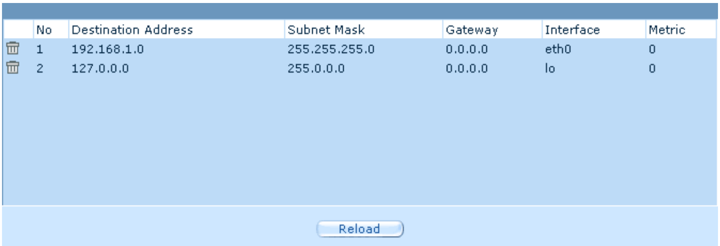
Follow these instructions to add a static route to the routing table.

1. Click the **Advanced ->Static Route** menu to open the **Static Route** configuration page.
2. Enter static routes information such as destination IP address, destination subnet mask, gateway IP address and the interface in the corresponding fields.

   To create a route that defines the default gateway for your LAN, enter 0.0.0.0 in both the Destination IP Address and Subnet Mask fields.

3. Click **Add** to add a new route.

7.3.3 Deleting Static Routes



	No	Destination Address	Subnet Mask	Gateway	Interface	Metric
🗑	1	192.168.1.0	255.255.255.0	0.0.0.0	eth0	0
🗑	2	127.0.0.0	255.0.0.0	0.0.0.0	lo	0

Figure 7.4. Sample Routing Table

Follow these instructions to delete a static route from the routing table.

1. Click the **Advanced ->Static Route** menu to open the Static Route configuration page.

2. Click on the 🗑 icon of the route to be deleted in the Routing Table.

WARNING Do not remove the route for default gateway unless you know what you are doing. Removing the default route will render the Internet unreachable.

7.3.4 Viewing the Static Routing Table

All IP-enabled computers and routers maintain a table of IP addresses that are commonly accessed by their users. For each of these destination IP addresses, the table lists the IP address of the first hop the data should take. This table is known as the device's routing table.

To view the iPBX30's routing table, click the **Advanced ->Static Route** menu. The Routing Table displays at the upper half of the Static Route Configuration page.

The Routing Table displays a row for each existing route containing the IP address of the destination network, subnet mask of destination network and the IP of the gateway that forwards the traffic.

8 Configuring DDNS

Dynamic DNS (DDNS) is a service that allows computers to use the same domain name, even when the IP address changes from time to time (during reboot or when the ISP's DHCP server resets IP leases). iPBX30 connects to a DDNS service provider whenever the WAN IP address changes. It supports setting up the web services such as Web server, FTP server using a domain name instead of the IP address. DDNS supports the DDNS clients with the following features:

- Update DNS records (addition) when an external interface comes up
- Force DNS update

HTTP DDNS Client

HTTP DDNS client uses the mechanism provided by the popular DDNS service providers for updating the DNS records dynamically. In this case, the service provider updates DNS records in the DNS. iPBX30 uses HTTP to trigger this update. iPBX30 supports HTTP DDNS update with the following service provider:

- www.dyndns.org

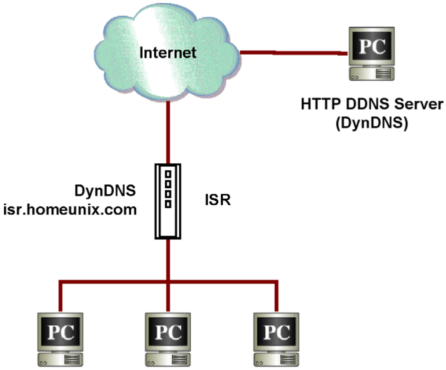


Figure 8.1. Network Diagram for HTTP DDNS

Whenever IP address of the configured DDNS interface changes, DDNS update is sent to the specified DDNS service provider. iPBX30 should be configured with the DDNS username and password that are obtained from your DDNS service provider.

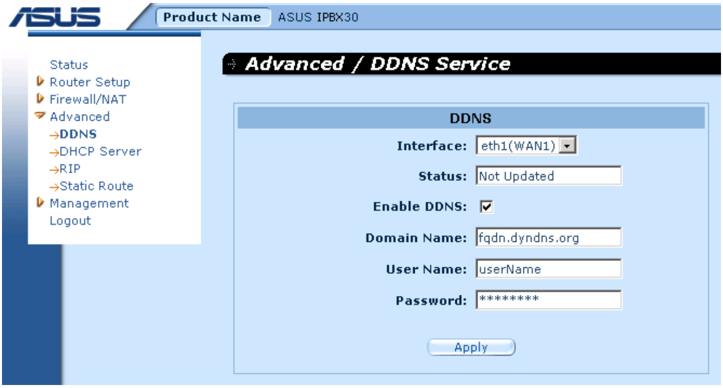
8.1 DDNS Configuration Parameters

The table below describes the configuration parameters available for DDNS service.

Table 8.1. DDNS Configuration Parameters

Field	Description
Interface	Select the interface that the DDNS service is to be used.
Status	Shows the state of DDNS.
Enable DDNS	Check this box to enable DDNS service; otherwise, keep the box unchecked.
Domain Name	Enter the registered domain name into this field. For example, If the host name of your iPBX30 is "host1" and the domain name is "yourdomain.com", The fully qualify domain name (FQDN) is "host1.yourdomain.com".
Username	Enter the username provided by your DDNS service provider in this field.
Password	Enter the password provided by your DDNS service provider in this field.

8.2 Configuring HTTP DDNS Client



Interface: eth1(WAN1)

Status: Not Updated

Enable DDNS: ☑

Domain Name: fqdn.dyndns.org

User Name: userName

Password: ********

Figure 8.2. HTTP DDNS Configuration Page

Follow these instructions to configure the HTTP DDNS:

1. Make sure you have registered a domain name to the DDNS service provider, dyndns. If you have not done so, visit www.dyndns.org for more details.
2. Click **Advanced -> DDNS Service** menu to open the DDNS configuration page.
3. Select the interface that the DDNS service is to be used.
4. Check **Enable DDNS** checkbox to enable the DDNS service.
5. Enter the registered domain name in the **Domain Name** field.
6. Enter the username and password provided by your DDNS service provider.
7. Click on **Apply** button to send a DNS update request to your DDNS service provider. Note that DNS update request will also be sent to your DDNS service provider automatically whenever the WAN port status is changed.

9 Configuring Firewall and NAT

The iPBX30 provides built-in firewall/NAT functions, enabling you to protect the system against denial of service (DoS) attacks and other types of malicious accesses to your LAN while providing Internet access sharing at the same time. You can also specify how to monitor attempted attacks, and who should be automatically notified.

This chapter describes how to create/modify/delete ACL (Access Control List) rules to control the data passing through your network. You will use firewall configuration pages to:

- Configure firewall global and DoS settings
- Create, modify, delete and view ACL rules.

When you define an ACL rule, you instruct the iPBX30 to examine each data packet it receives to determine whether it meets criteria set forth in the rule. The criteria can include the network or internet protocol it is carrying, the direction in which it is traveling (for example, from the LAN to the Internet or vice versa), the IP address of the sending computer, the destination IP address, and other characteristics of the packet data.

If the packet matches the criteria established in a rule, the packet can either be accepted (forwarded towards its destination), or denied (discarded), depending on the action specified in the rule.

9.1 Firewall Overview

9.1.1 Stateful Packet Inspection

The stateful packet inspection engine in the iPBX30 maintains a state table that is used to keep track of connection states of all the packets passing through the firewall. The firewall will open a “hole” to allow the packet to pass through if the state of the packet that belongs to an already established connection matches the state maintained by the stateful packet inspection engine. Otherwise, the packet will be dropped. This “hole” will be closed when the connection session terminates. No configuration is required for stateful packet inspection; it is enabled by default when the firewall is enabled. Please refer to section 9.3.1 “Firewall ” to enable or disable firewall service on the iPBX30.

9.1.2 DoS (Denial of Service) Protection

Both DoS protection and stateful packet inspection provide first line of defense for your network. No configuration is required for both protections on your network as long as firewall is enabled for the iPBX30. By default, the firewall is enabled at the factory. Please refer to section 9.3.1 “Firewall ” to enable or disable firewall service on the iPBX30.

9.1.3 Firewall and Access Control List (ACL)

9.1.3.1 Priority Order of ACL Rule

All ACL rules have a rule ID assigned – the smaller the rule ID, the higher the priority. Firewall monitors the traffic by extracting header information from the packet and then either drops or forwards the packet by looking for a match in the ACL rule table based on the header information.

The ACL rule checking starts from the rule with the smallest rule ID until a match is found or all the ACL rules are examined. If no match is found, the packet is dropped; otherwise, the packet is either dropped or forwarded based on the action defined in the matched ACL rule.

9.1.3.2 Tracking Connection State

The stateful packet inspection engine in the firewall keeps track of the state, or progress, of a network connection. By storing information about each connection in a state table, iPBX30 is able to quickly determine if a packet passing through the firewall belongs to an already established connection. If it does, it is passed through the firewall without going through ACL rule evaluation.

For example, an ACL rule allows outbound ICMP packet from 192.168.1.1 to 192.168.2.1. When 192.168.1.1 send an ICMP echo request (i.e. a ping packet) to 192.168.2.1, 192.168.2.1 will send an ICMP echo reply to 192.168.1.1. In the iPBX30, you don't need to create another inbound ACL rule because stateful packet inspection engine will remember the connection state and allows the ICMP echo reply to pass through the firewall.

9.1.4 Default ACL Rules

The iPBX30 supports two types of access rules:

- ACL Rules: for controlling all access to the computers on the LAN and DMZ and for controlling access to external networks for hosts on the LAN and DMZ.
- Self-Access Rules: for controlling access to the IPBX30 itself.

Default Access Rules

- All traffic from external hosts to the hosts on the LAN and DMZ is denied.
- All traffic originated from the LAN is forwarded to the external network using NAT.

WARNING: It is not necessary to remove the default ACL rule from the ACL rule table! It is better to create higher priority ACL rules to override the default rule.

9.2 NAT Overview

Network Address Translation allows use of a single device, such as the iPBX30, to act as an agent between the Internet (public network) and a local (private) network. This means that a NAT IP address can represent an entire group of computers to any entity outside a network. Network Address Translation (NAT) is a mechanism for conserving registered IP addresses in large networks and simplifying IP addressing management tasks. Because of the translation of IP addresses, NAT also conceals true network address from privy eyes and provide a certain degree security to the local network.

The NAT modes supported are static NAT, dynamic NAT, NAPT, reverse static NAT and reverse NAPT.

9.2.1 NAPT (Network Address and Port Translation) or PAT (Port Address Translation)

Also called IP Masquerading, this feature maps many internal hosts to one globally valid Internet address. The mapping contains a pool of network ports to be used for translation. Every packet is translated with the globally valid Internet address and the port number is translated with an un-used port from the pool of network ports. The figure below shows that all the hosts on the local network gain access to the Internet by mapping to only one globally valid IP address and different port numbers from a free pool of network ports.

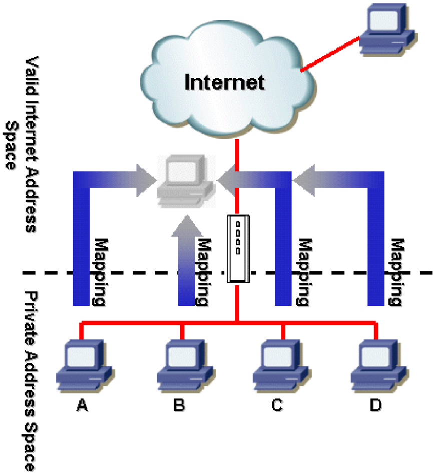


Figure 9.1 NAPT – Map Any Internal PCs to a Single Global IP Address

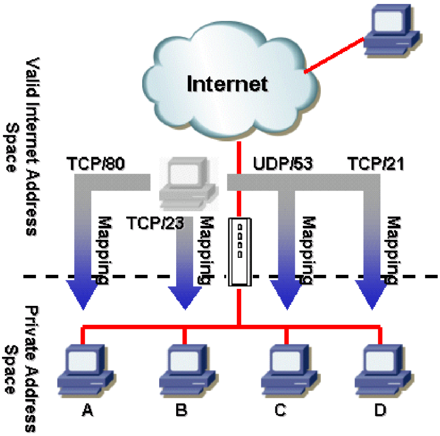


Figure 9.2 Reverse NAPT – Relayed Incoming Packets to the Internal Host Base on the Protocol, Port Number or IP Address

9.2.2 Reverse NAPT / Virtual Server

Reverse NAPT is also called inbound mapping, port mapping, or virtual server. Any packet coming to the iPBX30 can be relayed to the internal host based on the protocol, port number and/or IP address specified in the ACL rule. This is useful when multiple services are hosted on different internal hosts. Web server (TCP/80) is hosted on PC A, telnet server (TCP/23) on PC B, DNS server (UDP/53) on PC C and FTP server (TCP/21) on PC D. This means that the inbound traffic of these four services will be directed to respective host hosting these services.

9.3 Firewall Settings – (Firewall/NAT ->Settings)

9.3.1 Firewall Options

The table below lists the firewall options parameters.

Table 9.1. Firewall Options Parameters

Field	Description
DoS Check	Check or uncheck this box to enable or disable DoS check. When DoS check is disabled, the following functionalities are disabled: • Stateful packet inspection • Skip all DoS attack check
Default NAT	
Log Port Probing	Connection attempt to closed ports will be logged if this option is enabled.
Stealth Mode	If enabled, iPBX30 will not respond to remote peer's attempt to connect to the closed TCP/UDP ports.

To configure firewall settings, follow the instructions below:

1. Click on **Firewall/NAT ->Settings** menu to open the **Firewall Settings** configuration page.
2. Check or uncheck individual check box for each firewall option.
3. Click **Apply** to save the settings.

9.3.2 DoS Configuration

The iPBX30 has an Attack Defense Engine that protects internal networks from Denial of Service (DoS) attacks such as SYN flooding, IP smurfing, LAND, Ping of Death and all re-assembly attacks. It can drop ICMP redirects and IP loose/strict source routing packets. For example, a security device with the iPBX30 Firewall provides protection from "WinNuke", a widely used program to remotely crash unprotected Windows systems in the Internet. The iPBX30 Firewall also provides protection from a variety of common Internet attacks such as IP Spoofing, Ping of Death, Land Attack, and Reassembly attacks.

9.3.2.1 DoS Protection Configuration Parameters

The table below provides explanation for each type of DoS attacks. You may check or uncheck the check box to enable or disable the protection for each type DoS attacks.

Table 9.2. DoS Attack Definition

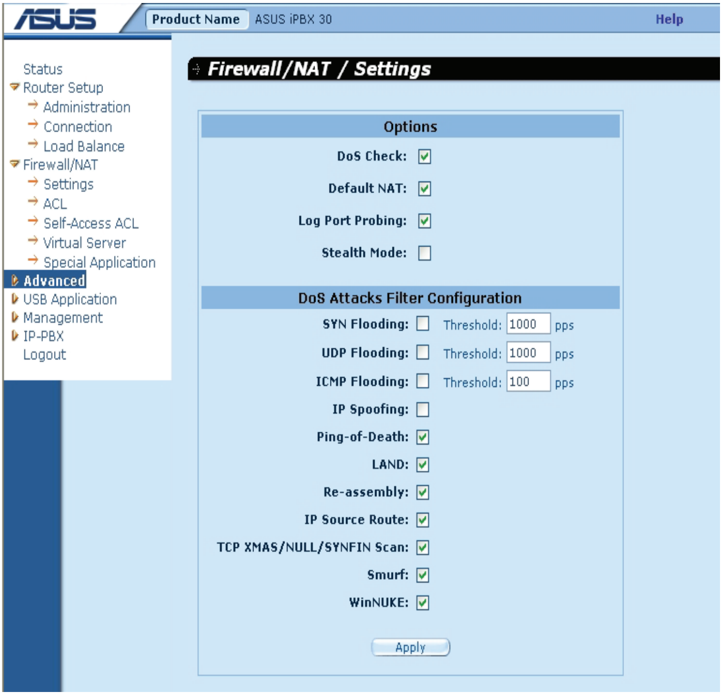
Field	Description
IP Source Route	Intruder uses "source routing" in order to break into the target system.
IP Spoofing	Spoofing is the creation of TCP/IP packets using somebody else's IP address. IP spoofing is an integral part of many network attacks that do not need to see responses.
Land	Attacker sends out packets to the system with the same source and destination IP address being that of the target system and causes the target system trying to resolve an infinite series of connections to itself. This can cause the target system to slow down drastically.
Ping of Death	An attacker sends out larger than 64KB packets to cause certain operating system to crash.
Smurf	An attacker issues ICMP echo requests to some broadcast addresses. Each datagram has a spoofed IP source address to be that of a real target-host. Most of the addressed hosts will respond with an ICMP echo reply, but not to the real initiating host, instead all replies carry the IP address of the previously spoofed host as their current destination and cause the victim host or network to slow down drastically.

Field	**Description**
SYN/ ICMP/ UDP Flooding	Check or un-check this option to enable or disable the logging for SYN/ICMP/UDP flooding attacks. These attacks involve sending lots of TCP SYN/ICMP/UDP to a host in a very short period. iPBX30 will not drop the flooding packets to avoid affecting the normal traffic.
TCP XMAS/ NULL/ FIN Scan	A hacker may be scanning your system by sending these specially formatted packets to see what services are available. Sometimes this is done in preparation for a future attack, or sometimes it is done to see if your system might have a service, which is susceptible to attack. **XMAS scan:** A TCP packet has been seen with a sequence number of zero and the FIN, URG, and PUSH bits are all set. **NULL scan:** A TCP packet has been seen with a sequence number of zero and all control bits are set to zero. **FIN scan:** A hacker is scanning the target system using a “stealth” method. The goal of the hacker is to find out if they can connect to the system without really connecting using the “FIN” scanning. It attempts to close a non-existent connection on the server. Either way, it is an error, but systems sometimes respond with different error results depending upon whether the desired service is available or not.
Re-assembly	In the teardrop attack, the attacker’s IP puts a confusing offset value in the second or later fragment. If the receiving operating system does not have a plan for this situation, it can cause the system to crash.
WinNUKE	Check or un-check this option to enable or disable protection against Winnuke attacks. Some older versions of the Microsoft Windows OS are vulnerable to this attack. If the computers in the LAN are not updated with recent versions/patches, you are advised to enable this protection by checking this check box.

9.3.2.2 Configuring DoS Settings

To configure DoS settings, follow the instructions below:

1. Click on **Firewall / NAT ->Settings** menu to open the Firewall General configuration page.
2. Check or uncheck individual check box for each type DoS protection.
3. Click **Apply** to save the settings.



