IPNext190

[System Installation Guide]

AddPac Technology Co., Ltd.
www.addpac.com

IPNext190

Note:

The specification and information in this document are subject to change without notice. All statements, information, and recommendations in this document are believed to be accurate but are presented without warranty of any kind, express or implied. In no event shall AddPac or its suppliers disclaim all warranties, expressed or implied, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual. For detail specification, information or sales and warranty, please contact Technical Sales division of AddPac.

[CONTENTS]

[FIGURES]

[TABLES]

If you have any questions regarding AP-VP200 or your product has any failures, please contact AddPac Technology Co., Ltd.

AddPac Technology Co., Ltd.
Floor Nos. 2/3/5, Jeong Am Bldg., 769-12, Yoksam-dong, Kangnam-ku, Seoul
Phone (02) 568-3848 (Rep.)
Facsimile (02) 568-3847
E-mail Address: info@addpac.com
http://www.addpac.com

The revision history of the IPNext PBX Installation and Operation Manual is listed in the followings:

Version	Date	Revision Action	Prepared by
Version 1.00	August 25, 2008	Initial Released	R&D, AddPac Technology

Chapter 1.   Introduction

Overview

IPNext190 is a next-generation IP Keyphone System and a new IP telephony solution for all IP environments. IPNext190 inter-works with various IP terminals of AddPac (e.g. AP-VP300, AP-VP250, AP-VP200, AP-VP150, AP-VP120 IP Video Phone, and AP-IP300, AP-IP150, AP-IP100 IP Phone) and analog phones(low cost compared with IP terminals, also reused) to provide multimedia IP telephony services as well as the traditional voice-based PBX features. This product is based on the advanced embedded RISC that enables firmware upgrade, and can be equipped with various VoIP interfaces (FXS, FXO, etc) depending on module options. IPNext190 is suitable for small and medium size companies, and inter-works with the VoIP and video products of AddPac Technology to provide a variety of IP application services appropriate for your network. Also, IPNext190 supports H.323 VoIP inter-working as well as SIP protocol for outbound call.

Features

1) Next Generation IP Keyphone System

The front panel of IPNext190 IP Keyphone System supports LED displays of device status and has two(2) 10/100 Mbps Fast Ethernet ports, the RS-232C console port for Command Line Interface (CLI), Power Inlet and Power ON/OFF Switch. Its rear panel supports various VoIP interfaces such as FXO, FXS depending on module options. IPNext190 can support maximum 32 port VoIP interface (4 slots x 8Port VoIP Module). The call scenarios supported by IPNext190 provide SIP-based basic calls, color ring services, music on hold, blind transfer, call pickup, group call pickup, consult calls, switching calls, consult transfer, call waiting, call waiting notification, call park, call pickup remote, and hunt group. This product is designed to provide application services that require much memory such as voice mail using internal memory.

2) RTP Proxy Service Features for Private IP and IPv6 Address

Since the enterprise network environments configured with a Call Manager like as IP keyphone system and IP terminals require larger number IP address, either IPv6 or a private IP address in the NAT environment must be supported to the enterprise networks due to the deficient resources of a public IP

address. In such a private IP address environment, the RTP proxy feature is required for reliable multimedia communications between endpoint terminals. The RTP proxy feature of IPNext190 is used to make a communication between a private IP terminal and a public IP terminal among endpoint terminals such as IP phones, make a communication between a private IP terminal and a public IP terminal in the NAT environment, make a communication between private IP terminals, make audio/video broadcasting in private and public IP environments, and to enable audio/video conference calls in private and public IP environments. The RTP proxy feature can operate regardless of VoIP signaling protocols such as H.323 and SIP, and supports dual address systems such as IP version 4 and IP version 6 addresses.

3) User Presence Service for Unified Communication

For enterprise with small number of employee, IPNext190 IP keyphone system supports the user presence server function beside call manager function. But, in case of large enterprise, external User Presence Server should be used with IP-PBX due to performance issue independently. In order to support user presence features on real-time basis, such as user busy, on-line, user away, etc, user presence service function should be provided on IP telephony solution. User presence service function in a Call Manager gathers user information (on-line, busy, etc) of each IP terminals, and broadcasts user information to all or group IP terminals with speed-dial keys (built-in presence indication lamp) , AP-PT100 User Presence dedicate terminal, Smart Messenger Program at every second.

4) Intelligent IVR Features

One of the most important IP telephony service features is either ARS or IVR. Different IVR features are required by regular companies, government offices, and call centers respectively. IPNext190 IP Keyphone System provides an IVR tool to meet your requirements. Also, this solution provides an IVR scenario editor to allow you to make and enable a desired call scenario.

5) Built-in Network based Media Service

AddPac Technology's IPNext190 supports network-based media service. Together with IP terminals, Video Terminals and VoIP gateways, IPNext190 supports various media service like as Announcement, Ring Back Tone Service, and Music on Hold.
The media service of IPNext190 provides Ring Back Tone and Music on Hold either individually or by group. Ring Back Tone and Music on Hold files can be changed by Schedule. The media service has been designed to support the video codec of MPEG-4 basically, the services of multimedia Ring Back Tone and multimedia CID (MCID)*.

6) Unified Messaging Service

IPNext190 supports network based unified messaging service like as IP phone voice mailing service, E-mail notification, and web based Mailbox browsing service, etc. Basically, this service supports SIP

VoIP signaling and IVR scenario managing tool for voice/video message recording/retrieval. Using VXML based IVR scenario editor software (AddPac Technology provided), user can make new IVR scenario and edit the pre-existed IVR scenario for new service addition, service modification, etc. IPNext190 supports memory (NAND Flash Memory, etc) Quota functions for each user's voice/video mailbox, etc and e-mail notification function via internet. On business travel, user can monitor IP phone or video phone's leaving message in office via internet e-mail check and using MS window media player software. Also, user can play voice/video message under various environments such as PSTN phone via VoIP gateway, E-mail, Web, Smart Messenger (AddPac) in addition to IP terminals (IP phone, IP video phone).