Firewall/NAT / Settings

Options

DoS Check: ☑

Default NAT: ☑

Log Port Probing: ☑

Stealth Mode: ☐

DoS Attacks Filter Configuration

SYN Flooding: ☐ Threshold: 1000 pps

UDP Flooding: ☐ Threshold: 1000 pps

ICMP Flooding: ☐ Threshold: 100 pps

IP Spoofing: ☐

Ping-of-Death: ☑

LAND: ☑

Re-assembly: ☑

IP Source Route: ☑

TCP XMAS/NULL/SYNFIN Scan: ☑

Smurf: ☑

WinNUKE: ☑

Figure 9.3. Firewall General Configuration Page

9.4 ACL Rule Configuration Parameters

9.4.1 ACL Rule Configuration Parameters

The table below describes the configuration parameters firewall inbound, outbound and self-access ACL rules.

Table 9.3. ACL Rule Configuration Parameters

Field	**Description**
Traffic Direction – select from the available option in the drop-down list to configure the ACL. For dual-WAN configuration, two options are available – LAN ->WAN and WAN ->LAN. For WAN + DMZ configuration, six options are available – LAN ->WAN, WAN ->LAN, LAN ->DMZ, DMZ->LAN, WAN ->DMZ and DMZ ->WAN.	
ID	
Add New	Click on this option to add a new ACL rule.
Rule Number	Select a rule from the drop-down list, to modify its settings.
Move to This option allows you to set a priority for this rule. The iPBX30 Firewall acts on packets based on the priority of the rules. Set a priority by specifying a number for its position in the list of rules:	
1 (First)	This number marks the highest priority.
Other numbers	Select other numbers to indicate the priority you wish to assign to the rule.
Log Check this box to enable loggingfor this ACL rule; otherwise, keep it unchecked.	
Action	
Allow	Select this button to configure the rule as an allow rule. This rule when bound to the Firewall will allow matching packets to pass through.
Deny	Select this button to configure the rule as a deny rule. This rule when bound to the Firewall will not allow matching packets to pass through.
Route to – keep the setting to “AUTO” unless packets are routed to specific interface. Available options include AUTO, eth1 (WAN1), eth2 (WAN2), PPP1 (WAN1-unnumbered), PPP1 (WAN2-unnumbered), PPP3 (WAN1-PPPoE1), PPP4 (WAN1-PPPoE2), PPP5 (WAN2-PPPoE1), PPP6 (WAN2-PPPoE2). If WAN interface is set to DMZ mode, only AUTO, eth1, PPP1/3/4 are available. These options are selectable from the drop-down list. If AUTO is selected, the router will route the packets based on the information in the routing table.	

Field	Description
NAT	
None	Select this option if you don't intend to use NAT in this ACL rule.
IP Address	Select this option to specify the source IP address for outgoing traffic. This option is called.
Auto	iPBX30 automatically uses the IP address of the interface as the source IP address for outgoing traffic. It is recommended that you select this option if NAT is to be used for outgoing traffic.
Source This option allows you to set the source network to which this rule should apply. Use the drop-down list to select an option:	
Any	This option allows you to apply this rule to all the computers in the source network, such as those on the Internet for the inbound traffic or all the computers in the local network for outbound traffic.
IP Address	This option allows you to specify an IP address on which this rule will be applied.
IP Address	Specify the appropriate network address
Subnet	This option allows you to include all the computers that are connected in an IP subnet. When this option is selected, the following fields become available:
Field	**Description**
Address	Enter the appropriate IP address.
Mask	Enter the corresponding subnet mask.
MAC Address	This option allows you to specify a MAC address on which this rule will be applied.
MAC	Enter the desired MAC address.
Destination This option allows you to set the destination network to which this rule should apply. Use the drop-down list to select one of the following options:	
Any	This option allows you to apply this rule to all the computers in the local network for inbound traffic or any computer in the Internet for outbound traffic.

IP Address, Subnet	Select any of these options and enter details as described in the Source IP section above.
Service Select a service, from the drop-down list, to which this rule should apply. If the desired service is not listed, click on the Edit button to create a new service.	
Time Select a time slot during which this rule should apply.	
Enable	Check this box if you want to activate the ACL rule at the time specified. Uncheck this box to make the rule active at all times
Date and Time	Chck the desired dates and time for this ACL rule.

Table 9.4. Service Configuration Parameters

Field	**Description**
Service Name Enter a distinctive name identifying the new service.	
Protocol Select a protocol type from the drop-down list. Available options are All, TCP, UDP, ICMP, IGMP, AH ESP and TCP/UDP.	
Port This option allows you to specify the port number(s) used by the device. Use the drop-down list to select one of the following options:	
Any	Select this option if the service is used to designate an arbitary application.
Single	Select this option if the service uses a specific port number.
Port Number	Enter the port number
Range	Select this option if the service uses a range of ports. The following fields become available for entry when this option is selected.
Start Port	Enter the starting value of the port range
End Port	Enter the ending value of the port range

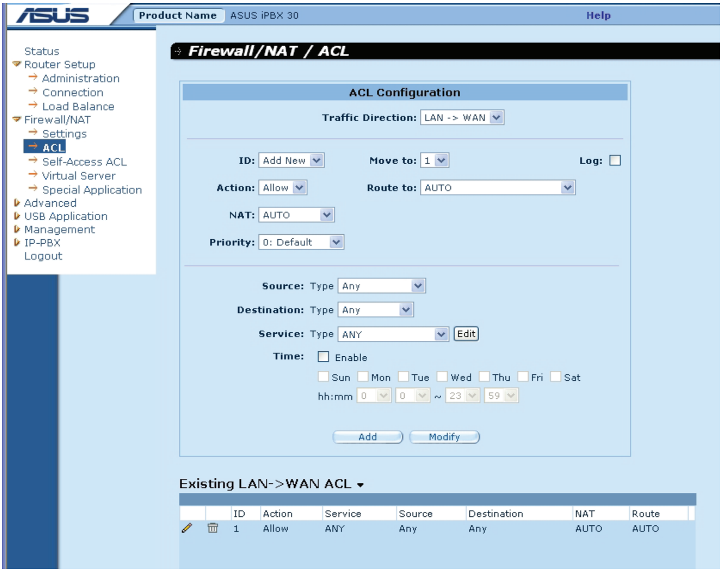
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td colspan="2">This option allows you to select the ICMP message type for the service. The supported ICMP message types are:
• Any (default)
• 0: Echo reply
• 1: Type 1
• 2: Type 2
• 3: Dst unreach: destination unreachable
• 4: Src quench: source quench
• 5: Redirect
• 6: Type 6
• 7: Type 7
• 8: Echo req:
• 9: Router advertisement
• 10: Router solicitation
• 11: Time exceed: time exceeded
• 12: Parameter problem
• 13: Timestamp request
• 14: Timestamp reply
• 15: Info request: information request
• 16: Info reply: information reply
• 17: Addr mask req: address mask request
• 18: Addr mask reply: address mask reply</td></tr>
</table>

9.5 Configuring ACL Rules – (Firewall ->ACL)

By creating ACL rules in the ACL configuration page, you can perform access control (allow or deny) to both the trusted and un-trusted networks.

Options in this configuration page allow you to:

- Add a rule, and set parameters for it
- Modify an existing rule
- Delete an existing rule
- View configured ACL rules



Traffic Direction: LAN -> WAN

ID: Add New **Move to:** 1 **Log:** ☐

Action: Allow **Route to:** AUTO

NAT: AUTO

Priority: 0: Default

Source: Type Any

Destination: Type Any

Service: Type ANY

Time: ☐ Enable

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

hh:mm 0 0 ~ 23 59

Existing LAN->WAN ACL

		ID	Action	Service	Source	Destination	NAT	Route
✎	🗑	1	Allow	ANY	Any	Any	AUTO	AUTO

Figure 9.4. ACL Configuration Page

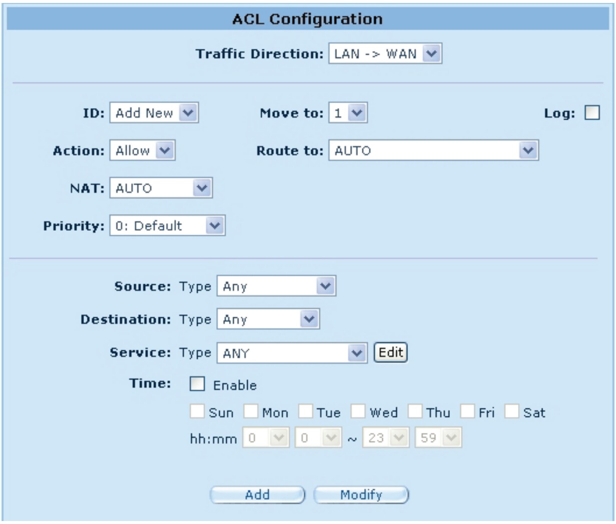
9.5.1 Add an ACL Rule

To add an ACL rule, follow the instructions below:

1. Click **Firewall/NAT ->ACL** menu to open the ACL Rule configuration page.
2. Select an option from the **Traffic Direction** drop-down list. For example, if you want to create an ACL to filter traffic originated from LAN and destined to WAN, then choose **LAN ->WAN** option.
3. Select **Add New** from the “ID” drop-down list.
4. Set desired action (Allow or Deny) from the **Action** drop-down list.
5. Select from the **Route To** drop-down list if you intend to direct the traffic to a specific interface. Choose AUTO if you want to have the iPBX30 to route the traffic automatically.
6. Choose NAT type and enter the required information for the selected NAT type.

7. Make changes to any or all of the following fields: source/destination IP, service, time and log.
8. Assign a priority for this rule by selecting a number from the **Move to** drop-down list. Note that the number indicates the priority of the rule with 1 being the highest. Higher priority rules will be examined prior to the lower priority rules by the firewall.
9. Click on the **Add** button to create the new ACL rule. The new ACL rule will then be displayed in the inbound access control list table at the bottom half of the Inbound ACL Configuration page.

The figure below illustrates how to create a rule to deny outbound HTTP traffic originated from the host w/ IP address 192.168.1.129.



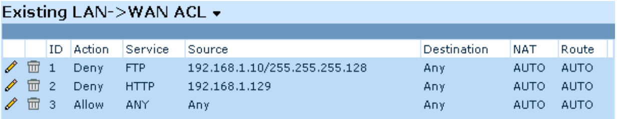
ACL Configuration

Traffic Direction: LAN -> WAN

ID: Add New
Move to: 1
Log: ☐
Action: Allow
Route to: AUTO
NAT: AUTO
Priority: 0: Default

Source: Type Any
Destination: Type Any
Service: Type ANY
Time: ☐ Enable
☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
hh:mm 0 0 ~ 23 59

Figure 9.5. ACL Configuration Example



Existing LAN->WAN ACL ▾

	ID	Action	Service	Source	Destination	NAT	Route
✎ 🗑	1	Deny	FTP	192.168.1.10/255.255.255.128	Any	AUTO	AUTO
✎ 🗑	2	Deny	HTTP	192.168.1.129	Any	AUTO	AUTO
✎ 🗑	3	Allow	ANY	Any	Any	AUTO	AUTO

Figure 9.6. Sample ACL List Table

9.5.2 Modify an ACL Rule

To modify an ACL rule, follow the instructions below:

1. Click **Firewall/NAT ->ACL** menu to open the ACL Rule Configuration page.
2. Click on the ✏ icon of the rule to be modified in the inbound ACL table or select the rule number from the **ID** drop-down list.
3. Make desired changes to any or all of the following fields: action, source/destination IP, service, time and log.
4. Click on the **Modify** button to modify this ACL rule. The new settings for this ACL rule will then be displayed in the access control list table at the bottom half of the ACL Configuration page.

9.5.3 Delete an ACL Rule

To delete an ACL rule, click on the 🗑 icon in front of the rule to be deleted.

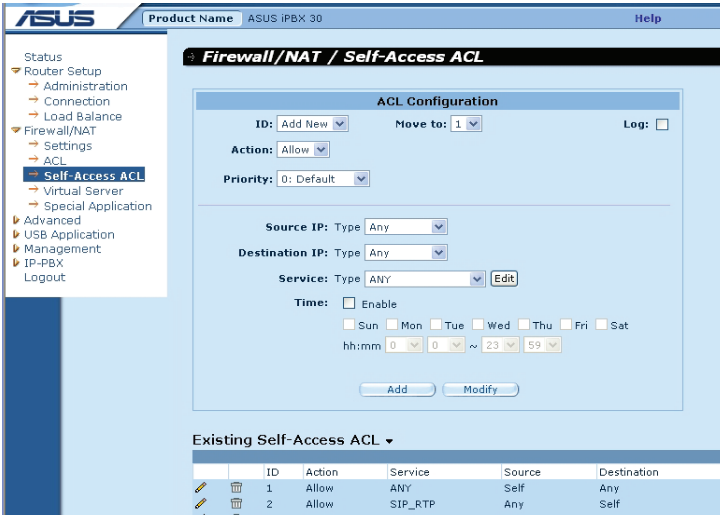
9.5.4 Display ACL Rules

To see existing ACL rules, just open the ACL Rule Configuration page by clicking **Firewall/NAT ->ACL** menu and then select a traffic direction from the T**raffic Direction** drop-down list.

9.6 Configuring Self-Access ACL Rules –(Firewall/NAT ->Self-Access ACL)

Self-Access rules control access to/from the iPBX30 itself. You may use Self-Access Rule Configuration page to:

- Add a Self-Access rule
- Modify an existing Self-Access rule
- Delete an existing Self-Access rule
- View existing Self-Access rules



ID: Add New
Move to: 1
Log: ☐
Action: Allow
Priority: 0: Default
Source IP: Type Any
Destination IP: Type Any
Service: Type ANY Edit
Time: ☐ Enable
☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
hh:mm 0 0 ~ 23 59

Existing Self-Access ACL

		ID	Action	Service	Source	Destination
✎	🗑	1	Allow	ANY	Self	Any
✎	🗑	2	Allow	SIP_RTP	Any	Self

Figure 9.7. Self-Access ACL Configuration Page

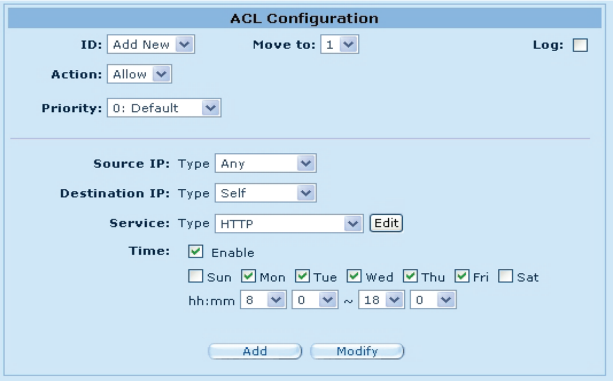
9.6.1 Add a Self-Access Rule

To add a Self-Access rule, follow the instructions below:

1. Click **Firewall/NAT ->Self-Access ACL** menu to open the Self-Access Rule Configuration page.
2. Select "**Add New**" from the "ID" drop-down list.
3. Set desired action (Allow or Deny) from the "**Action**" drop-down list.
4. Assign a priority for this rule by selecting a number from the "**Move to**" drop-down list. Note that the number indicates the priority of the rule with 1 being the highest. Higher priority rules will be examined prior to the lower priority rules by the firewall.
5. Make desired changes to any or all of the following fields: source/destination IP, service, time and log.
6. Click on the "**Add**" button to create the new Self-Access rule. The new rule will then be displayed in the Existing Self-Access ACL list table at the bottom half of the Self-Access ACL configuration page.

Example

The figure below shows a sample self-access ACL configuration to allow HTTP traffic from any one to iPBX30.


ACL Configuration

ID: Add New   Move to: 1   Log: ☐

Action: Allow

Priority: 0: Default

Source IP: Type Any

Destination IP: Type Self

Service: Type HTTP

Time: ☑ Enable

☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat

hh:mm 8 0 ~ 18 0

Figure 9.8. Self-Access ACL Configuration Example

9.6.2 Modify a Self-Access Rule

To modify a Self-Access rule, follow the instructions below:

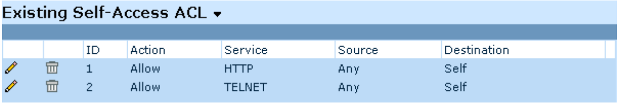
1. Click **Firewall/NAT ->Self-Access ACL** menu to open the Self-Access ACL configuration page.
2. Click on the icon of the Self-Access rule to be modified in the **Existing Self-Access ACL** table or select the Self-Access ACL from the **ID** drop-down list.
3. Make desired changes to any or all of the following fields: action, source/destination IP, service, time and log.
4. Click on the "**Modify**" button to save the changes. The new settings for this Self-Access rule will then be displayed in the Existing Self-Access ACL table located at the bottom half of the Self-Access ACL configuration page.

9.6.3 Delete a Self-Access Rule

To delete a Self-Access rule, click on the icon of the rule to be deleted.

9.6.4 View Configured Self-Access Rules

To see existing Self-Access Rules, just open the Self-Access ACL configuration page by clicking **Firewall/NAT ->Self-Access ACL** menu.



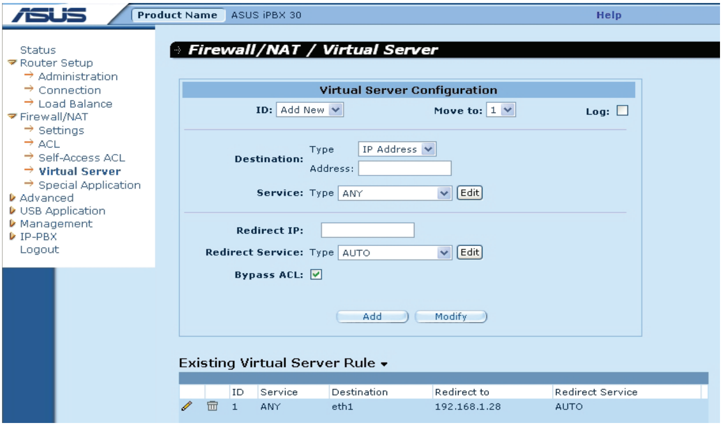
Existing Self-Access ACL ▾

		ID	Action	Service	Source	Destination
✎	🗑	1	Allow	HTTP	Any	Self
✎	🗑	2	Allow	TELNET	Any	Self

9.7 Configure Virtual Server

Virtual server allows you to configure up to ten public servers (such as a Web, E-mail, FTP server and etc.) accessible by external users of the Internet. Each service is provided by a dedicated server configured with a fixed IP Address. Although the internal service addresses are not directly accessible to the external users the router is able to identify the service requested by the service port number and redirects the request to the appropriate internal server.

Note: iPBX30 supports only one server of any particular type at a time.