7) Firmware Upgradable System

Since the high-performance RISC CPU of IPNext190 is programmable, the service features of IPNext190 can continue to be improved, changed, or added. If you download an added or changed feature from the home page directly or set an automatic upgrade option whenever feature addition or change is done, you can use the latest features without further operations.

8) Reliable IP-PBX Solution with Outstanding Network Service Capability

IPNext190 is an integrated network device that supports routing services, NAT/PAT, DHCP Server/Relay, and Quality of Service (QoS). If you want to adapt to a variety of network environments such as Metro Ethernet, Metro ATM, dedicated lines, flexible IP environments, and high-speed private subscriber networks such as xDSL, cable networks, and FTTH, advanced QoS and security features in addition to multiple network services should be supported. In this regard, IPNext190 supports two 10/100 Mbps Fast Ethernet interfaces. Based on this feature, IPNext 190 supports advanced LAN-to-LAN routing and bridge services as well as various network and security services such as NAT/PAT. IPNext190 IP keyphone system is a reliable solution built by using excellent technologies.

9) Now more worries for keeping Privacy

'Standard & Extended IP Access List' of the IPNext190 supports beyond the network security, but also service security. IPNext190 can support VPN, Secure RTP to secure data, voice and video, as to collaborate with the AddPac IP terminals.

10) AddPac IP-PBX Total Solution

AddPac Technology is not just another vendor of IP-PBX, but provides various product families appropriate for your network environment. To meet your needs, AddPac supports VoIP and media gateways, audio/video terminals, audio/video MCU, IP audio/video broadcast, VoD solutions, network DVR solution, audio/video recording solutions, and traffic controller QoS device solutions. In the

future all IP-based multimedia telephony environment, various audio/video resources should be shared on an IP network; thus, the integration of the entire solution and that of solutions for each area are very important. AddPac IP-PBX is designed considering the integrated multimedia solution, and can meet your various needs.

The performance and reliability of AddPac VoIP gateway series and multimedia network devices have been recognized in global markets. IPNext190, which is a collection of experiences and know-how accumulated in the enterprise and service provider markets, would meet the needs of customers who ask for a next-generation IP-PBX solution.

Main Features

High Performance RISC Microprocessor

Four (4) VoIP Module Slots for FXS, FXO, Digital E1

Network Interface: 2-port 10/100 Mbps Fast Ethernet interface

1-port RS-232C serial console interface

User Terminals : AP-VP500, AP-VP300, AP-VP250, AP-VP150, AP-VP120, AP-IP300, AP-IP150, AP-IP100, Smart Messenger

	AP-VP500	AP-VP500 Video Phone High Performance & Powerful Communication Method
	AP-VP300	AP-VP300 Video Phone High Performance & Powerful Communication Method
	AP-VP250	AP-VP250 Video Phone High Performance & Powerful Communication Method
	AP-VP150	AP-VP150 Video Phone High Performance & Powerful Communication Method
	AP-VP120	AP-VP120 Video Phone High Performance & Powerful Communication Method

AP-IP300	AP-IP300 IP Phone High Performance & Powerful Communication Solution

AP-IP150	AP-IP150 IP Phone High Performance & Powerful Communication Solution

AP-IP100	AP-IP100 IP Phone High Performance & Powerful Communication Solution

High Performance RISC Microprocessor

IP Key Phone: Various call scenarios, color ring service, and music on hold, etc.

SIP, H.323 Signaling

Scenario editor for IVR services and supporting tools.

Voice Mail and Unified Messaging Service

Voice Media Service: Announcement, Ring Back Tone, Music on Hold

3-Party Voice Conferencing (optional: DSP-based hardware voice MCU module)

Media Gateway for PSTN Interface (the interface for PSTN line and analog phone)

Fault tolerant and Scalability

Table 1-1 IPNext190: Collaborative Features

Service Feature	Description of Service Feature	Required Devices for Connection
IP Key Phone Features	● Basic SIP-based call features and call transfer, call pickup and various call scenarios ● Coloring Service. ● Music on Hold. ● 3-Party Audio-Conferencing ● Voice Mail, IVR	● AP-VP300:Video Phone (Advanced Model) ● AP-VP150: Video Phone (Distribution Model) ● AP-IP300 IP Phone (Advanced Model) ● AP-IP150 IP Phone (Distribution Model) ● AP-IP100 IP Phone (Distribution Model) ● Smart Messenger
PSTN Line Interface	E1, FXO interface with VoIP Gateway functionality for the incoming PSTN call	● AddPac AP-N1-FXO8 8-Port PSTN Interface Module (optional) ● AddPac AP-N1-E1T1 Digital E1/T1 PSTN Interface Module (optional)
PSTN Phone Interface	FXS Interface with VoIP Gateway functionality for connection with analog phone	● AddPac AP-N1-FXS8 8-Port FXS Analog Interface Module