Virtual Server Configuration

ID: Add New **Move to:** 1 **Log:** ☐

Destination: Type IP Address
Address:

Service: Type ANY

Redirect IP:

Redirect Service: Type AUTO

Bypass ACL: ☑

Existing Virtual Server Rule ▾

		ID	Service	Destination	Redirect to	Redirect Service
✎	🗑	1	ANY	eth1	192.168.1.28	AUTO

Figure 9.9. Virtual Server Configuration Page

9.7.1 Virtual Server Configuration Parameters

The table below describes the configuration parameters available for virtual server configuration.

Table 9.5. Virtual Server Configuration Parameters

Setting	Description
ID	
Add New	Click on this option to add a new virtual server.
Number	Select the ID of a virtual server from the drop-down list to modify its settings.
Move to	This option allows you to set a priority for virtual server rule check. NAT does the IP and/or port mapping based on the priority of the rules. Set a priority by specifying a number for its position in the list of rules
1 (First)	This number marks the highest priority.
Other numbers	Select other numbers to indicate the priority you wish to assign to the rule.
Destination	This option allows you to set the destination network to which this rule should apply. Use the drop-down list to select one of the following options:
IP Address	Enter the IP address of the virtual server if the virtual server has a known public IP address.
Interface	Use the IP address of the selected interface as the destination IP address. Available options are: eth1 (WAN1) eth2 (WAN2) ppp1 (WAN1 – unnumbered) ppp2 (WAN2 – unnumbered) ppp3 (WAN1 – PPPoE 1) ppp4 (WAN1 – PPPoE 2) ppp5 (WAN2 – PPPoE 1) ppp6 (WAN2 – PPPoE 2)
Service	Select a service, from the drop-down list, to which this rule should apply. If the desired service is not listed, click on the **Edit** button to create a new service.
Redirect IP	Enter the IP address of the computer (usually a server in your LAN) that you want the incoming traffic to be directed. For example, if IP address of the web server on your LAN is 192.168.1.28, please enter 192.168.1.28 here.

Setting	Description
Redirect Service	Select a service, from the drop-down list, to which this rule should apply. If the desired service is not listed, click on the "**Edit**" button to create a new service.
Bypass ACL	Check this option if you do not want firewall to perform access control on this virtual server. This means that the virtual server allows anyone to access the service provided. If you want to control who has access to this virtual server, un-check this option and create a proper ACL rule to control access to the virtual server.

Table 9.6. Port Numbers for Popular Applications

Application	Service Port Numbers
AOE II (Server)	2300-2400
AUTH	113
Baldurs Gate II	2300-2400
Battle Isle	3004-3004
Counter Strike	27005-27015
Cu See Me	7648-7648, 56800, 24032
Diablo II	4000-4000
DNS	UDP 53-53
FTP	TCP 21-21
FTP	TCP 20(ALG)-21
GOPHER	TCP 70-70
HTTP	TCP 80-80
THHP8080	TCP 8080-80880
HTTPS	TCP 443-443
I-phone 5.0	TCP/UDP 22555-22555
ISAKMP	UDP 500-500
mirc	66011-700
MSN Messenger	1863 ALG
Need for Speed 5	9400-9400
Netmeeting Audio	TCPP 1731-1731
Netmeeting Call	TCP 1720-1720
Netmeeting Conference	UDP 495000-49700
Netmeeting File Transfer	TCP 1503--1503

Application	Service Port Numbers
Netmeeting or VoIP	1503-1503, 1720(ALG)
NEWS	TCP 119-119
PC Anywhere	TCP 5631
PC Anywhere	TCP 5631, UDP 5632
POP3	TCP 110-110
Powwow Chat	13233-13233
Red Alert II	1234-1237
SMTP	TCP 25-25
Sudden Strike	2300-2400
TELNET	TCP 23-23
Win VNC	UDP 5800-5800

9.7.2 Virtual Server Example 1 – Web Server

The figure below shows illustrates the network topology for the web server deployment. This web server provides HTTP service using TCP port 8080.

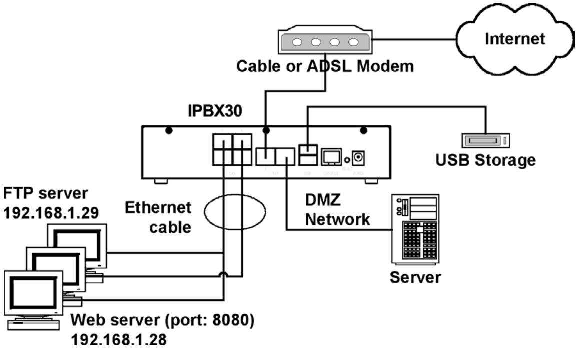
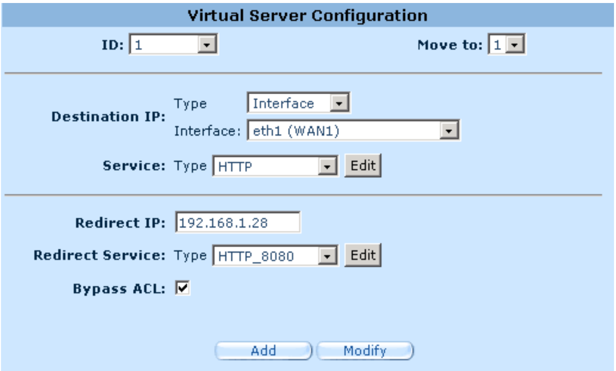


Figure 9.10. Virtual Server Deployment Topology

Following describes the procedure to setup the web server.

1. Click the **Firewall/NAT ->Virtual Server** menu to open the Virtual Server configuration page.
2. Select destination IP type and service type.



Virtual Server Configuration

ID: 1

Move to: 1

Destination IP: Type: Interface

Interface: eth1 (WAN1)

Service: Type: HTTP

Redirect IP: 192.168.1.28

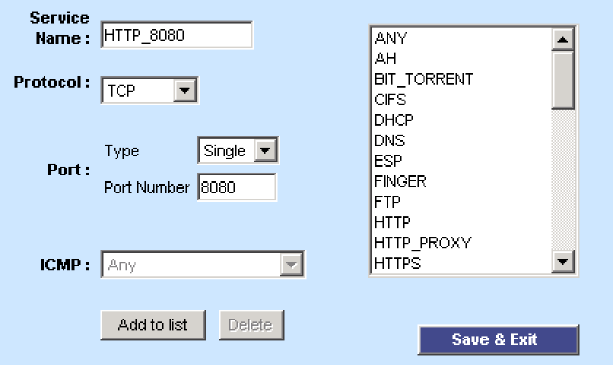
Redirect Service: Type: HTTP_8080

Bypass ACL: ☑

Figure 9.11. Virtual Server Example 1 – Web Server

3. Enter the IP address of the web server, which is 192.168.1.28, in **Redirect IP** field.

4. Since the web server is not using the standard TCP port, which is 80, for providing the http service, a new service type must be created for http service using TCP port 80. Click on the **Edit** button on the redirect service field to create a new service type. In the popped up Service configuration page, enter the service name, protocol and port number and then click on the **Add to list** to create the new service type, HTTP_8080. Finally, click the **Save & Exit** button to save the new service.



Service Name : HTTP_8080

Protocol : TCP

Port : Type: Single

Port Number: 8080

ICMP : Any

Figure 9.12. Adding a New Service

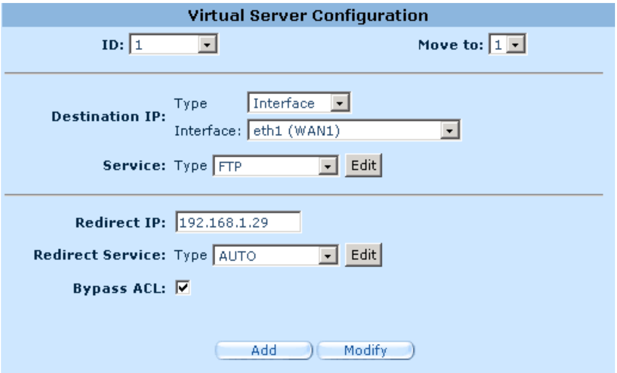
5. Select the service, HTTP_8080, from the Redirect Service drop-down list.
6. Click **Add** to save the virtual server settings.

9.7.3 Virtual Server Example 2 – FTP Server

This FTP server provides FTP service using standard FTP port.

Following describes the procedure to setup the FTP server.

1. Click the **Firewall/NAT ->Virtual Server** menu to open the Virtual Server configuration page.
2. Enter the needed information.
3. Click **Add** to save the virtual server settings.



Virtual Server Configuration

ID: 1 Move to: 1

Destination IP: Type Interface

Interface: eth1 (WAN1)

Service: Type FTP

Redirect IP: 192.168.1.29

Redirect Service: Type AUTO

Bypass ACL: ☑

Figure 9.13. Virtual Server Example 2 – FTP Server

9.7.4 Virtual Server Example 3 – FTP Server with Access Control

This example is similar to the previous example described in section 9.7.3 but with access control dictated by the firewall ACL rule. In this example, we want to limit the FTP server access to a network, 168.192.128.0.

The following describes the procedure to setup such a FTP service.

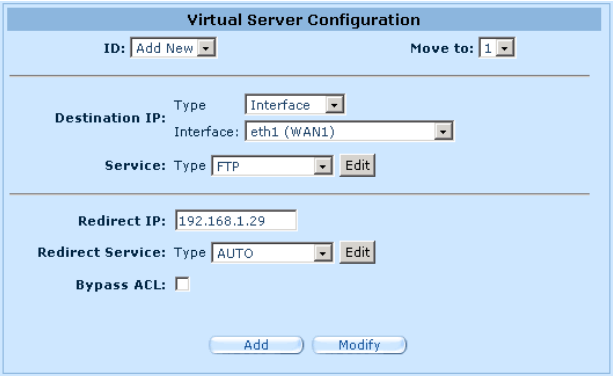
1. Create an FTP virtual server.

a) Click the **Firewall/NAT ->Virtual Server** menu to open the Virtual Server Configuration.

b) Enter the needed information.

c) Make sure that **Bypass ACL** box is unchecked.

d) Click **Add** to save the virtual server settings.



ID: Add New

Move to: 1

Destination IP: Type Interface

Interface: eth1 (WAN1)

Service: Type FTP

Redirect IP: 192.168.1.29

Redirect Service: Type AUTO

Bypass ACL: ☐

Figure 9.14. Virtual Server Example 3 – FTP Server

2. Create an ACL rule to control access to the FTP server.

a) Click **Firewall ->ACL** menu to open the ACL Rule configuration page.

b) Select **WAN ->LAN** option from the **Traffic Direction** drop-down list.

c) Select **Add New** from the **ID** drop-down list.

d) Select **Allow** from the **Action** drop-down list.

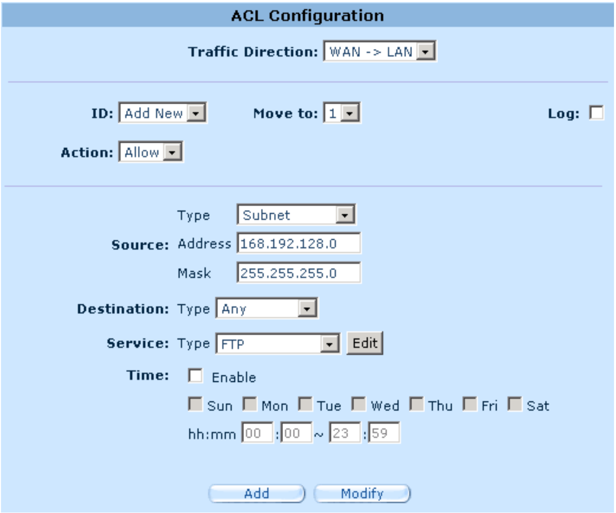
e) Select **Subnet** from the **Source Type** drop-down list.

f) Enter the **168.192.128.0** and **255.255.255.0** for the **Source Address** and **Mask** fields respectively.

g) Select **FTP** from the **Service Type** drop-down list.

h) Assign a priority for this rule by selecting a number from the **Move to** drop-down list. Note that the number indicates the priority of the rule with 1 being the highest. Higher priority rules will be examined prior to the lower priority rules by the firewall.

i) Click on the **Add** button to create the new ACL rule.



ACL Configuration

Traffic Direction: WAN -> LAN

ID: Add New

Move to: 1

Log: ☐

Action: Allow

Source: Type Subnet

Address 168.192.128.0

Mask 255.255.255.0

Destination: Type Any

Service: Type FTP

Time: ☐ Enable

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

hh:mm 00 : 00 ~ 23 : 59

Figure 9.15. Firewall ACL for Virtual Server Example 3 – FTP Server

9.8 Configuring Special Application

Some applications use multiple TCP/UDP ports to transmit data. Due to NAT, these applications cannot work with the router. Special Application setting allows some of these applications to work properly.

Note: Only one PC can use one particular special application at a time.

9.8.1 Special Application Configuration Parameters

The table below describes the configuration parameters available for virtual server configuration.

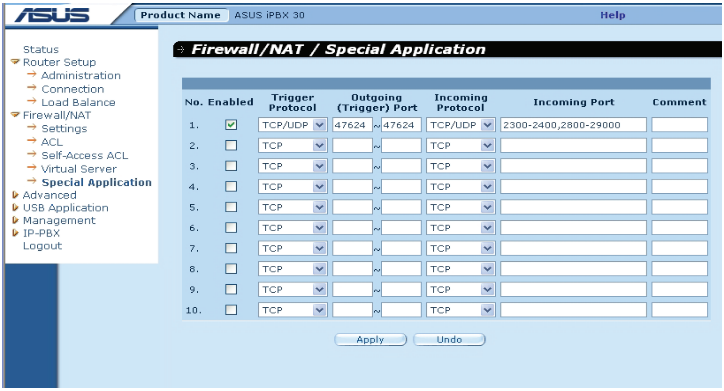
Table 9.7. Special Application Configuration Parameters

Setting	Description
Enabled	Check this box to activate the policy.
Trigger Protocol	Select the protocol type from the drop-down list. The available options are TCP, UDP and TCP/UDP.
Outgoing (Trigger) Port	The port range this application uses when it sends outbound packets. The outgoing port numbers act as the trigger. When the router detects the outgoing packets with these port numbers, it will allow the corresponding inbound packets with the incoming port numbers specified in the **Incoming Port Range** field to pass through the router.
Incoming Protocol	The protocol that the corresponding inbound packet used. The available options are TCP, UDP and TCP/UDP.
Incoming Port	The port range that the corresponding inbound packet used. The port range is indicated by a pair of numbers w/ a dash separating the numbers, e.g. 100-200. Multiple port ranges is separated by a comma, e.g. 100-200, 700-800.
Comment	You may enter a description for the application here, e.g. a name identifying the application.

Table 9.8. Port Numbers for Popular Applications

Application	Outgoing Port Number	Incoming Port Range
Battle.net	6112	6112
DialPad	7175	51200, 51201, 51210
ICU II	2019	2000-2038, 2050-2051, 2069, 2085, 3010-3030
MSN Gaming Zone	47624	2300-2400, 28800-29000
PC to Phone	12053	12120, 12122, 150-24220
Quick Time 4	554	6970-6999
wowcall	8000	4000-4020
Yahoo Messenger	5050	5000-5101

9.8.2 Special Application Example



No.	Enabled	Trigger Protocol	Outgoing (Trigger) Port		Incoming Protocol	Incoming Port	Comment
1.	☑	TCP/UDP	47624	~47624	TCP/UDP	2300-2400,2800-29000	
2.	☐	TCP		~	TCP		
3.	☐	TCP		~	TCP		
4.	☐	TCP		~	TCP		
5.	☐	TCP		~	TCP		
6.	☐	TCP		~	TCP		
7.	☐	TCP		~	TCP		
8.	☐	TCP		~	TCP		
9.	☐	TCP		~	TCP		
10.	☐	TCP		~	TCP		

Figure 9.16. Special Application Configuration Page

Following describes the procedure to setup a special application for MSN Gaming Zone.

1. Click the **Firewall/NAT ->Special Application** menu to open the Special Application configuration page.
2. Check **Enabled** checkbox.
3. Select **TCP/UDP** from the trigger protocol drop-down list. If you are not sure whether the application uses TCP or UDP protocol, you may select TCP/UDP in this field.
4. Enter outgoing port range, in this case: 47624 ~ 47624.
5. Select **TCP/UDP** from the incoming protocol drop-down list. If you are not sure whether the application uses TCP or UDP protocol, you may select TCP/UDP in this field.
6. Enter incoming port range, in this case: 2300-2400 and 28800-29000
7. In the **Comment** field, enter the name identifying this application, which is MSN Gaming Zone in this instance.
8. Click **Apply** to save the settings.

10 USB Application

This chapter describes how to configure the USB network storage for sharing your data via FTP service. The iPBX30 supports two USB2.0 ports on board and provides two major functions for attached USB storage space - FTP server and Voicemail and CDR data storage. Before using the FTP server, ensure that your USB storage meets the following requirements.

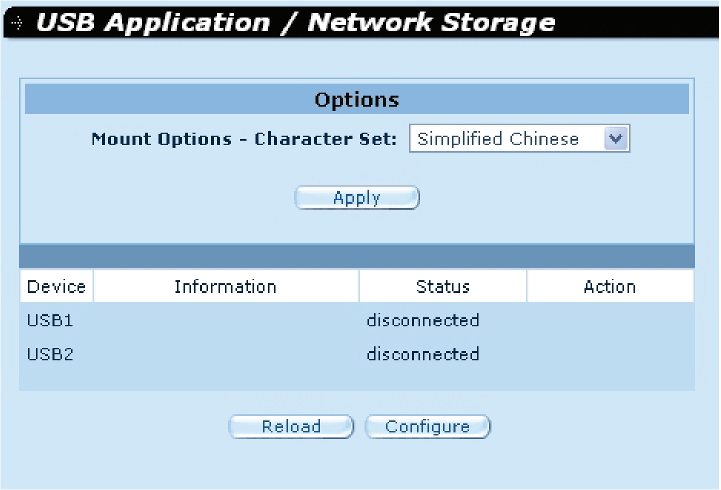
- Only HDD and flash drive are supported. CD-ROM and DVD drives are not supported. For a list of compatible devices, please refer to www.asus.com.
- Supports read/write functions for FAT/FAT32 and Linux EXT2 file systems. It does not support NTFS file system.
- Devices with multiple partitions can be detected; however, only the first five partitions are accessible.

Note: iPBX30 only supports USB storage recognized as a "Mass Storage Device" such as HDD and flash drives. Most compatible USB storage devices are plug and play; you do not need to power off the router when connecting these devices.

10.1 Configure USB Devices

To configure Network Storage settings, follow the instructions below:

1. Make sure that your USB storage is powered on and connected to one of the USB ports at the rear of your router.
2. Click **USB Application ->Network Storage** menu to open the Network Storage page.
3. Select an appropriate language from the Character Set drop down list for accessing your USB storage. Choose English if your USB storage contains only English characters.
4. Setup FTP service if necessary. Note that the USB storage will not be available until the FTP service is activated. To start FTP server configuration, click on the **Configure** button and follow the instructions described in section 10.3 "Configure FTP Service".



USB Application / Network Storage

Options

Mount Options - Character Set: Simplified Chinese

Device	Information	Status	Action
USB1		disconnected	
USB2		disconnected	

Figure 10.1. Network Storage – FTP Server Setting

Table 10.1. Network Storage Configuration

Setting	Description
Mount Options – Character Set	Select appropriate language for accessing your USB storage device. If your USB storage device contains simplified Chinese characters, please choose simplified Chinese language. Available options are simplified Chinese, traditional Chinese and English.
Device	Maximum of two USB storage devices are supported.
Information	This field shows the USB device's vendor information. Click the icon for further detail information of that device.
Status	Disconnected: no device is attached. Connected: device is attached but is not in use. You will see this status when the FTP service is not configured or the file system on the USB storage is not supported. Mounted: device is attached and in use. Note that system will mount the attached USB storage device automatically if FTP server is enabled and the file system on the device is supported.
Action	Mount: Make the USB storage device accessible by this router otherwise FTP server will not be able to access it. Unmount: Unload the USB storage so that you can safely remove it later.

10.2 View the Status of Attached USB Storage Devices

To view the status of attached USB storage devices, follow the instructions below:

1. Open the Network Storage page by clicking **USB Application** -> **Network Storage** menu.
2. Click on **Reload** button to see the updated status of the attached USB storage devices.

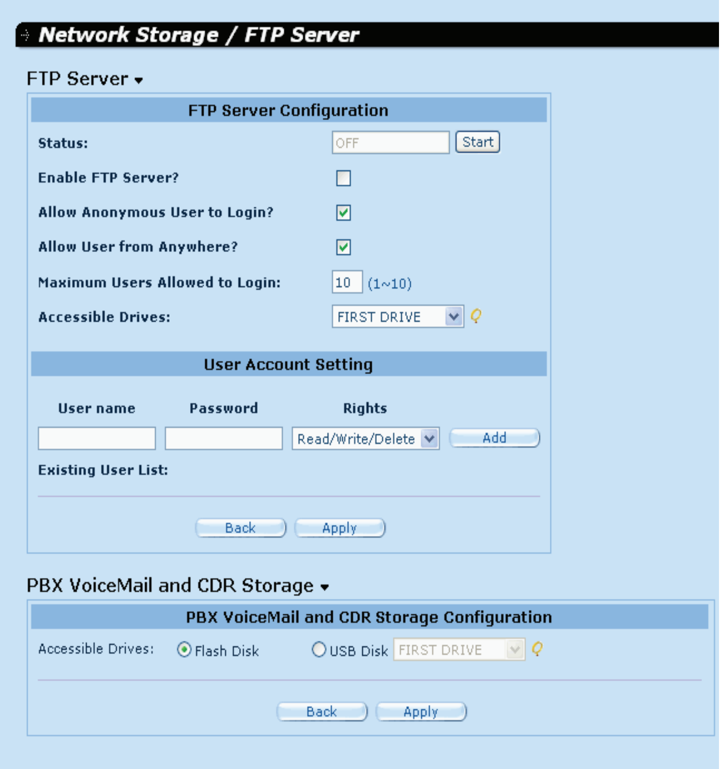
10.3 Configure FTP Service

To configure FTP service, follow the instructions below:

1. Click **USB Application ->Network Storage** menu to open the Network Storage page.
2. Click on **Configure** button to configure FTP service.
3. Check the desired options. Please refer to Table 10.2 FTP Server Configuration for details.
4. (Optional) Enter the username and password and select an access right from the drop-down list. This option is needed only when certain users are allowed to access the attached USB storage.
5. Click on the **Apply** button to save the settings.

To configure PBX Voicemail and CDR Storage on the same page, follow the instructions below:

1. Select the storage device of IP-PBX voice mail message and Call Detail Record (CDR). The default device is the on board 8Mbytes flash memory.
2. Click on the **Apply** button to save the settings.



Network Storage / FTP Server

FTP Server

FTP Server Configuration

Status: OFF

Enable FTP Server? ☐

Allow Anonymous User to Login? ☑

Allow User from Anywhere? ☑

Maximum Users Allowed to Login: 10 (1~10)

Accessible Drives: FIRST DRIVE

User Account Setting

User name	Password	Rights
		Read/Write/Delete

Existing User List:

PBX VoiceMail and CDR Storage

PBX VoiceMail and CDR Storage Configuration

Accessible Drives: ● Flash Disk ○ USB Disk FIRST DRIVE

Figure 10.2. Network Storage – FTP Server Configuration

Table 10.2. FTP Server Configuration

Setting	Description
Status	On: FTP server is activated. Off: FTP server is disabled.
Enable FTP Server	Check this box to activate the FTP service. Note that system will mount the attached USB storage device automatically if FTP server is enabled
Allow Anonymous User to Login	Select this if you allow anonymous users with read only access right to the FTP service. The user name is anonymous or ftp. No password is required.

Setting	Description
Allow User from Anywhere	Select this if you don't care about where the clients come from. If you do not select this option, you need to configure Firewall/NAT-> Sef-Access ACL to control who can access the FTP service. For example: allow your LAN network 192.168.1.0/24 access to FTP service.
Maximum Users Allowed to Login	Enter the maximum number of users allowed to log into FTP service simultaneously. Maximum number of users is 10.
Root Directory	If your USB storage device contains multiple partitions, choose the appropriate partition/drive as FTP server root directory. Choose First Drive if you want to use first mounted partition as FTP root directory. Note that only one partition can be accessed by FTP server.

Table 10.3. User Account Setting

Setting	Description
User name	Enter the user name for the FTP account.
Password	Enter the password of the FTP account.
Rights	This field indicates the access right assigned to this FTP account: Read/Write/Delete: Users associated with this account access right can read, write and delete files on the drive. Read/Write: Users associated with this account access right can read and write to the drive; however, users cannot delete files on the drive. Read Only: Users associated with this account access right can read files on the drive; however, users cannot write or delete files on the drive.

11 System Management

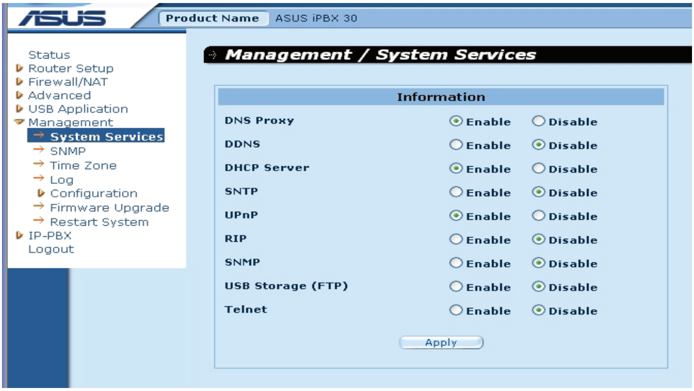
This chapter describes the following administrative tasks that you can perform using the web-based configuration software:

- Configure available system services
- Modify password and configure system settings
- View system information
- Modify system date and time
- Configure SNMP
- Reset system configuration to factory default settings
- Backup and restore system configuration
- Restart system
- Update firmware

11.1 Configure System Services

You can use the System Services configuration page to enable or disable services supported by the iPBX30. All services, except DDNS, SNTP, UPnP and RIP, are all enabled in the predefined configuration. To disable or enable individual service, follow the steps below:

1. Click **Management ->System** Services menu to open the System Services configuration page.
2. Click on the corresponding **Enable** or **Disable** radio button to enable or disable the desired service.
3. Click on **Apply** button to save the changes.



Management / System Services

Information		
DNS Proxy	● Enable	○ Disable
DDNS	○ Enable	● Disable
DHCP Server	● Enable	○ Disable
SNTP	○ Enable	● Disable
UPnP	● Enable	○ Disable
RIP	○ Enable	● Disable
SNMP	○ Enable	● Disable
USB Storage (FTP)	○ Enable	● Disable
Telnet	○ Enable	● Disable

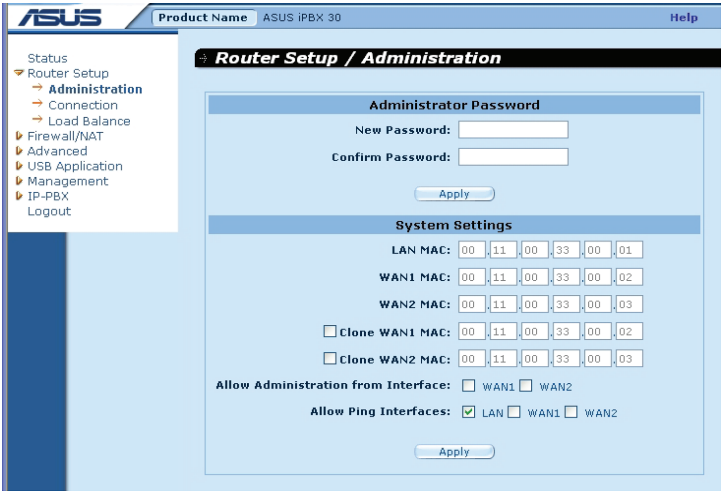
Figure 11.1. System Services Configuration Page

11.2 Login Password and System Settings

11.2.1 Changing Password

The first time you log into the configuration software, the default username and password (admin and admin) are used. For security reasons, it is advised that you change this password to avoid router configuration from unauthorized changes.

Note: This username and password is only used for logging into the configuration software; it is not the same login password that you use to connect to your ISP.



Router Setup / Administration

Administrator Password

New Password:

Confirm Password:

System Settings

LAN MAC: 00 . 11 . 00 . 33 . 00 . 01

WAN1 MAC: 00 . 11 . 00 . 33 . 00 . 02

WAN2 MAC: 00 . 11 . 00 . 33 . 00 . 03

☐ Clone WAN1 MAC: 00 . 11 . 00 . 33 . 00 . 02

☐ Clone WAN2 MAC: 00 . 11 . 00 . 33 . 00 . 03

Allow Administration from Interface: ☐ WAN1 ☐ WAN2

Allow Ping Interfaces: ☑ LAN ☐ WAN1 ☐ WAN2

Figure 11.2. System Administration Configuration Page

Follow the steps below to change password:

1. Click the **Router Setup ->Administration** menu to open the System Administration configuration page.

2. Changing login password

   a) Type the new password in the New Password text field and again in the Confirm Password text field. The password can be up to 16 characters long. The system distinguishes between upper and lower case characters.

3. Click on **Apply** button to save the new password.

11.2.2 Configure System Settings

Follow the steps below to modify the system settings:

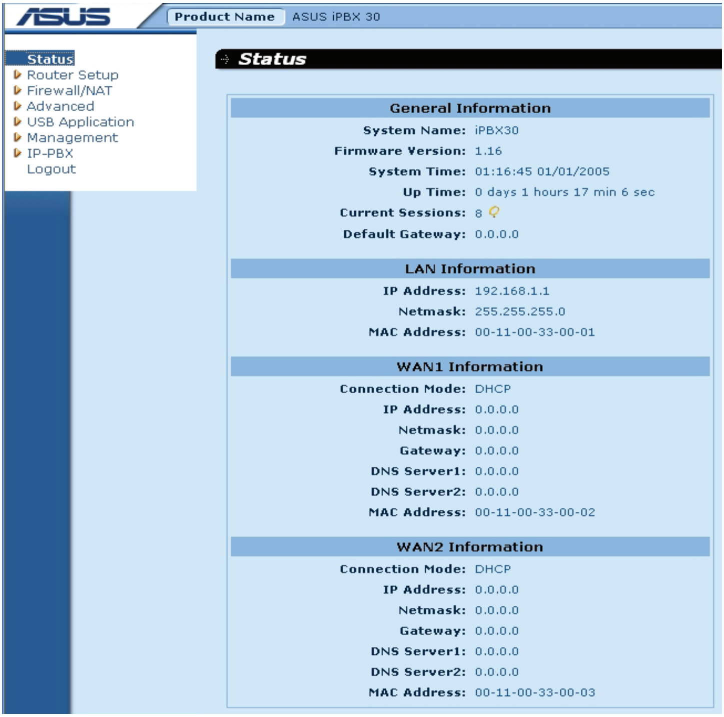
1. Click the **Router Setup ->Administration** menu to open the System Administration configuration page.
2. Clone the MAC address for WAN

a) If you had previously registered a specific MAC address with your ISP for Internet access, check the **Clone WAN MAC** check box and enter the registered MAC address here.

3. Allow Administration from WAN: check or uncheck the check box to enable or disable remote management via WAN port.
4. Allow Ping Interface: This option allows user to control access to the router using ping via the LAN or WAN ports. Check the respective check box to enable ping from the respective interface.
5. Click on **Apply** button to save the settings.

11.3 Viewing System Information

System Information page displays whenever you log into iPBX30. You may also click on the Status menu to see the system information. This page shows information of the overall system settings.



Product Name ASUS iPBX 30

Status

General Information

System Name: iPBX30
Firmware Version: 1.16
System Time: 01:16:45 01/01/2005
Up Time: 0 days 1 hours 17 min 6 sec
Current Sessions: 8
Default Gateway: 0.0.0.0

LAN Information

IP Address: 192.168.1.1
Netmask: 255.255.255.0
MAC Address: 00-11-00-33-00-01

WAN1 Information

Connection Mode: DHCP
IP Address: 0.0.0.0
Netmask: 0.0.0.0
Gateway: 0.0.0.0
DNS Server1: 0.0.0.0
DNS Server2: 0.0.0.0
MAC Address: 00-11-00-33-00-02

WAN2 Information

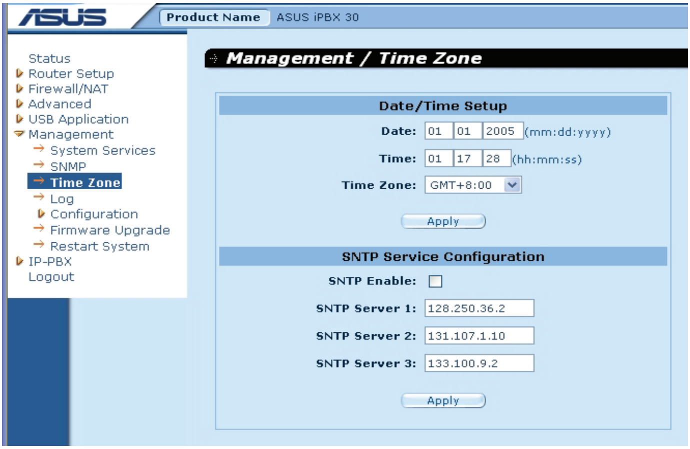
Connection Mode: DHCP
IP Address: 0.0.0.0
Netmask: 0.0.0.0
Gateway: 0.0.0.0
DNS Server1: 0.0.0.0
DNS Server2: 0.0.0.0
MAC Address: 00-11-00-33-00-03

Figure 11.3. System Information Page

11.4 Setup Date and Time

iPBX30 keeps a record of the current date and time, which it uses to calculate and report various data. Although there is a real time clock inside iPBX30; you may also rely on external time servers to maintain correct time. iPBX30 allows you to configure up to three external time servers. Make sure that the **Enable** check box is checked to activate the SNTP (Simple Network Time Protocol) service for time keeping.

Note: Changing the date and time on iPBX30 does not affect the date and time on your PCs.



Date/Time Setup

Date: 01 01 2005 (mm:dd:yyyy)

Time: 01 17 28 (hh:mm:ss)

Time Zone: GMT+8:00

SNTP Service Configuration

SNTP Enable: ☐

SNTP Server 1: 128.250.36.2

SNTP Server 2: 131.107.1.10

SNTP Server 3: 133.100.9.2

Figure 11.4. Time Zone Configuration Page

To manually change the time for the router:

1. Click the **Management ->Time Zone** menu to open the Time Zone configuration page.
2. Enter the current date and time in the proper fields.
3. Select your time zone from the drop-down list.
4. Click on **Apply** button to save the settings.

The synchronize the time between the real time clock and the external time servers:

1. Click the **Management ->Time Zone** menu to open the Time Zone configuration page.
2. Select your time zone from the drop-down list.
3. Check the **Enable** check box to activate the SNTP service.
4. Enter IP addresses for the SNTP servers that will be used to update the system time.
5. Click on **Apply** button to save the settings.

11.4.1 View the System Date and Time

To view the updated system date and time, log into the configuration software, click the **Management ->Time Zone** menu.

11.5 SNMP Setup

SNMP (Simple Network Management Protocol) as its name suggests is used for network management. You may use the SNMP configuration page to enable or disable the SNMP support.

11.5.1 SNMP Configuration Parameters

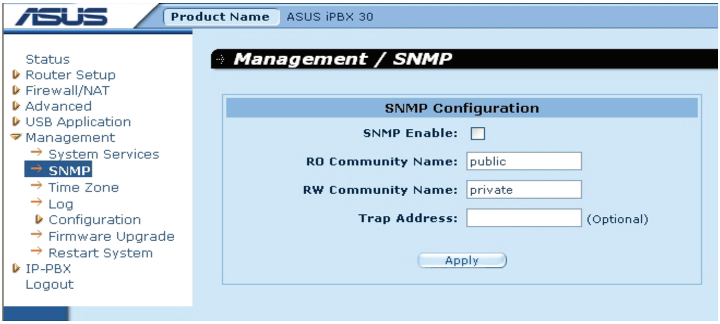
The table below describes the configuration parameters available for SNMP setup.

Table 11.1. SNMP Configuration Parameters

Field	Description
SNMP Enable	Check this box to enable the SNMP support; otherwise, uncheck this box.
RO Community Name	Community string is a clear text string that is used as password between the SNMP management station and the Internet Security Router. This "Read Only" community name is used by the SNMP management station to read the settings in the Internet Security Router.
RW Community Name	Community string is a clear text string that is used as password between the SNMP management station and the Internet Security Router. This "Read and Write" community name is used by the SNMP management station to read and configure the settings in the Internet Security Router.
Trap Address	Trap message is sent by the Internet Security Router to tell the SNMP management station that something has happened on the Internet Security Router. This field is used to enter the IP address of the SNMP management station that is supposed to receive trap messages from the Internet Security Router.