System Architecture
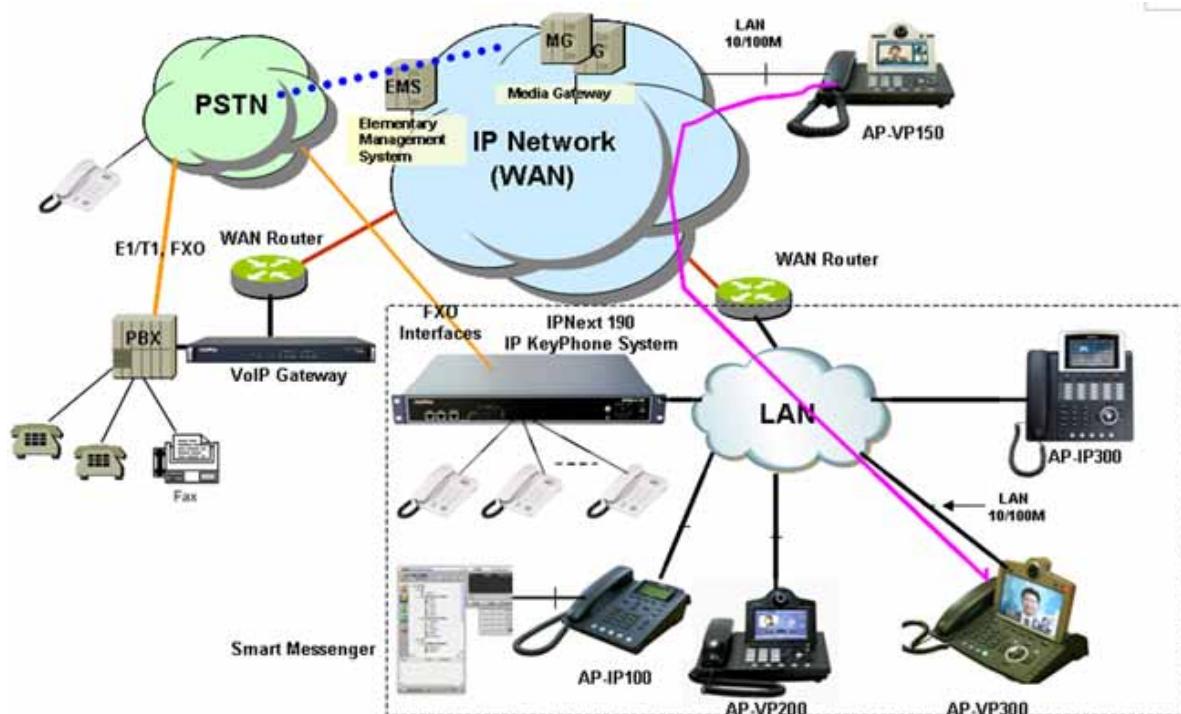
Figure 1-1 Network Diagram for the System Architecture of IPNext190

Hardware Features

Table 1-2 IPNext190 Hardware Specifications

Category	Specification	
Microprocessor	CPU	High Performance RISC Integrated Host Processor
Memory	Flash Memory	2Gbyte
	Main Memory	128Mbyte
	Boot Memory	512Kbyte Flash Memory
Fixed Network Interface	Fixed LAN0 Port	One(1) 10/100Mbps Fast Ethernet
	Fixed LAN1 Port	One(1) 10/100Mbps Fast Ethernet
	Console Port	One(1) RS-232C Interface for CLI
Voice Interface Module	AP-N1-FXS8	8-Port FXS Voice Interface Module (8 x RJ11)
	AP-N1-FXO8	8-Port FXO Voice Interface Module (8 x RJ11)
	AP-N1-FXS4O4	4-FXO & 4-FXS Voice Interface Module (8 x RJ11)
	AP-N1-E1/T1	1-Port PBX Digital E1/T1 Module (1 x RJ45)
Power Requirement	Power VAC 110~220 VAC, 50/60Hz, 40 Watt	
Operating Temperature	0°C ~ + 50°C (32° to 122°F)	
Storage Temperatures	-40°C ~ +85°C (-40° to 176°F)	
Relative Humidity	5% ~ 95% (Non-condensing)	
Dimensions	55 x 340 x 267(mm) - 19" Rack Mountable Chassis	
Weight	2.5Kg	

Software Feature

Table 1-3 IPNext190 Software Specifications

Category	Specification
Number & Call Routing	Trunk Hunting by Preference or Sequential
	Calling Hunting by Preference, Simultaneous, Random
	Calling Hunting by Chained Hunting Group
	Partition for Address Grading
	Call Class for Call Access Control
	Number Translation Rule for Inbound/Outbound Call
	Centrex with Prefix Support
	Multiple Shared Devices with One Number
	Multiple Numbers on One Device
	Individual Call Park within Park Number Pool
	Group Call Park within a Group or Other Group
	Call Pickup of Ringing Call of Same Group or Other Group
	Call Pickup of Parked Call
	Call Transfer- Blind, Consult
	Call Forwarding – Unconditional, Busy, No Answer, Voice Mail
	Call Waiting
	Call Swapping
	Call Hold
Advanced Features with AddPac IP phone, Video Phone, etc	Multiple Call Handling with Call Status and Calling Line Number and Name
	Plug and Play with Auto Discovery Function
	Softkey Map Download and Control
Telephony and Service & Features	Voice Mail List View
	Parked Call List View
	Call Forwarding Setting
	Recent Call List View
	Calling Number and Name Identification
	Individual Call Park within a Group or Other Group by Softkey
	Group Call Park within a Group or Other Group by Softkey
	Call Pickup of Ringing Call of Same Group or Other Group by Softkey
	Call Pickup of Parked Call by Softkey
	Call Transfer - Blind, Consult by Softkey
	Call Waiting Indication
	Call Swapping by Softkey
	Conference Control
Signaling Protocols	SIP Application Server, Proxy, Registrar and Location Server(RFC3261)

	Multiple ITSP Trunk with SIP & H.323 Account Support	
	- IP UA Client Role for Registering to ITSP SIP Server	
	- H.323 Gatekeeper Client Role for Registering to ITSP H.323 Gatekeeper Server	
IVR (Interactive Voice Response) & Auto Attendant	Default Auto Attendant Support	
	IVR Function	Provides with GUI-based Smart IVR Scenario Editor
		Upload/Download Scenario by Smart IVR Scenario Editor
		Supports Multiple Concurrent Scenarios
		Support Recordable IVR Prompts
Voice Mail	Support Voice Mail with IVR	
	Access from Remote Site via Trunk Support	
	Voice Mail Notification Support	
Conference	G.711 u-law, G.711 a-law Internal 3-Party Audio Conference Support, MCU (8 , G.729,G.723.1)	
	Ad-Hoc Conference	
	Dial-Out Conference	
	Meet-me Conference	
	Multiple External MCU Support (Video, Audio, etc) : AP-MC1000, AP-MC3000	
	Conference Chair and Participants Management	
Music & Announcement	Music on Hold	
	Replaceable Announcements	
	Dialing Music/Tone Service	
IP-PBX User & Device Management	LDAP(Lightweight Directory Access Protocol) Support	
	- Support Hierarchical Organization	
	Auto Discovery of IP Phones & IP Video Phones	
	Monitoring Status of Phones	
IP-PBX Miscellaneous Function	Distinctive Ring by Calling User	
	Auto Config & Upgrade	
	Intercom	
	Personal Directory	
	Downloadable Ring	
Basic Routing	IPv4/IPv6 Dual Stack	
	Management Routing	Telnet, FTP, TFTP, SSH, SNMP, Syslog support
		Packet filtering (Access-list)
		Static
Network	Standard SNMP Agent (MIB v2) Support	

Management	Traffic Queuing
	Remote Management using Console, Rlogin, Telnet
	Web based Managements using HTTP Server Interface
Security Functions	Standard & Extended IP Access List
	Access Control and Data Protections
	Enable/Disable for Specific Protocols
	Multi-Level User Account Management
	Auto-disconnect for Telnet/Console Sessions

	PPP User Authentication Supports
	    Password Authentication Protocol(PAP)
	    Challenge Handshake Authentication Protocol (CHAP)

Operation & Management	System Performance Analysis for Process, CPU, Connection I/F
	Configuration Backup & Restore for APOS Managements
	Debugging, System Auditing, and Diagnostics Support
	System Booting and Auto-rebooting with Watchdog Feature
	System Managements with Data Logging
	IP Traffic Statistics with Accounting
Other Scalability Features	DHCP Server & Relay Functions
	Network Address Translation (NAT) Function
	Port Address Translation (PAT) Function

	Transparent Bridging (IEEE Standard) Function
	    Spanning Tree Bridging Protocol Support
	    Remote Bridging Support
	    Concurrent Routing and Bridging Support

	Cisco Style Command Line Interface(CLI)
	Network time Protocol(NTP) Support

Input/Output Components

Components of the Front Panel

Figure 1-2 Front View

Table 1-4 Description for the Components of the Front Panel

No.	Component	Description
(1)	RST	Indicating reboot of the system
(2)	LAN 0	Fast Ethernet Interface of 10/100Mbps for WAN (RJ45)
(3)	LAN 1	Fast Ethernet Interface of 10/100Mbps for LAN (RJ45)
(4)	CONSOLE	The console interface for network management (RJ45)
(5)	RUN	Indicating the normal operation of the system (green)
(6)	LAN0/LAN1 LED	LED for indicating the status of Link/Act LAN0/LAN1 (LINK – lighting in green, ACT- blinking in green)
(7)	Voice Port LED	LED for indicating the voice port status(green)

Components of the Rear Panel

Figure 1-3 IPNext190 Rear View

Table 1-5 Description for the Components of the Rear Panel

No.	Component	Description
(1)	SLOT 0	The slot mounting the Voice Module (optional) (AP-N1-FXS8, AP-N1-FXO8, AP-N1-FXO4S4, AP-N1-E1/T1 are the mountable modules)
(2)	HS	Press the switch fro Hot-Swap operation and check the green lamp on the left of the switch(green)
(3)	SLOT 1	The slot for mounting the voice module (option) (AP-N1-FXS8, AP-N1-FXO8, AP-N1-FXO4S4, AP-N1-E1/T1 are the mountable modules)
(4)	AC 110-220 V	The plug for connecting AC power cable for power supply
(5)	SW	The switch for turning on/off the power of the system.

Chapter 2.   Installing

Preparing for Installation

Safety Recommendations

The following safety guidelines are recommended when working with the equipment:

- Keep the area around the IPNext190 as free from dust as is practical before and after installation.

- When you need to open the cover of the IPNext190 Series, please place the equipment on a flat and safe place.

- When you work on the equipment, please do not wear any loose clothes, When you wear a tie or scarf, please be careful not to slip down and roll up the sleeves because if you don't, you can entangled to the equipment.

- Avoid any actions that may effect the equipment or the operator.

Maintaining Safety with Electricity

There are two main sources of electrical problems with the IPNext190: the power supply and static electricity.

This section describes safety recommendations for each case.

- **Electrical Safety**
  - ✓ Work in a place where you can shut down the power immediately in case of an accident due to electricity.
  - ✓ When you install or uncover the equipment, please turn off the power.
  - ✓ Avoid operating the equipment alone at a potentially dangerous environment.
  - ✓ Do not assume the power is switched off, but always confirm the power status.
  - ✓ Be extremely cautious when operating in a humid environment or with an uncovered power extension cable.

- **Preventing Electrostatic Discharge Damage**
  - ✓ The main chip-set of the Gateway are very delicate and misuse may result in static electrostatic discharge damage.

✓ If a static prevention waist strap is available, strap it around the wrist and earth the cord before operating the equipment.

✓ If no waist tap is available, stand on the ground and hold a metal part of the chassis will help prevent static electricity.

Site Requirements in General

The IPNext190 is ready for use where electronic products are used. However, a location with the following conditions is recommended for the maximum performance.

- A level and well ventilated location is recommended.
- Secure the equipment safely where intended to install.
- Avoid placing objects on top of the equipment.
- Install the equipment in a cool location avoiding direct sunlight.
- Maintain distance from flammable, chemical, or magnetic objects

Required Tools and Equipment

This procedure is to follow EIA standards and other EMI regulations when you install the gateway

The following section describes the Ethernet Cable, and the Console Cable which can be connected to the IPNext190.