11.5.2 Configuring SNMP

1. Click the **Management ->SNMP** menu to open the SNMP configuration page.



SNMP Enable: ☐

RO Community Name: public

RW Community Name: private

Trap Address: (Optional)

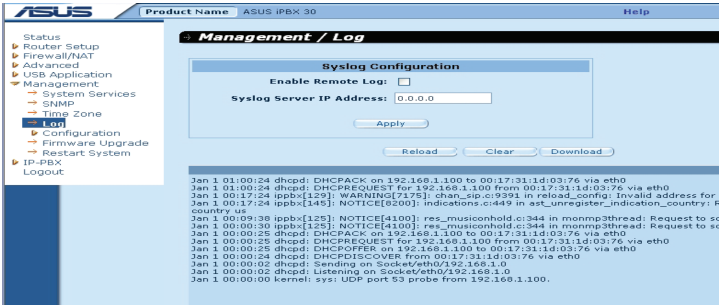
Figure 11.5. SNMP Configuration Page

2. Check the **SNMP Enable** box to enable the SNMP support; otherwise, uncheck the box.
3. Enter **RO** (read only) and **R/W** (read and write) community names.
4. Enter the IP address of the SNMP management station that receives trap messages from the iPBX30.
5. Click on **Apply** button to save the settings.

11.6 Log Setup

Log messages are stored in dynamic memory and will disappear after system is rebooted. To keep a copy of the log messages, you can setup a syslog server and have iPBX30 send out the log messages to the server.

11.6.1 Setting Up Remote Logging Using a Syslog Server



Enable Remote Log: ☐

Syslog Server IP Address: 0.0.0.0

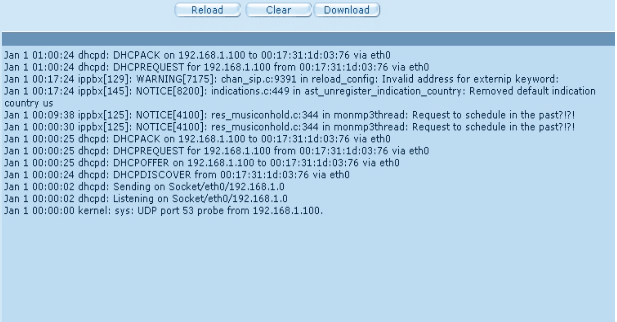
```
Jan 1 01:00:24 dhcpd: DHCPACK on 192.168.1.100 to 00:17:31:1d:03:76 via eth0
Jan 1 01:00:24 dhcpd: DHCPREQUEST for 192.168.1.100 from 00:17:31:1d:03:76 via eth0
Jan 1 00:17:24 ippbx[129]: WARNING[7175]: chan_sip.c:9391 in reload_config: Invalid address for
Jan 1 00:17:24 ippbx[145]: NOTICE[8200]: indications.c:449 in ast_unregister_indication_country: R
country us
Jan 1 00:09:38 ippbx[125]: NOTICE[4100]: res_musiconhold.c:344 in monmp3thread: Request to sc
Jan 1 00:00:30 ippbx[125]: NOTICE[4100]: res_musiconhold.c:344 in monmp3thread: Request to sc
Jan 1 00:00:25 dhcpd: DHCPACK on 192.168.1.100 to 00:17:31:1d:03:76 via eth0
Jan 1 00:00:25 dhcpd: DHCPREQUEST for 192.168.1.100 from 00:17:31:1d:03:76 via eth0
Jan 1 00:00:25 dhcpd: DHCPOFFER on 192.168.1.100 to 00:17:31:1d:03:76 via eth0
Jan 1 00:00:24 dhcpd: DHCPDISCOVER from 00:17:31:1d:03:76 via eth0
Jan 1 00:00:02 dhcpd: Sending on Socket/eth0/192.168.1.0
Jan 1 00:00:02 dhcpd: Listening on Socket/eth0/192.168.1.0
Jan 1 00:00:00 kernel: sys: UDP port 53 probe from 192.168.1.100.
```

Figure 11.6. Syslog Server Configuration

1. Click the **Management ->Log** menu to open the Log configuration page.
2. Click **Enable Remote Log** check box to enable remote logging.
3. Enter the syslog server IP address in the **Syslog Server IP Address** field.
4. Click on **Apply** button to save the settings.

11.6.2 View the System Log

You may open the firewall log page by clicking **Firewall/NAT ->Log** menu to see any logged. You may click on the **Reload** button at the bottom of the Log configuration page to see the updated log messages. To clear the log messages, just click on the **Clear Log** button.



```
Jan 1 01:00:24 dhcpd: DHCPACK on 192.168.1.100 to 00:17:31:1d:03:76 via eth0
Jan 1 01:00:24 dhcpd: DHCPREQUEST for 192.168.1.100 from 00:17:31:1d:03:76 via eth0
Jan 1 00:17:24 ippbx[129]: WARNING[7175]: chan_sip.c:9391 in reload_config: Invalid address for externip keyword:
Jan 1 00:17:24 ippbx[145]: NOTICE[8200]: indications.c:449 in ast_unregister_indication_country: Removed default indication
country us
Jan 1 00:09:38 ippbx[125]: NOTICE[4100]: res_musiconhold.c:344 in monmp3thread: Request to schedule in the past?!?!
Jan 1 00:00:30 ippbx[125]: NOTICE[4100]: res_musiconhold.c:344 in monmp3thread: Request to schedule in the past?!?!
Jan 1 00:00:25 dhcpd: DHCPACK on 192.168.1.100 to 00:17:31:1d:03:76 via eth0
Jan 1 00:00:25 dhcpd: DHCPREQUEST for 192.168.1.100 from 00:17:31:1d:03:76 via eth0
Jan 1 00:00:25 dhcpd: DHCPOFFER on 192.168.1.100 to 00:17:31:1d:03:76 via eth0
Jan 1 00:00:24 dhcpd: DHCPDISCOVER from 00:17:31:1d:03:76 via eth0
Jan 1 00:00:02 dhcpd: Sending on Socket/eth0/192.168.1.0
Jan 1 00:00:02 dhcpd: Listening on Socket/eth0/192.168.1.0
Jan 1 00:00:00 kernel: sys: UDP port 53 probe from 192.168.1.100.
```

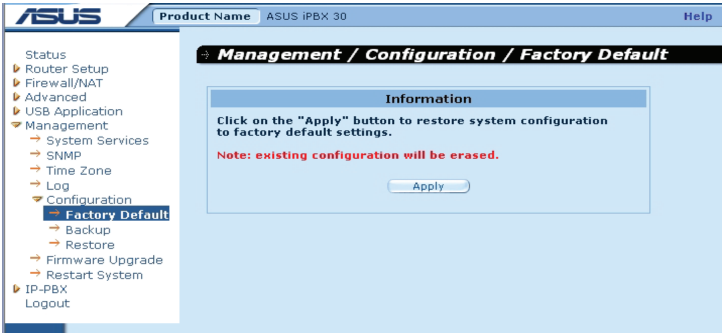
Figure 11.7 Sample Log

11.7 Configuration Management

11.7.1 Restore System Configuration to Factory Default Settings

At times, you may want to restore system configuration to the factory default settings to eliminate problems resulted from incorrect system configuration. Follow the steps below to reset the system configuration:

1. To open the Factory Default configuration page, click the **Management ->Configuration ->Factory Default** menu.



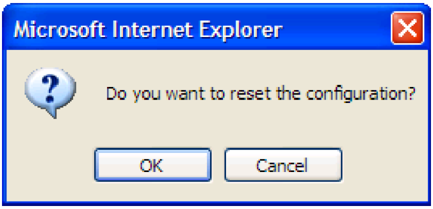
Click on the "Apply" button to restore system configuration to factory default settings.

Note: existing configuration will be erased.

Figure 11.8 Factory Reset Page

2. Click on **Apply** button to restore the system configuration to the factory default settings.

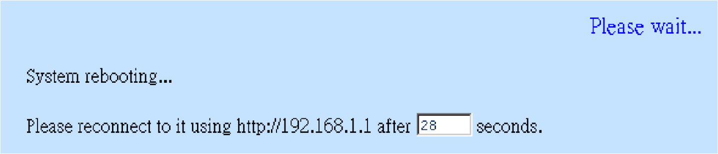
3. A dialog window will pop up to ask for confirmation. Click on the **OK** button to proceed; otherwise, click on the **Cancel** button to cancel the action.



Do you want to reset the configuration?

Figure 11.9 Factory Reset Confirmation

4. iPBX30 will then reboot thereafter to make the factory default configuration in effect. A count-down timer displays to indicate when the reboot process will be completed.



Please wait...

System rebooting...

Please reconnect to it using http://192.168.1.1 after 28 seconds.

Figure 11.10 Factory Reset Count Down Timer

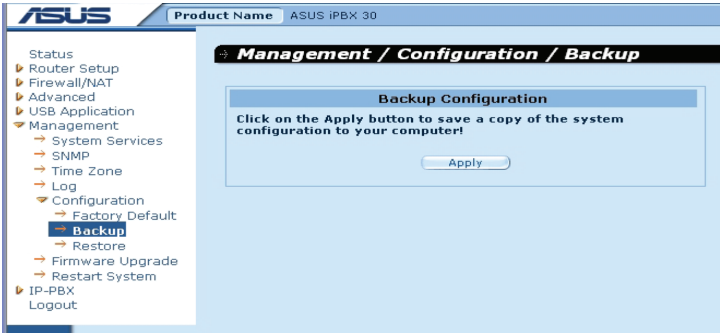
Sometimes, you may find that you have no way to access the iPBX30, e.g. you forget your password or the IP address of iPBX30. The only way out in this scenario is to reset the system configuration to the factory default by pressing the reset button for at least 5 seconds. The system configuration will be reverted back to the factory default settings after iPBX30 is rebooted.

11.7.2 Backup System Configuration

Follow the steps below to backup system configuration:

1. Click the **Management ->Configuration ->Backup** menu to open the Configuration Backup page.

2. Click on **Apply** button to backup the system configuration.



Product Name: ASUS iPBX 30

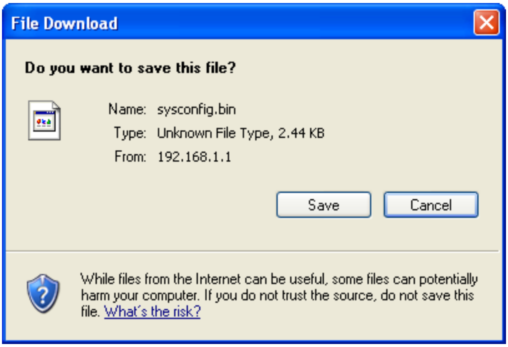
Management / Configuration / Backup

Backup Configuration

Click on the Apply button to save a copy of the system configuration to your computer!

Figure 11.11 Backup System Configuration Page

3. Click on **Save** button to backup the system configuration.



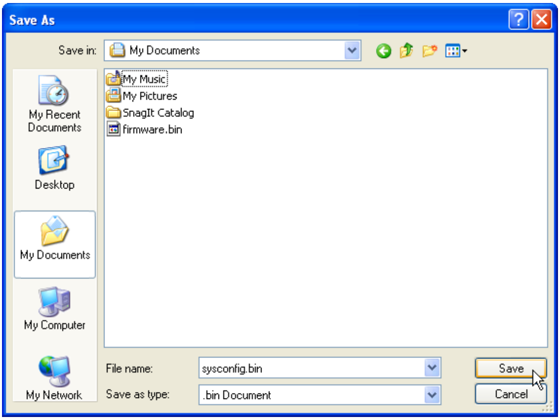
File Download

Do you want to save this file?

Name: sysconfig.bin
Type: Unknown File Type, 2.44 KB
From: 192.168.1.1

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

4. Click on button to backup the system configuration.



Save in: My Documents

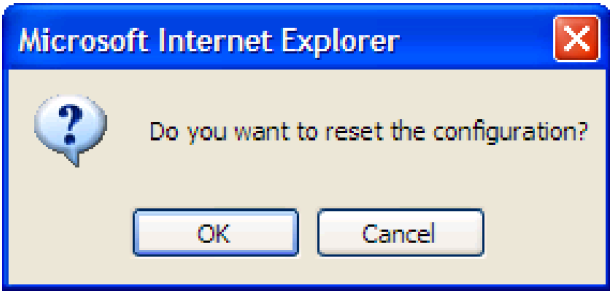
File name: sysconfig.bin

Save as type: .bin Document

11.7.3 Restore System Configuration

Follow the steps below to backup system configuration:

1. Click the **Management ->Configuration ->Restore** menu to open the System Configuration Restore page.



Do you want to reset the configuration?

Figure 11.12 Restore System Configuration Page

2. Enter the path and name of the system configuration file that you want to restore in the **Configuration File** text box. Alternatively, you may click on the **Browse** button to search for the system configuration file on your hard drive. A window will pop up for you to select the configuration file to restore.

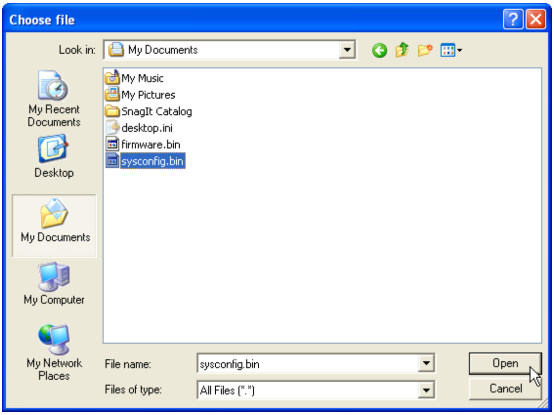
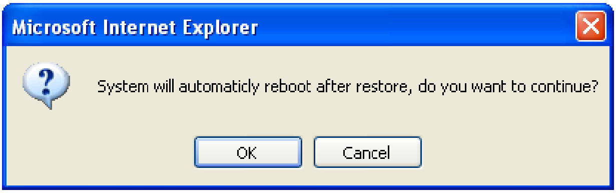


Figure 11.13 Selecting System Configuration from the File Manager

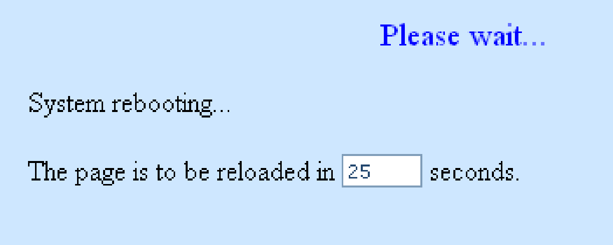
3. Click on **Apply** button to restore the system configuration. A dialog window, such as the one below, will pop up to ask for confirmation for restoring the system configuration. Click the **OK** button to proceed; otherwise, click the **Cancel** button to cancel the action. The iPBX30 will reboot for the new system configuration to take effect.



System will automaticly reboot after restore, do you want to continue?

Figure 11.14 System Configuration Restoration Confirmation

4. A system reboot count down timer will display. You'll be reconnected back to iPBX30 when the counter returns to zero. You may need to manually connect back to the iPBX30 if you are not connected back to iPBX30 automatically.



Please wait...

System rebooting...

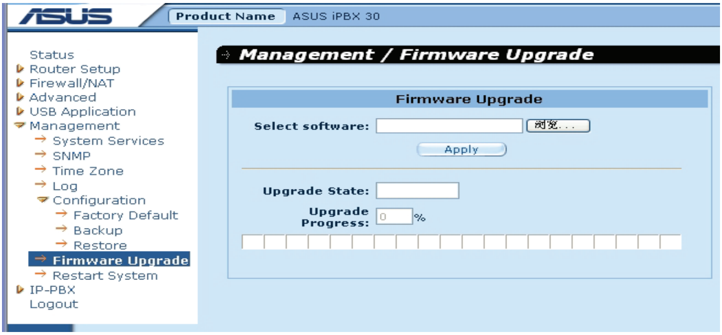
The page is to be reloaded in 25 seconds.

Figure 11.15 System Reboot Counter Timer

11.8 Firmware Upgrade

ASUSTeK may from time to time provide you with an update to the firmware running on the iPBX30. All system software is contained in a single file, called an image. Web UI Management provides an easy way to upload the new firmware image. To upgrade the image, follow this procedure:

1. Click the **System ->Firmware Upgrade** menu to open the Firmware Upgrade page.



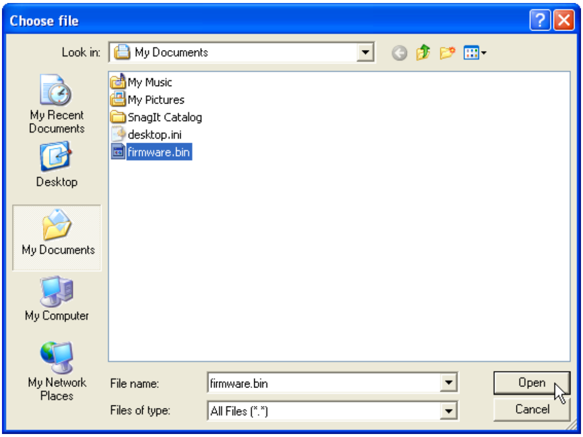
Select software:

Upgrade State:

Upgrade Progress: 0 %

Figure 11.16 Firmware Upgrade Page

2. In the Select Firmware text box, enter the path and name of the firmware image file. Alternatively, you may click on **Browse** button to open a file manager to search for the firmware image on your computer.



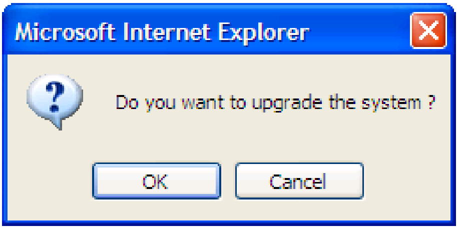
Look in: My Documents

File name: firmware.bin

Files of type: All Files (*.*)

Figure 11.17 Selecting Firmware from the File Manager

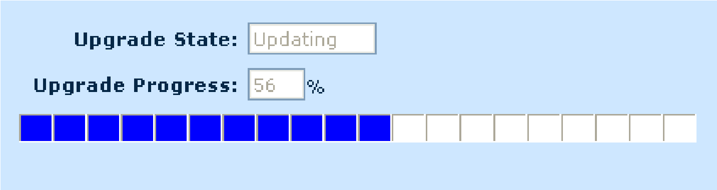
3. Click on **Apply** button to update the firmware. A dialog window, such as the one below, will pop up to ask for confirmation of the firmware upgrade. Click the OK button to proceed; otherwise, click the Cancel button to cancel the action.



Do you want to upgrade the system ?

Figure 11.18 Firmware Upgrade Confirmation

4. Firmware upgrade status and progress will be shown.

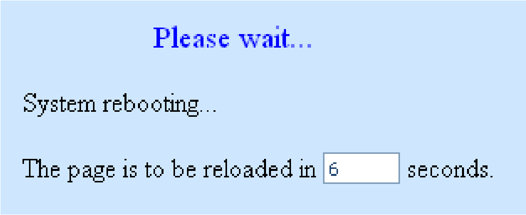


Upgrade State: Updating

Upgrade Progress: 56 %

Figure 11.19 Firmware Upgrade Progress

5. A count down timer will display after the firmware upgrade is completed. You'll be reconnected back to iPBX30 when the counter returns to zero. You may need to manually connect back to the iPBX30 if you are not connected back to iPBX30 automatically.