Some cables and equipment are not included and your need to purchase them separately. Please prepare the following tools and equipment

- A standard screw driver set
- The cables to connect LAN and console port
- RJ-45 to RJ-45 connection type for LAN port
- RS-232C cable type for console with RJ-45 connector type (included in the package)

- **Ethernet Port**
  The IPNext PBX Series have two RJ-45 types of Ethernet ports on the rear panel and also has LEDs indication the port status. Use the standard cable and connector types of this port to access LAN. Refer to Appendix B for pin details for the Ethernet cable.
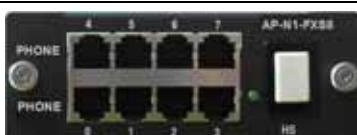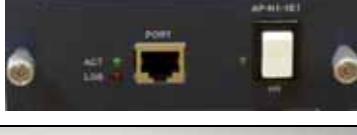
- **Console Port**

    On the Front, the IPNext190 has one RJ-45 type of RS-232C Female DCE connector interface of one CPU on the front. Through this port, you can perform initial setups, monitoring and debugging. The cable and connector are required. Refer to the appendix of this guide for the cable and pin specifications for RS-232C console cable.

Package contents

Completely unpack all of the contents from the box and inspect each item for damage and ensure that you have all of the components listed below:

Table 2-1 IPNext190 Product Package

No	Items	Contents	Unit
1	**IPNext190**		1
	AP-N1-FXS4O4 **(optional)**		
	AP-N1-FXS8 **(optional)**		
	AP-N1-FXO8 **(optional)**		
	AP-N1-1E1 **(optional)**		
2	**LAN Cable** **(RJ45 to RJ45 Type)**		1
3	**Console Cable** **(RJ45 to DB9 Type**		1
4	**Power Cable and Adapter**		1

5	**Rack Mount Adapter Kit (For 19" Standard Chassis)**		1

Installing

Connecting Async Serial interface

Connect RJ-45 type of RS-232C Serial Console Cable to the console port. Then connect the serial connector to the serial port of the PC management on the other side.

RJ45 to DB9
Console Cable

Management
PC
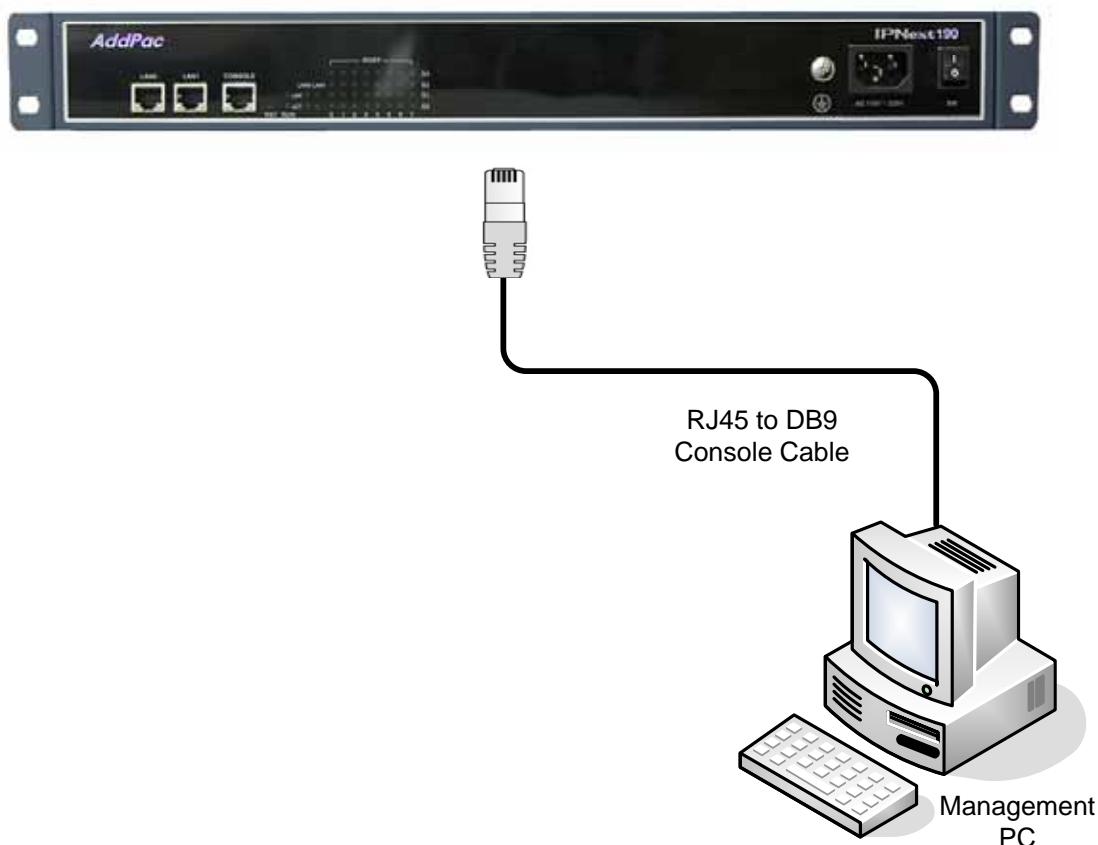
Figure 2-1 Connecting Async Serial Interface

Connecting Ethernet

Use RJ-45 standard of UTP cable to connect to the equipment with WAN interface (router or ADSL/ Cable Modem). To connect to the router or modem directly, use cross0over cable. For connection to a hub, use direct-through cable.