Please wait...

System rebooting...

The page is to be reloaded in 6 seconds.

Figure 11.20 System Reboot Count Down Timer for Firmware Upgrade

6. When you are reconnected to the iPBX30, click **Status** menu to check if the new firmware is properly upgraded. You probably need to clear the cache of your web browser to see the new System Information page. Following is the procedure to clear the browser cache for Microsoft Internet Explorer:

   a) Click on **Tools** menu.

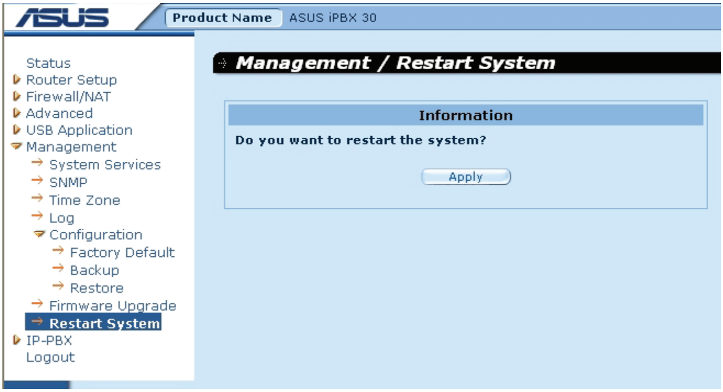
   b) Click on **Internet Options** menu.

   c) Click on **Delete Files** button to clear the browser cache.

11.9 Restart System

1. Click the **Management ->Restart System** menu to open the Restart System page.

2. Click on the **Apply** button to restart the system.



Management / Restart System

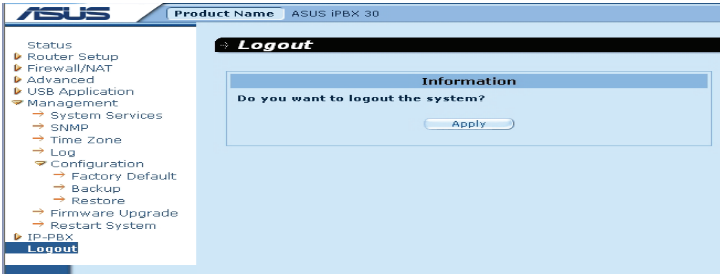
Information

Do you want to restart the system?

Figure 11.21 Restart System Page

11.10 Logout from the Web UI Management

To logout of the configuration software, open the Logout page by clicking the Logout menu and click on the **Apply** button. If you are using IE as your browser, a window will prompt for confirmation before closing your browser.

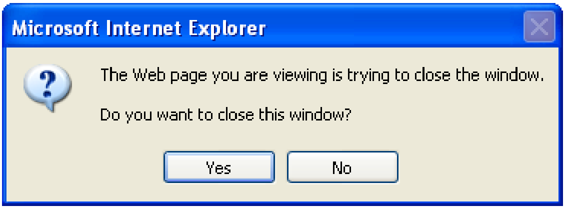


Logout

Information

Do you want to logout the system?

Figure 11.22 Logout Page



Microsoft Internet Explorer

The Web page you are viewing is trying to close the window.

Do you want to close this window?

Figure 11.23 Confirmation for Closing Browser (IE)

12 SIP IP-PBX

The iPBX30 integrates the functionalities of SIP registrar server, proxy server and voice media application, supporting up to 30 SIP clients with all necessary call functions together with voice mail capability.

The iPBX30 can work with any RFC3261 compliant gateway, IP phone, ATA. iPBX30 can connect to legacy PBX by the FXS/FXO ports of gateway, and is able to handle up to10 concurrent calls.

The following diagram shows a typical iPBX30 application scenario in office.

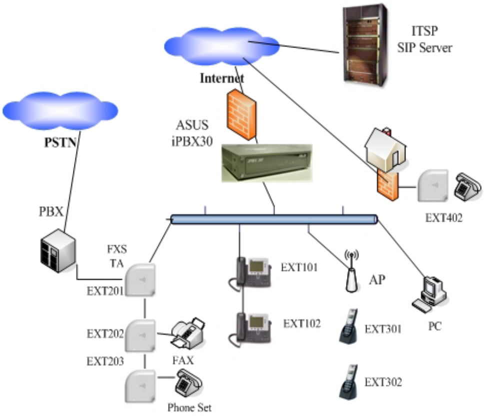


Figure 12.1 iPBX30 application office scenario

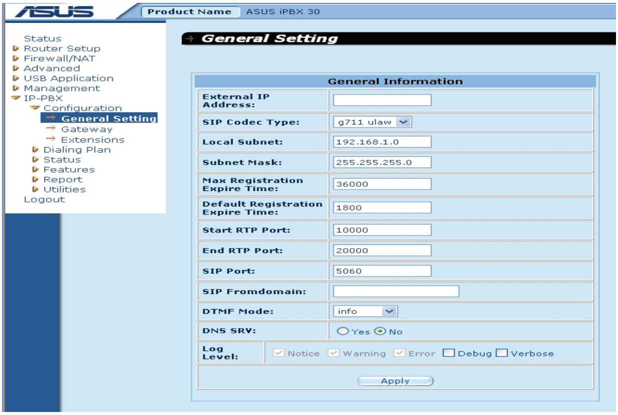
12.1 Configuration

A basic IP-PBX system should have three major components including IP-PBX server, user clients and gateway working together to provide necessary PBX functions. A user client can be an embedded hardware device such as ATA, IP phone or software IP phone running on PC, PDA. The following table shows their roles and configuration parameters required.

Table 12.1 Configuration Parameters

	IP_PBX server	User clients	Gateway
Function	1) Accept registration from user clients 2) Resolve IP address of destination client for call invitation. 3) Provide media service such as voice mail, IVR, DISA, etc.	1) Register to server 2) Make or terminate call via server 3) Voice codec and echo handling 4) Call function handling 5) 3-way conferencing	1) Register to server 2) Accept call from server to trunk port (FXO, FXS, or digital trunk T1/E1/DSDN) 3) Forward call from trunk to server 4) Voice codec and echo handling
Parameters required	1) WAN port IP 2) Gateway IP (if installed) 3) Extension number, ID, password table 4) Dialing plan for call routing 5) PBX related functions setting	1) WAN mode/IP 2) Server IP 3) Signaling/RTP port 4) User name, phone number, ID, password 5) Codec and parameters	1) Server IP, signal/RTP port 2) Dialing plan for routing prefix code remove/add 3) Codec and parameters 4) Signaling protocol

12.1.1 General Setting



General Setting

General Information	
External IP Address:	
SIP Codec Type:	g711 ulaw
Local Subnet:	192.168.1.0
Subnet Mask:	255.255.255.0
Max Registration Expire Time:	36000
Default Registration Expire Time:	1800
Start RTP Port:	10000
End RTP Port:	20000
SIP Port:	5060
SIP Fromdomain:	
DTMF Mode:	info
DNS SRV:	○ Yes ● No
Log Level:	☑ Notice ☑ Warning ☑ Error ☐ Debug ☐ Verbose

Figure 12.2 General setting page

In the web-based configuration software, the following items can be configured.

- **External IP address (Not configurable)**

  This IP address is the same with the WAN IP address. It shows the same IP if the iPBX30 WAN port. The SIP server uses this IP to distinguish the incoming VoIP call location by checking if it is from external WAN or local LAN.

- **SIP codec type**

  Choose one codec type for SIP server from G.711u/G.711a/ G.729A. The iPBX30 SIP server uses the selected codec to negotiate with the SIP client requesting for registration. The iPBX30 will request every client to use the same codec for compatibility.

- **Local subnet**

  This subnet value defines the SIP server LAN segment. For example, if you have assigned the LAN IP segment to 192.168.10.x, the value for this field is 192.168.10.0.

- **Subnet mask**

  SIP server uses this subnet mask to judge if the clients are registered in LAN environment. It can be a C-class or B-Class mask.

- **Max. registration expire time**

This value defines the maximum allowable expiry time for client registration. The SIP client notifies the server its registration expiry time when registration is in progress.

- **Default registration expire time**

The server uses this expiry time as default value if any client registered without expire time value attached.

- **Start RTP port/ End RTP port**

The user can assign the starting RTP port number and End RTP port number for VoIP service to define the iPBX30 VoIP RTP port usage range.

- **SIP port**

The 5060 port is commonly used for SIP call signaling. The user can change it if necessary.

- **DTMF mode**

Users can select one of the three available DTMF transmission methods: Inband, RFC2833, and Info.

Note: We recommend "Info" mode for normal use. SIP client and server side should use the same DTMF mode.

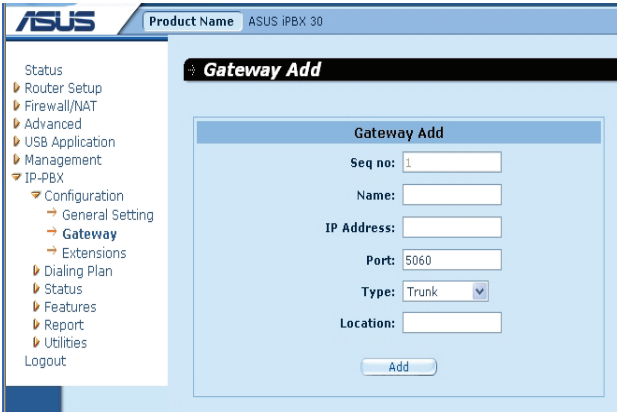
- **Log Level**

This option allows the user to determine how detailed the log message would be in the log file.

12.1.2 Gateway

The user can add an SIP gateway node for the iPBX30 IP-PBX server to provide inbound/outbound call capabilities from/to PSTN or PBX system.

Assign the IP-PBX server IP to the SIP gateway, and the gateway can forward PSTN incoming calls to the IP-PBX. Assign the gateway IP address to the IP-PBX, and the outgoing calls can be forwarded to the gateway.



Seq no: 1
Name:
IP Address:
Port: 5060
Type: Trunk
Location:

Figure 12.3 Gateway page

- **Seq. number (Not configurable)**

  This field is not configurable and for sequence identification purpose only. You may have more than one gateway in an IP-PBX system for different call routing with pre-defined dialing plans.

- **Name**

  This field is for management purpose only.

- **IP address**

  Define the proper IP address assigned for this gateway that iPBX30 can access to. The user can locate this SIP gateway in either LAN or WAN environment.

- **Port**

Defines the SIP port assigned for this gateway to communicate with.Use default 5060 port for SIP signaling. You can change SIP signaling port value, if necessary.

Note: The server and gateway should use the same port number.

- **Type**

This field allows the user to configure the service type that the gateway provides. Select the gateway to be connected to PSTN (Trunk) or PBX (Line) extension line, or both in a single gateway.

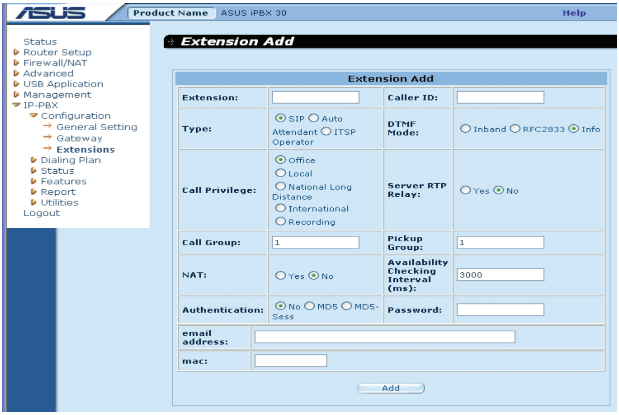
- **Location**

This field allows you to set the location for the gateway.

12.1.3 Extensions

You can add SIP user accounts in this page. The SIP extension accounts must be added before allowing extension client devices for registration. You may create up to 30 extensions. Some extensions can be used for registering to ITSP or other SIP servers.

Click **Extension** item to see the current extension list, and Click **Add** to create a new extension account for clients.



Extension Add

Extension:		Caller ID:	
Type:	● SIP ○ Auto Attendant ○ ITSP Operator	DTMF Mode:	○ Inband ○ RFC2833 ● Info
Call Privilege:	● Office ○ Local ○ National Long Distance ○ International ○ Recording	Server RTP Relay:	○ Yes ● No
Call Group:	1	Pickup Group:	1
NAT:	○ Yes ● No	Availability Checking Interval (ms):	3000
Authentication:	● No ○ MD5 ○ MD5-Sess	Password:	
email address:			
mac:			

Figure 12.4 Extension page

- **Extension**

  Assign an extension number for an SIP client to register. Extension number, the password and user ID are for authentication requirement when registering to SIP server.

- **Caller ID**

  Assign a caller ID, either in numeric or text characters, which will be sent to the called party when you are making a call.

- **Type**

  Select the service type for the extension. An extension can be selected as a standard SIP extension, auto attendant virtual extension, or ITSP registration account. To work with ITSP service, an extension must be created for both forwarding outbound call and accepting inbound call. The user has to do the other configuration for ITSP operation, such as IP address, port number assignment, ID and password setting. Refer to “Dialing plan” section for more details.

- **DTMF mode**

  Select the DTMF mode for this extension to work with the iPBX30 server. The available selections are: Inband, RFC2833 and info.

  Note: We recommend using “info” mode for most cases.

  The SIP client and the server should select the same DTMF mode to work properly.

  We do not recommend using ‘Inband' mode for iPBX30, although it is supported.

  If the SIP client enabled ‘Inband’ mode, it will send out DTMF tone to server and server has to process the tone and decide which DTMF code has received. Processing the DTMF tone needs very complex calculation. This makes iPBX30 CPU very busy and it will be incapable of processing many channels at the same time.

- **Call Privilege**

  For different extension users, you may want to control their outbound call authorization level, in other words, the rights to call local city call, long distance call, international call or only office call.

Note: Check the item "Recording" to assign this extension into greeting voice announcement recording function. The user can record voice message into the extension.

- **Server RTP relay**

This function allows the user to choose if the IP-PBX server should relay the RTP packets from this extension.

This function is useful when the extension client is located behind some special NAT device and unable to make a VoIP call successfully. The RTP packet relay will increase the loading of the server, but this is a good solution to penetrate NAT devices for VoIP client.

- **Call group**

This allows the user to assign a group number for identification when this extension makes a call to other parties. This will enable another extension to know the group number when it receives a call.

- **Pickup group**

Pickup grouping allows you to group the different extensions with the same working attribute into the same pickup group, so the group members can answer their colleague's phone call if they were temporary unavailable.

- **NAT**

You have to check this item with yes when the extension is located behind an NAT device, and uncheck this item if the extension is located at LAN environment.

- **Availability checking intervals (ms)**

Assign the time duration for IP-PBX server sending out an availability check request to the extension device. Server will change the extension available status to "Unreachable" if the extension has no response to this checking request, and mark the client status as on line if the device response in time.

- **Authentication**

  You can select the authentication algorithm for this extension when the extension device sends registration to server. Allowable algorithm is MD5, MD5-sess or none.

- **Password**

  Assign the authentication password here if you choose MD5, MD5-sess algorithm for extension registration.

- **Email address**

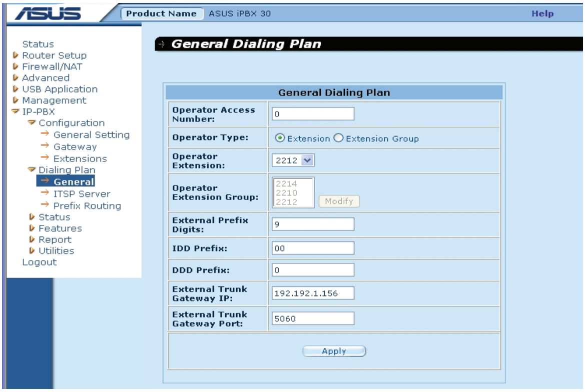
  When this extension has a voicemail, the server will send a email notification to this email address.

- **MAC**

  You can give the MAC address of the SIP client device (AX-112) for this extension number. It is for auto-provision function which AX-112 downloads the configuration file from iPBX30. iPBX30 will generate a configuration data file for each extension with the MAC address defined here.

12.2 Dialing Plan

12.2.1 General



General Dialing Plan

Operator Access Number:	0
Operator Type:	● Extension ○ Extension Group
Operator Extension:	2212
Operator Extension Group:	2214 2210 2212
External Prefix Digits:	9
IDD Prefix:	00
DDD Prefix:	0
External Trunk Gateway IP:	192.192.1.156
External Trunk Gateway Port:	5060

Figure 12.5 General Dialing Plan page

- **Operator access number**

  Assign the code for accessing operator, for example “0” or “9”, so the extensions can dial this access code to call the operator.

- **Operator type**

  Assign the operator type as a single extension or a group of extensions. If the operator type is “Group”, all the extensions defined in operator group rings when the operator code is dialed.

- **Operator extension**

  Assign a single extension number here as the operator.

- **Operator extension group**

  Select all the operator extension numbers if operator type is set as “Extension group”.

- **External prefix digits**

  Define the outbound call (call to PSTN) access prefix code. It is associated with “local” privilege in Extensions configuration page. Do duplicate with other access code that is already used.

- **IDD prefix**

  Define the “International Direct Dial” prefix code for call privilege control checking. It associated with “International” privilege in Extensions configuration page. When an extension is limited and not able to make international long distance call, the server will check the dialing number from extension with this IDD prefix, and the call will be denied if the prefix matched.

- **DDD prefix**

  Similar with above, this field allows user to define the “Domestic Direct Dial” prefix code for call privilege control checking. It is associated with “National Long Distance” privilege in Extensions configuration page.

- **External trunk gateway IP**

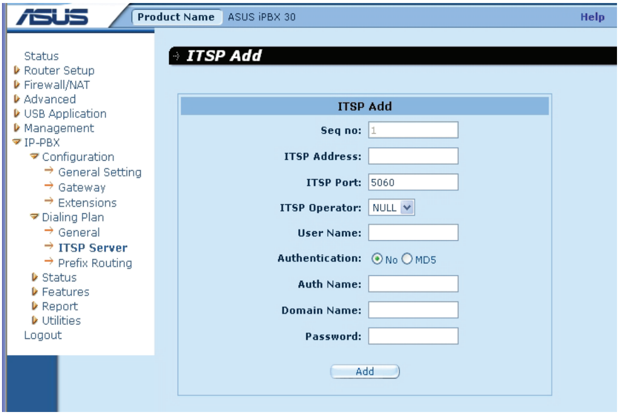
  Enter the gateway IP for IDD, DDD and outbound call access.

- **External trunk gateway port**

  Assign the port for the gateway.

12.2.2 ITSP Server

The iPBX30 allows you to link with Internet Telephony Service Provider (ITSP) providing SIP service. You must have a valid ITSP user account and password for iPBX30. To link the iPBX30 to ITSP account, register the iPBX30 to ITSP and assign an extension number with Auto attendant or ITSP Operator type as the ITSP inbound call operator.



ITSP Add

Seq no: 1
ITSP Address:
ITSP Port: 5060
ITSP Operator: NULL
User Name:
Authentication: ● No ○ MD5
Auth Name:
Domain Name:
Password:

Figure 12.6 ITSP Server page

- **Seq. no: (Not configurable)**

  The iPBX30 allows you to define more than one ITSP service account, and this field is used for sequence identification.

- **ITSP Address**

  Enter the ITSP server IP address or domain name here.

- **ITSP Port**

  Enter the ITSP server port number here. Port 5060 is usually for SIP.

- **ITSP Operator**

  Select one extension number as the ITSP inbound call reception operator. The extension must be predefined in the “Extension” page. All incoming calls from ITSP SIP will be forwarded to this extension.

- **User Name/Password**

  The ITSP will give you an account name and password for device registration authentication. Enter the account name here, followed by password and authentication method.

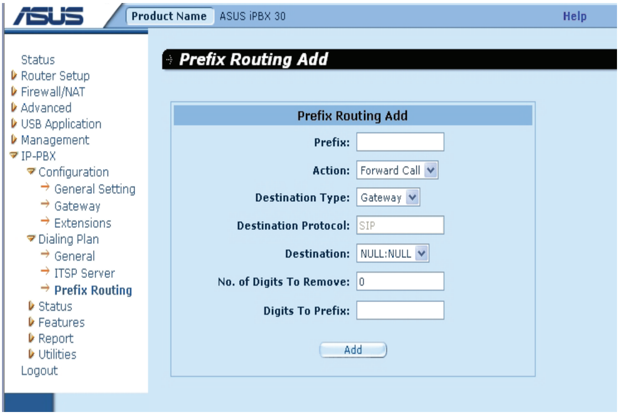
- **Authentication**

  The iPBX30 supports MD5 authentication method while registering to ITSP. Normally the SIP server registration is protected for preventing unauthorized user login.

12.2.3 Prefix Routing

“Prefix routing” enables user to define a prefix code mapping for routing calls to a specified destination.

The destination could be a gateway or ITSP service server. Prefix routing must work with “Gateway” or “ITSP” setting.



Prefix Routing Add

Prefix:

Action: Forward Call

Destination Type: Gateway

Destination Protocol: SIP

Destination: NULL:NULL

No. of Digits To Remove: 0

Digits To Prefix:

Figure 12.7 Prefix Routing page

- **Prefix**

  Enter the prefix code here to be matched with each user call attempt. If the digits from a call fail to be matched with any prefix digits defined in prefix routing, it will be treated as a local extension call.

- **Action**

  Select the action of a call if the prefix digits were matched. You can select to forward the call or block the call.

- **Destination type**

  Select the destination type, either a gateway or ITSP service.

- **Destination protocol**

  The iPBX30 supports SIP protocol .

- **Destination**

  Select the available destination gateway or ITSP from the pull down menu. The available gateways must be predefined in Gateway configuration page.

- **Digits to remove**

  The user can define the length of digits to be removed from a call before forwarding to a destination gateway or ITSP server. Prefix code removing is necessary because the ITSP will not recognize these codes and may cause call failure.

- **Digits to prefix**

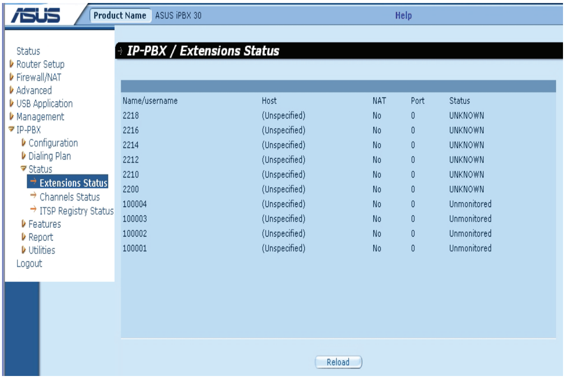
  The user can define the length of digits to be added to a call before forwarding to a destination gateway or ITSP server. Prefix code removing is only necessary when ITSP or gateway devices needed to parse your dialing rule.

12.3 Status

12.3.1 Extensions status

You can check all the extension client registration status in this page. This page automatically refreshes every 30 seconds. You can make call to the extension if it is indicated in “OK” status. .

You can also check the extension's IP address, port number and NAT setting here



IP-PBX / Extensions Status

Name/username	Host	NAT	Port	Status
2218	(Unspecified)	No	0	UNKNOWN
2216	(Unspecified)	No	0	UNKNOWN
2214	(Unspecified)	No	0	UNKNOWN
2212	(Unspecified)	No	0	UNKNOWN
2210	(Unspecified)	No	0	UNKNOWN
2200	(Unspecified)	No	0	UNKNOWN
100004	(Unspecified)	No	0	Unmonitored
100003	(Unspecified)	No	0	Unmonitored
100002	(Unspecified)	No	0	Unmonitored
100001	(Unspecified)	No	0	Unmonitored

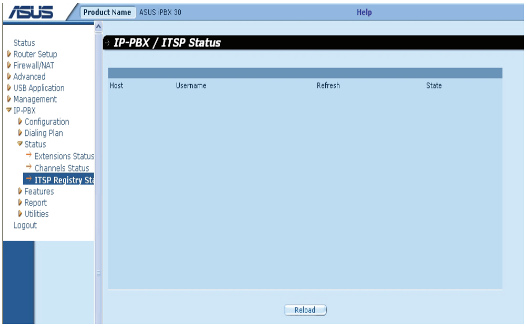
Figure 12.8 Extensions Status page

12.3.2 Channel status

You can check the extensions call status in this page, and this page is empty when there is no any extension making calls or ITSP/ gateway activities in progressing.

12.3.3 ITSP registry

If you have ITSP SIP account and it is properly setup, you can check the ITSP registration status here. The iPBX30 keeps trying to register to ITSP account until it is successful. The iPBX30 allows you to register to multiple ITSP accounts at the same time.



IP-PBX / ITSP Status

Host	Username	Refresh	State

Figure 12.9 ITSP Status page

12.4 Features

12.4.1 Voicemail

The iPBX30 supports voice mail feature, the caller party can leave a message to the called party when the call is not answered, and IPBX30 can send the user an e-mail notification when the voice message recording is done.

To enable mail notification function, the iPBX30 needs a mail sender account to send mail. You can set up the mail account and tag message here.

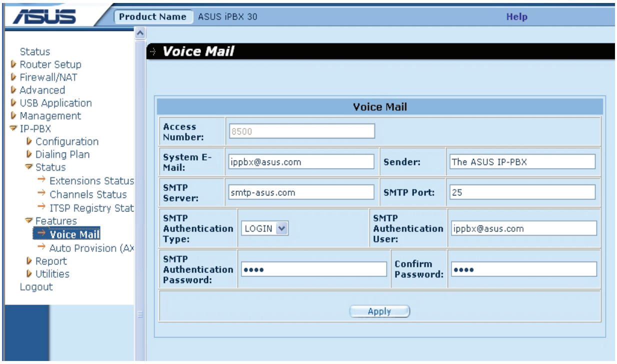
The iPBX30 voice mail message data are kept in on-board flash memory.

Voicemail is a centralized system of managing telephone messages for a large group of people. In its simplest form it mimics the functions of an answering machine. Voicemail systems are much more sophisticated than answering machines in that they can:

- Answer many phones at the same time
- Store incoming voice messages in personalized mailboxes associated with the user's phone number
- Enable users to forward received messages to another voice mailbox
- Store voice messages for future delivery
- Send email to notify the uset a message has arrived in the mailbox
- Transfer callers to another phone number for personal assistance

Voicemail messages are stored on hard disk drives or on board flash memory, media generally used by computers to store other forms of data. Messages are recorded in digitized natural human voice similar to how music is stored on a CD. You can call the system from any phone, logs on using DTMF codes (clearing security) to retrieve messages. Multiple users can retrieve or store messages at the same time on the same voicemail system.

There is 8Mbytes space for voice message as default and the recording time depends on the voice codec you selected. G.711 (uLaw, aLaw) is 8K bytes per second, and G.729 is 1K bytes per second. If you have attached the USB device onto iPBX30 USB port and setup the USB storage device for CDR and voice mail, then the voice message recording time is limited by the USB storage size.



Access Number: 8500
System E-Mail: ippbx@asus.com
Sender: The ASUS IP-PBX
SMTP Server: smtp-asus.com
SMTP Port: 25
SMTP Authentication Type: LOGIN
SMTP Authentication User: ippbx@asus.com
SMTP Authentication Password: ••••
Confirm Password: ••••

Figure 12.10 Voice mail page

- **Access Number**

  Defines the voicemail box function access number for extensions to dial. When the SIP extension receives the notification email, dial this number to enter the voicemail system to listen to the voice message.

- **System E-Mail**

  The iPBX30 email address to send out mail.

- **Sender**

  The data in this field is shown on the email “Sender” field.

- **SMTP Servers/SMTP Port**

  The iPBX30 uses this SMTP Server to send the email notification out.

- **SMTP Authentication Type**

  The iPBX30 supports two authentication types to mail server: LOGIN and PLAIN

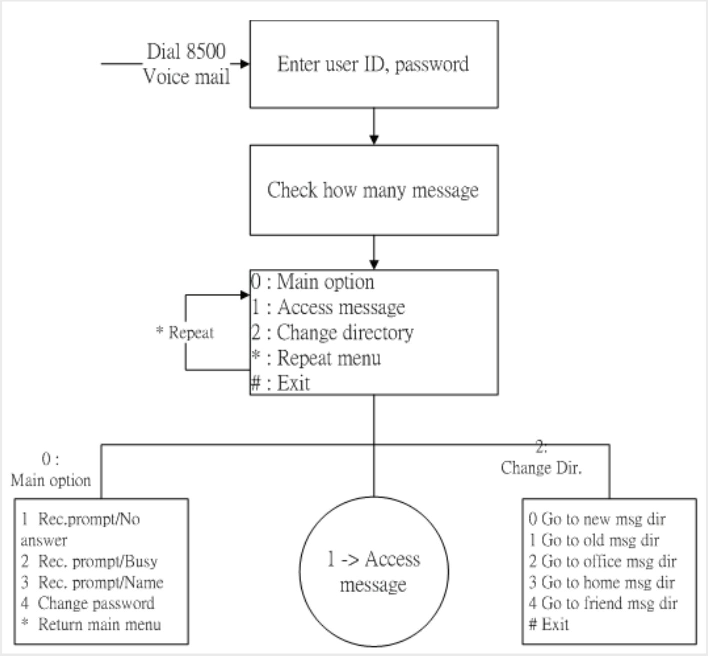
- **SMTP Authentication User/Password**

  The user name and password for SMTP server's authentication.

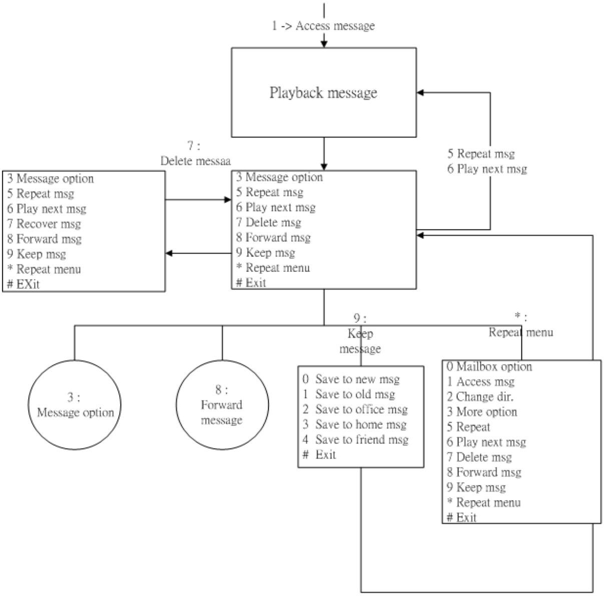
In the above configuration example, follow the instructions below to access your voice message:

1. Dial "8500" from your IP phone to enter iPBX30 voicemail box function main menu.
2. Enter the extension number and password to access your message after entering voicemail box.
3. The password is identical to the "registration password" which you set up in the "Extension" page. Refer to section 12.1.3 Extension.
4. Follow the voice prompt for more operation.

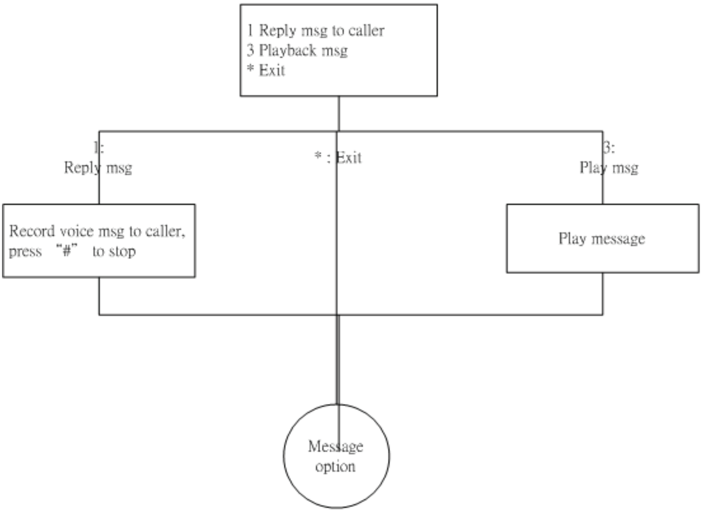
Voice mail function main menu flowchart:



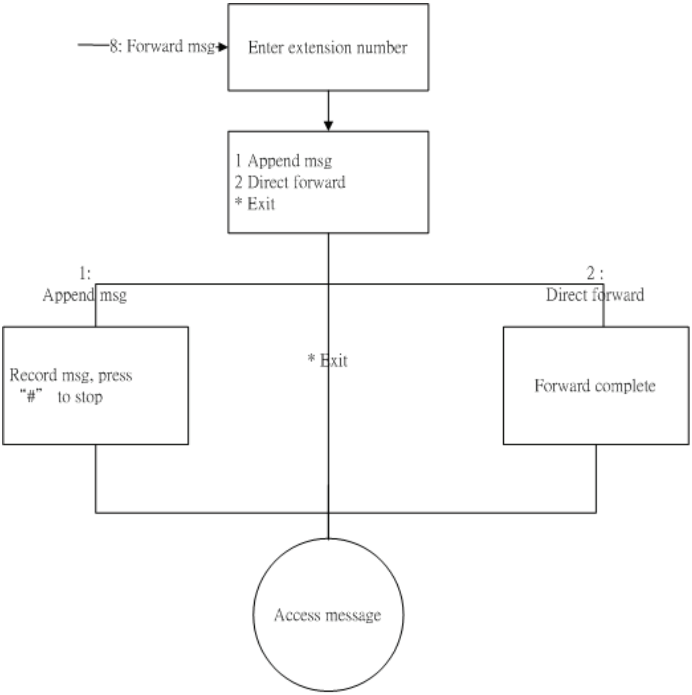
Press “1” to enter play back message menu,and refer to the following flowchart.



To enter message option menu, press “3” in the message option menu after message played. You can select to reply message to caller or repeat the message again.



To enter message forward menu, press “8” in the message option menu after message played. You can select to forward message directly to another extension or record a tag message and forward.

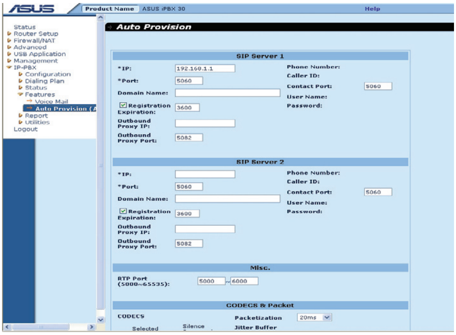


12.4.2 Auto-provision (for AX-112)

The iPBX30 supports auto provisioning function for ASUS SIP ATA whose model name is AX-112. Since there is no standard algorithm for provisioning, so it’s nature that iPBX30 only supports the device now. Autoprovision function allows system maintainer to define the configuration data for SIP client devices on iPBX30 server GUI. This function can minimize the deployment efforts of ATA, IP phone and increase the consistence and flexibility when replacing client devices.

The iPBX30 must have a copy of configuration data for client device so the client can download the configuration data when provisioning function is activated at client side. For this reason, the provision configuration of iPBX30 is basically the same with the GUI of AX-112.

The configuration data here will be saved into a file together with the MAC address defined in ‘Extensions’ configuration page.



Auto Provision

SIP Server 1

*IP: 192.168.1.1
*Port: 5060
Domain Name:
☑ Registration Expiration: 3600
Outbound Proxy IP:
Outbound Proxy Port: 5082
Phone Number:
Caller ID:
Contact Port: 5060
User Name:
Password:

SIP Server 2

*IP:
*Port: 5060
Domain Name:
☑ Registration Expiration: 3600
Outbound Proxy IP:
Outbound Proxy Port: 5082
Phone Number:
Caller ID:
Contact Port: 5060
User Name:
Password:

Misc.

RTP Port (5000~65535): 5000 ~ 6000

CODECS & Packet

CODECS
Selected
Silence
Packetization 20ms
Jitter Buffer

Figure 12.11 Auto Provision page

12.5 Report

- **CDR (Call Detail Record) Report**

  You can check the call log in this page which includes information of caller party, called party and call duration. But these call log are default recorded in SDRAM memory and will be lost when the system powers off. The log can be recorded to an external USB storage device if user has attached the USB device onto iPBX30 USB port. If an USB storage device has been configured for CDR and voice mail, then the records data will not be lost when iPBX30 is powered off.

12.6 Utilities

12.6.1 Hot reload

Every time you make changes on the IP-PBX settings, you have to tell the IP-PBX server to “reload” the new configuration and activate. Click the confirm button and the reload process will begin, taking about 10 seconds to load the new configuration.

12.6.2 Service restart

If you need to restart the IP-PBX server software, click this item and confirm. The iPBX30 will kill the old IP-PBX program task to restart it again. Your request for IP-PBX service restart won't affect the NAT function of iPBX30.