Connect LAN0/LAN1 Ethernet Interface to the equipment, which is suitable to the user's environment, by using RJ-45 connector. For IPNext1000, LAN0/LAN1 use Giga-Ethernet.
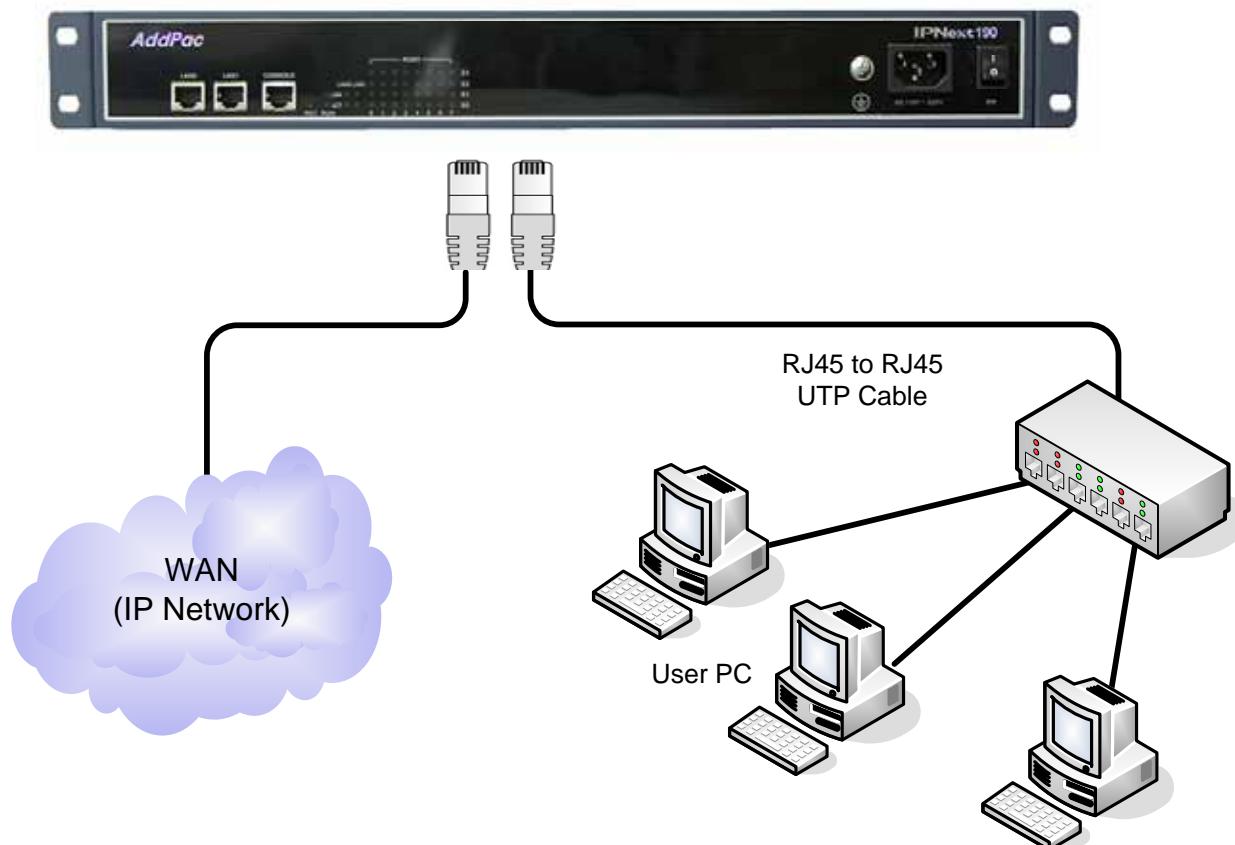
Figure 2-2 Connecting LAN0/LAN1

Connecting Analog Voice Interface (option)

Use RJ-11 stadard cable to connect FXS port with subscriber voice devices. FXS port is the interface with RJ-11 connector for connecting the basic phone device such as Keyphone, PBX and FAX.

FXO port connects the external PSTN with RJ-11 standard cable. FXO port is the interface with RJ-11 connector for connecting the standard Public Automatic Branch Exchange (PABX).
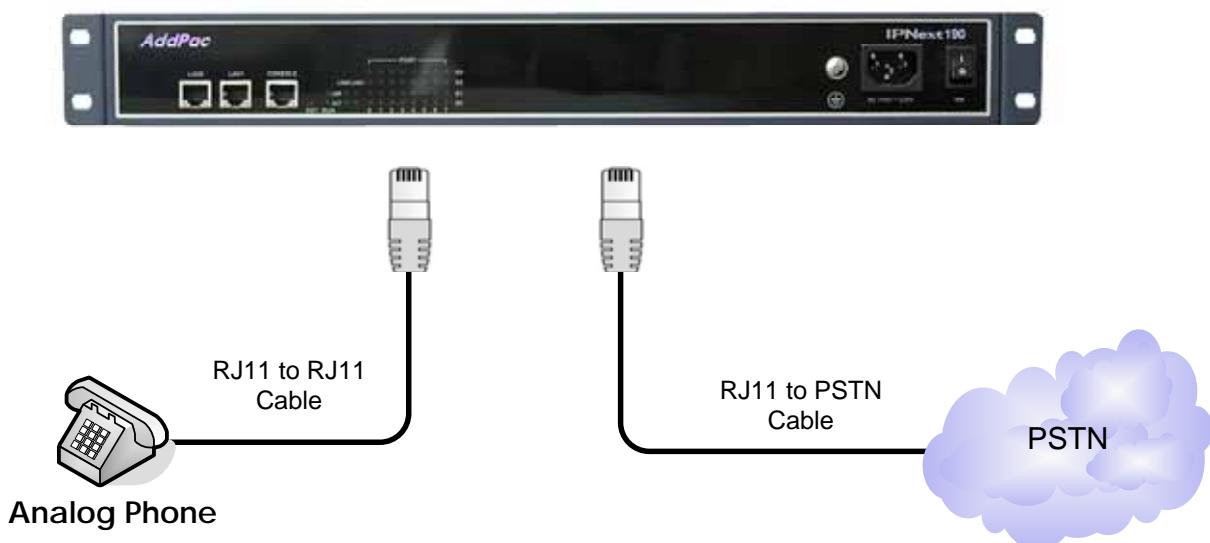
Figure 2-3 Connecting PSTN Interface

Connecting Digital E1 Interface (optional)

E1 port connects the external PSTN with RJ-45 standard cable.

E1 port is the interface, which provides RJ-45 connector to connect PSTN and the standard Public Automatic Branch Exchange (PABX).

RJ45 to PBX
Cable

PBX
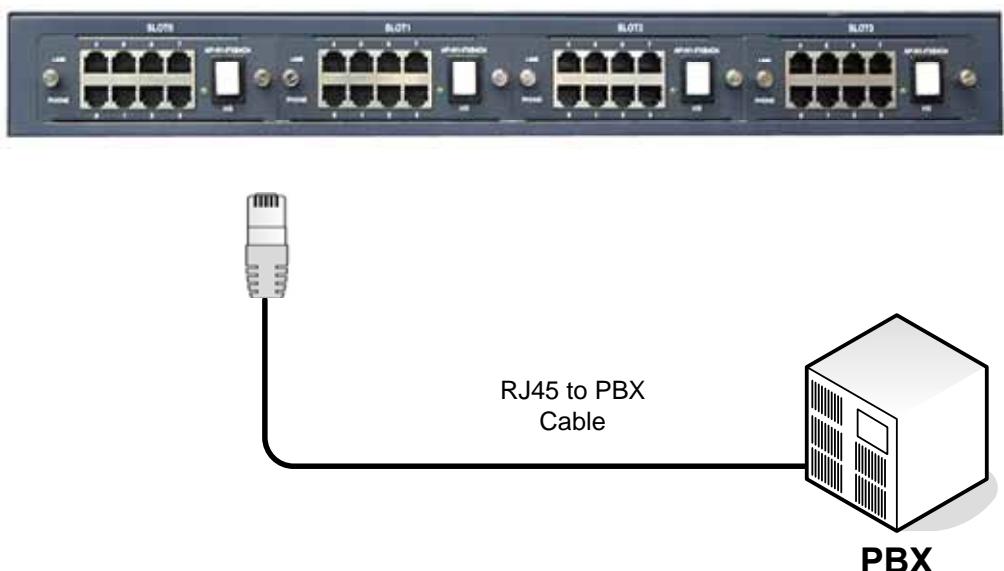
Figure 2-4 Connecting Digital E1

Booting Process and Operation Fundamentals

Before powering on the IPNext190, please be familiar with the following booting process:

- The IPNext190 goes though a self-testing process and check the basic operation of CPU, memory and interfaces

- As the Boot Loader starts up, it looks for the image file which can be proper to the IPNext190. At the default configuration, the IPNext PBX series are set to load the software from the flash memory.

- If IPNext190 can not find the software image file from the flash memory, the stand-by at the boot mode until they can download the proper software (at this time, FTP or TFTP protocol can be used to download the proper software for the IPNext190).

- The IPNext PBX series operate basing on the configured settings which are saved after the software is downloaded. Without the saved settings, the IPNext PBX Series operates at default. So the administrator should save the configured setting for the proper network operation.

During the installation, the IPNext PBX Series need to be powered on after the interface connection is finished. The power adapter is to be connected for the power supply after the connection is performed first. Please do not connect the interfaces after connecting the power adapter. The IPNext PBX Series automatically recognize the different voltage of 110V and 220V supplied from the adapter.

The following message is displayed after the IPNext190 is rebooted normally:

```
System Bootstrap, Version 1.2
Decompressing the image:
###########################[OK]
?
System Boot Loader, Version 5.1.3
Copyright (c) by AddPac Technology Co., Ltd. Since 1999.

[DUAL-BOOT] Start application (0xbc000000)...
```

```
System Bootstrap, Version 1.2

Decompressing the image:

############################################################################

#######################################################################

############################################################################

#######################################################################

############################################################################

#########[OK]
```

```
AddPac IP-PBX Series (IPNEXT190_G2)

32BIT RISC Processor With 125MHz Clock

128 Mbytes System Memory.

512 Kbytes System Boot Flash Memory

32 Mbytes System Flash Memory


1 RS232 Serial Console Interface


IPNEXT190_G2 System software Revision 8.47.024
 Released at Thu Nov 6 19:28:44 2008
 Program is 6273072 bytes, checksum is 0x3227feac

 Welcome, APOS(tm) Kernel Version 8.47.024


UTC Time is Thu Aug 21 09:01:40 2008

Copyright (c) by AddPac Technology Co., Ltd. Since 1999.


Allocating system mbuffer counter: 2560

Loading file system(ver2.2), flash-base: 0xffff0000 ram-base: 0x9912836c

Ethernet port initialization complete

Ethernet port initialization complete

System utilization reference (51/20/20/22)

USB OHCI Host Controller Driver v5.3

[USB] HUB 2 ports detected

Initializing USB Mass Storage driver...

USB Mass Storage support registered.

v0.0.1 (2005/09/09):USB HID Mouse driver

v0.0.1 (2005/09/09):USB HID Keyboard driver

Loading module: rt2570usb - v2.0.7 (2006/3/7)
```

```
[USB] Start ROOT HUB timer

Start Target Debug Server

Attach FastEthernet Interface at Slot 0, Port 0-1, <0-0>/<0-1>

[USB] Start HUB event processing

FastEthernet0/0: link is up 100 Mbps (full duplex)

FastEthernet0/1: link is up 100 Mbps (full duplex)

Interface FastEthernet0/0, changed state to UP

Interface FastEthernet0/1, changed state to UP

Hardware Type ID = 0

Hardware Revision ID = 0x0

Slot (0) Module type : FXO


Start SendMail Server

can't open configuration file [flash:/flash/apos.cfg]

Start File Transfer Protocol Server (listen tcp/21)

HTTP: document_root : /hd/smartclient

Start RtpCallScanTimer for group default


Press RETURN to get started.


RTA Module Ready

CPU internal DSP SRAM .... OK

Audio DSP S/W download ... OK

AudioConference Module Ready


Add default voipPeer(1000) ......


VoipGateway::Init1  - No IP address on the VoIP Interface

CM CREATE DOMAIN

CM CREATE DOMAIN


Welcome, APOS(tm) Kernel Version 8.47.010.

Copyright (c) 1999-2008 AddPac Technology Co., Ltd.


Login:

Login:
```