12.7 Configuring Examples

The diagram below shows a typical iPBX application scenario, and the iPBX30 plays the role of router and SIP server at the same time. Following sections describe how to setup 2 ATA in LAN, 1 ATA in internet and 1 SIP gateway in LAN. We have to give some assumption for these scenarios:

- iPBX30 WAN public IP: 210.80.66.110
- DHCP server is enabled for iPBX30 LAN, and LAN IP segment is 192.192.1.x
- Two AX-112 ATA in LAN with extension number 1001/1002, and the AX-112 WAN is in DHCP client mode, this means AX-112 will get IP from iPBX30 built-in DHCP server.
- One AX-112 ATA in Internet with extension number 1003, and its WAN IP is 192.168.10.10 which is obtained from the home router.
- One SIP gateway connected to PSTN lines with LAN IP:192.192.1.10.

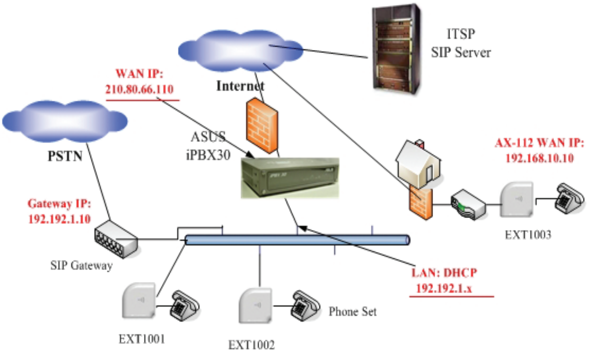
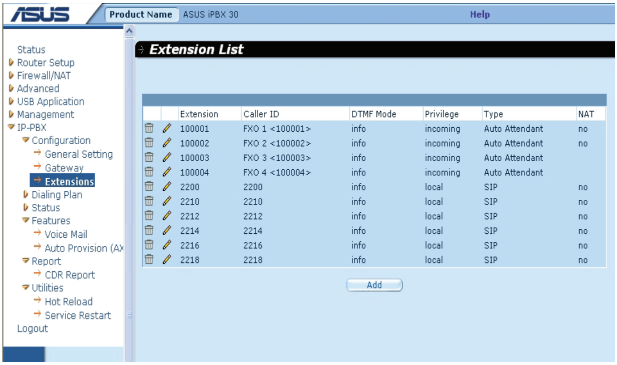


Figure 12.12 Typical iPBX30 application set up

Create extensions

You have to create extension accounts in iPBX30 for the registration from three SIP ATA devices.

Click **IP-PBX -> Configuration -> Extensions** to open the page as shown below.

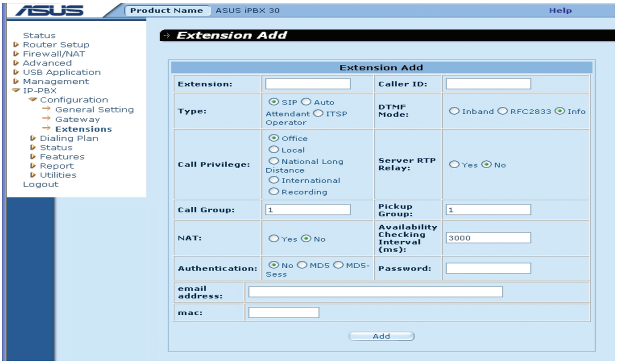


Extension List

Extension	Caller ID	DTMF Mode	Privilege	Type	NAT
100001	FXO 1 <100001>	info	incoming	Auto Attendant	no
100002	FXO 2 <100002>	info	incoming	Auto Attendant	no
100003	FXO 3 <100003>	info	incoming	Auto Attendant	
100004	FXO 4 <100004>	info	incoming	Auto Attendant	
2200	2200	info	local	SIP	no
2210	2210	info	local	SIP	no
2212	2212	info	local	SIP	no
2214	2214	info	local	SIP	no
2216	2216	info	local	SIP	no
2218	2218	info	local	SIP	no

Figure 12.13 Extension List page

Click the **Add** button to open the extension configuration page.



Extension Add

Extension:		Caller ID:	
Type:	● SIP ○ Auto Attendant ○ ITSP Operator	DTMF Mode:	○ Inband ○ RFC2833 ● Info
Call Privilege:	● Office ○ Local ○ National Long Distance ○ International ○ Recording	Server RTP Relay:	○ Yes ● No
Call Group:	1	Pickup Group:	1
NAT:	○ Yes ● No	Availability Checking Interval (ms):	3000
Authentication:	● No ○ MD5 ○ MD5-Sess	Password:	
email address:			
mac:			

Figure 12.14 Extension page

We recommend you set up parameters for extension 1001 as following:

1. Set “Extension”, “Caller ID”, “Password” to “1001”.
2. Check “Type” as “SIP”, “DTMF mode” as “Info”

3. Check server RTP relay as “No”, “NAT:” as “No”

4. Click “Add” to complete this configuration.

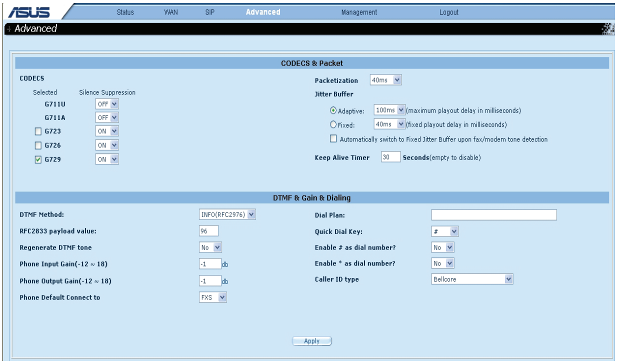
5. Follow the instructions above to set up extension “1002”.

6. For AX-112 user under NAT device over internet (extension 1003), all settings are the same except that you should check the “NAT:” field as “Yes”.

7. After all setting are completed, click “Utility” item from the left side menu , and click “Hot reload” to make iPBX30 reload all the settings and take effective.

Configure the SIP client devices

After you have created these AX-112 accounts, you have to setup proper parameters for each AX-112 account.



CODECS & Packet

CODECS

Selected	Silence Suppression
G711U	OFF
G711A	OFF
☐ G723	ON
☐ G726	ON
☑ G729	ON

Packetization 40ms

Jitter Buffer

● Adaptive: 100ms (maximum playout delay in milliseconds)

○ Fixed: 40ms (fixed playout delay in milliseconds)

☐ Automatically switch to Fixed Jitter Buffer upon fax/modem tone detection

Keep Alive Timer 30 **Seconds**(empty to disable)

DTMF & Gain & Dialing

DTMF Method:	INFO(RFC2976)	Dial Plan:	
RFC2833 payload value:	96	Quick Dial Key:	#
Regenerate DTMF tone	No	Enable # as dial number?	No
Phone Input Gain(-12 ~ 18)	-1 db	Enable * as dial number?	No
Phone Output Gain(-12 ~ 18)	-1 db	Caller ID type	Bellcore
Phone Default Connect to	FXS		

Figure 12.15 SIP page

To configure the SIP client devices:

1. Connect AX-112 to iPBX30 using RJ45 cable, connect an analog phone set to AX-112 using RJ11 cable, and power on AX-112.

2. Pick up the phone and dial “****” to hear AX-112 IVR (Interactive Voice Response) menu.

3. Dial “100#” and AX-112 reports you the device status. Listen carefully for WAN IP reporting and open a browser with this IP.

4. Enter AX-112 GUI and click “SIP” on the above menu. Enter iPBX30 LAN IP (192.168.1.1 as assumed) in “*IP” field. Enter

the Phone number, Caller ID, User Name and Password, and make sure they are identical to the settings in iPBX30. Click **Apply** after completing all settings.

5. Click “Advanced” on the menu to configure advanced setting:
   a. Choose “Silence Suppression” as “Off” for G.729 and G.711.
   b. Choose “INFO” mode for “DTMF method”
   c. Click “Apply” to update setting and then reboot AX-112.
6. Now your AX-112 with extension number 1001 can login iPBX30 and make a call.
7. Follow the above procedures to configure extension 1002
8. For AX-112 under NAT device over Internet, only the “*IP:” (SIP server IP address) setting is different. Assign the public IP of iPBX30 to this field (it is 210.80.66.110 in this example).

Enable the ITSP service

There are 3 steps to enable ITSP service.

- **Create an extension for ITSP**

  It is necessary for iPBX30 to use an extension as an UA (User Agent) to register to ITSP SIP server, and also to accept the incoming call from ITSP. Select an extension number for ITSP registration and click the type as “ITSP operator”.

- **Set up ITSP account**

  Enter the ITSP server public IP address or domain name, and the proper user name and password for authentication. You can have multiple gateways or ITSP service accounts at the same time.

- **Add a routing rule for ITSP service**

  You have to create a routing rule for ITSP call, just like the gateway prefix routing setup.

  After you have finished all the setup, go to **IP-PBX -> Utilities** and click the “Hot Reload” to make all the settings effective. Go to **IP-PBX -> Status** to check if the ITSP registration is successful, and make a call with proper prefix number to check if the call can be routed to gateway or ITSP server accordingly.

13 IP Addresses, Network Masks, and Subnets

13.1 IP Addresses

Note: This section pertains only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered.

This section assumes basic knowledge of binary numbers, bits, and bytes.

IP addresses, the Internet's version of telephone numbers, are used to identify individual nodes (computers or devices) on the Internet. Every IP address contains four numbers, each from 0 to 255 and separated by dots (periods), e.g. 20.56.0.211. These numbers are called, from left to right, field1, field2, field3, and field4.

This style of writing IP addresses as decimal numbers separated by dots is called dotted decimal notation. The IP address 20.56.0.211 is read "twenty dot fifty-six dot zero dot two-eleven."

13.1.1 Structure of an IP address

IP addresses have a hierarchical design similar to that of telephone numbers. For example, a 7-digit telephone number starts with a 3-digit prefix that identifies a group of thousands of telephone lines, and ends with four digits that identify one specific line in that group.

Similarly, IP addresses contain two kinds of information.

- Network ID

  Identifies a particular network within the Internet or Intranet

- Host ID

  Identifies a particular computer or device on the network

The first part of every IP address contains the network ID, and the rest of the address contains the host ID. The length of the network ID depends on the network's class (see following section). The table below shows the structure of an IP address.

Table 13.1. IP Address Structure

	Field 1	**Field 2**	**Field 3**	**Field 4**
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

Here are some examples of valid IP addresses:

Class A: 10.30.6.125 (network = 10, host = 30.6.125)

Class B: 129.88.16.49 (network = 129.88, host = 16.49)

Class C: 192.60.201.11 (network = 192.60.201, host = 11)

13.2 Network classes

The three commonly used network classes are A, B, and C. (There is also a class D but it has a special use beyond the scope of this discussion.) These classes have different uses and characteristics.

Class A networks are the Internet's largest networks, each with room for over 16 million hosts. Up to 126 of these huge networks can exist, for a total of over 2 billion hosts. Because of their huge size, these networks are used for WANs and by organizations at the infrastructure level of the Internet, such as your ISP.

Class B networks are smaller but still quite large, each able to hold over 65,000 hosts. There can be up to 16,384 class B networks in existence. A class B network might be appropriate for a large organization such as a business or government agency.

Class C networks are the smallest, only able to hold 254 hosts at most, but the total possible number of class C networks exceeds 2 million (2,097,152 to be exact). LANs connected to the Internet are usually class C networks.

Some important notes regarding IP addresses:

The class can be determined easily from field1:

field1 = 1-126: Class A

field1 = 128-191: Class B

field1 = 192-223: Class C

(field1 values not shown are reserved for special uses)

- A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

13.3 Subnet masks

Definition: mask: A mask looks like a regular IP address, but contains a pattern of bits that tells what parts of an IP address are the network ID and what parts are the host ID: bits set to 1 mean "this bit is part of the network ID" and bits set to 0 mean "this bit is part of the host ID."

Subnet masks are used to define subnets (what you get after dividing a network into smaller pieces). A subnet's network ID is created by "borrowing" one or more bits from the host ID portion of the address. The subnet mask identifies these host ID bits.

For example, consider a class C network 192.168.1. To split this into two subnets, you would use the subnet mask:

255.255.255.128

It's easier to see what's happening if we write this in binary:

11111111. 11111111. 11111111.10000000

As with any class C address, all of the bits in field1 through field 3 are part of the network ID, but note how the mask specifies that the first bit in field 4 is also included. Since this extra bit has only two values (0 and 1), this means there are two subnets. Each subnet uses the remaining 7 bits in field4 for its host IDs, which range from 0 to 127 (instead of the usual 0 to 255 for a class C address).

Similarly, to split a class C network into four subnets, the mask is:

255.255.255.192 or 11111111. 11111111. 11111111.11000000

The two extra bits in field4 can have four values (00, 01, 10, 11), so there are four subnets. Each subnet uses the remaining six bits in field4 for its host IDs, ranging from 0 to 63.

Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets. Such a mask is called a default subnet mask. These masks are:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

These are called default because they are used when a network is initially configured, at which time it has no subnets.

14 Troubleshooting

This appendix suggests solutions for problems you may encounter in installing or using the IPBX30, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

Table 14.1: Problems & suggested actions

Problem	Suggested Action
LEDs	
Power LED does not light up after product is turned on.	Verify that you are using the AC adapter provided with the device and that it is securely connected to the iPBX30 and a wall socket/power strip.
LINK WAN LED does not light up after Ethernet cable is attached.	Verify that an Ethernet cable like the one provided is securely connected to the Ethernet port of your ADSL or cable modem and the WAN port of the iPBX30. Make sure that your ADSL or cable modem is powered on. Wait 30 seconds to allow the iPBX30 to negotiate a connection with your broadband modem.
LINK LAN LED does not light up after Ethernet cable is attached.	Verify that the Ethernet cable is securely connected to your LAN hub or PC and to the iPBX30. Make sure the PC and/or hub is turned on. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (100BaseTx) should use cables labeled Cat 5. 10Mbit/sec cables may tolerate lower quality cables.

Internet Access	
PC cannot access the Internet	Use the ping utility, discussed in the following section, to check whether your PC can communicate with the iPBX30's LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. If you statically assigned a private IP address to the computer, (not a registered public address), verify the following: • Check that the gateway IP address on the computer is your public IP address (see section 3.2 for instructions on viewing the IP information.) If it is not, correct the address or configure the PC to receive IP information automatically. • Verify with your ISP that the DNS server specified for the PC is valid. Correct the address or configure the PC to receive this information automatically. • Verify that a Network Address Translation rule has been defined on the IPBX30 to translate the private address to your public IP address. The assigned IP address must be within the range specified in the NAT rules. Or, configure the PC to accept an address assigned by another device (see section 3.2 "Part 2 — Configuring Your Computers"). The default configuration includes a NAT rule for all dynamically assigned addresses within a predefined pool.
PC cannot display web pages on the Internet.	Verify that the DNS server specified on the PC is correct for your ISP, as discussed in the item above. You can use the ping utility, discussed in the following section, to test connectivity with your ISP's DNS server.

Web UI Management Program	
You forgot/lost your Web UI Management user ID or password.	If you have not changed the password from the default, try using “admin” as the user ID and “admin” for the password. Otherwise, you can reset the device to the default configuration by following the instructions provided in section 10.7.1 “Restore System Configuration”. **WARNING**: Resetting the device removes any custom settings and returns all settings to their default values.
Cannot access the Web UI Management program from your browser.	Use the ping utility, discussed in the following section, to check whether your PC can communicate with the iPBX30’s LAN IP address (by default 192.168.1.1). If it cannot, check the Ethernet cabling. Verify that you are using Internet Explorer 6.0 or newer. Support for Javascript® must be enabled in your browser. Support for Java® may also be required. Verify that the PC IP address is defined as being on the same subnet as the IP address assigned to the LAN port on the iPBX30.
Changes to Web UI Management are not being retained.	Be sure to click the **Apply** button to save any changes.

14.1 Diagnosing Problems using IP Utilities

14.1.1 ping

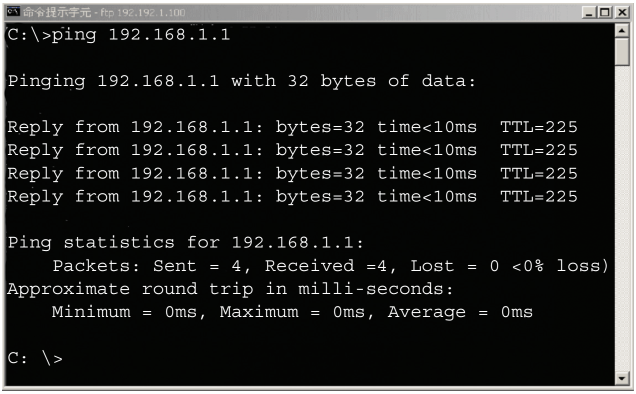
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer with which you are trying to communicate.

On Windows-based computers, you can execute a ping command from the Start menu. Click the Start button,

and then click Run. In the Open text box, type a statement such as the following:

ping 192.168.1.1

Click the **OK** button. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.



```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms  TTL=225
Reply from 192.168.1.1: bytes=32 time<10ms  TTL=225
Reply from 192.168.1.1: bytes=32 time<10ms  TTL=225
Reply from 192.168.1.1: bytes=32 time<10ms  TTL=225

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received =4, Lost = 0 <0% loss)
Approximate round trip in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C: \>
```

Figure 14.1. Using the ping utility

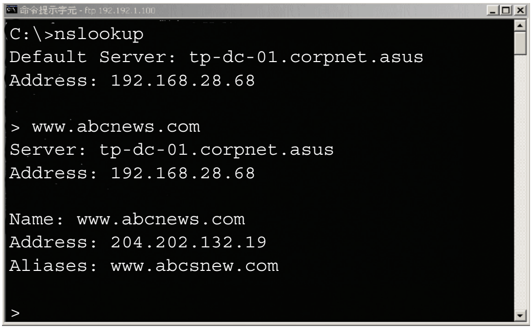
If the target computer cannot be located, you will receive the message “Request timed out.”

Using the ping command, you can test whether the path to the iPBX30 is working (using the preconfigured default LAN IP address 192.168.1.1) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for www.yahoo.com (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the nslookup command, as explained in the following section.

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

14.1.2 nslookup



```
C:\>nslookup
Default Server: tp-dc-01.corpnet.asus
Address: 192.168.28.68

> www.abcnews.com
Server: tp-dc-01.corpnet.asus
Address: 192.168.28.68

Name: www.abcnews.com
Address: 204.202.132.19
Aliases: www.abcsnew.com

>
```

Figure 14.2. Using the nslookup utility

You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the nslookup command from the Start menu. Click the **Start -> Run**. In the Open text box, type the following:

nslookup

Click the **OK** button. A Command Prompt window displays with a bracket prompt (>). At the prompt, type the name of the Internet address you are interested in, such as www.absnews.com.

The window will display the associate IP address, if known.

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

To exit from the nslookup utility, type **exit** and press <**Enter**> at the command prompt.

15 Index