Chapter 3.   Console Commands

Overview

Using Hyper-Terminal on the Console Port for Initial Setups

To use the console terminal on PC, Terminal Emulator Application must be installed first and then use HyperTeminal Application for MS-Windows series.
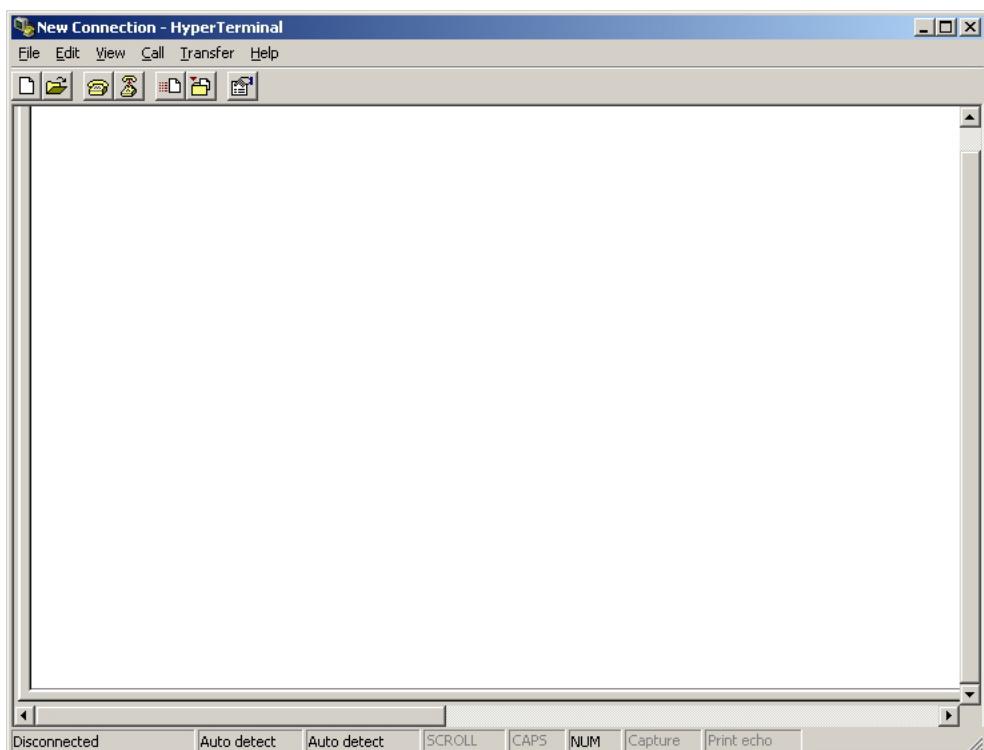
Figure 3-1 MS-Windows   Terminal Emulator HyperTerminal

After HyperTerminal is started, create a name for a new connection. The connection name is created at the user's discretion. In here, the new connection is named as 'AddPac'.
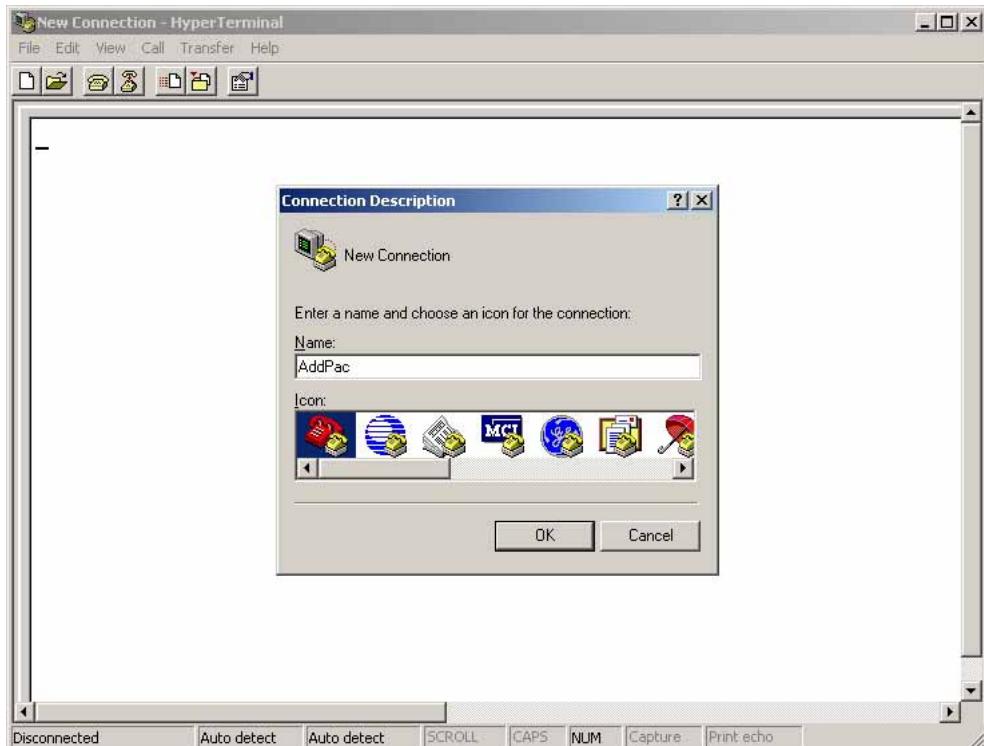
Figure 3-2 Connection Name Entry for HyperTerminal

Specify an interface to which the console cable is connected in the following connect options.

Console cable is generally   connected to RS-232C 9Pin Serial Port of PC. Choose the right port for user's network environment. In here, 'COM1' is connected.
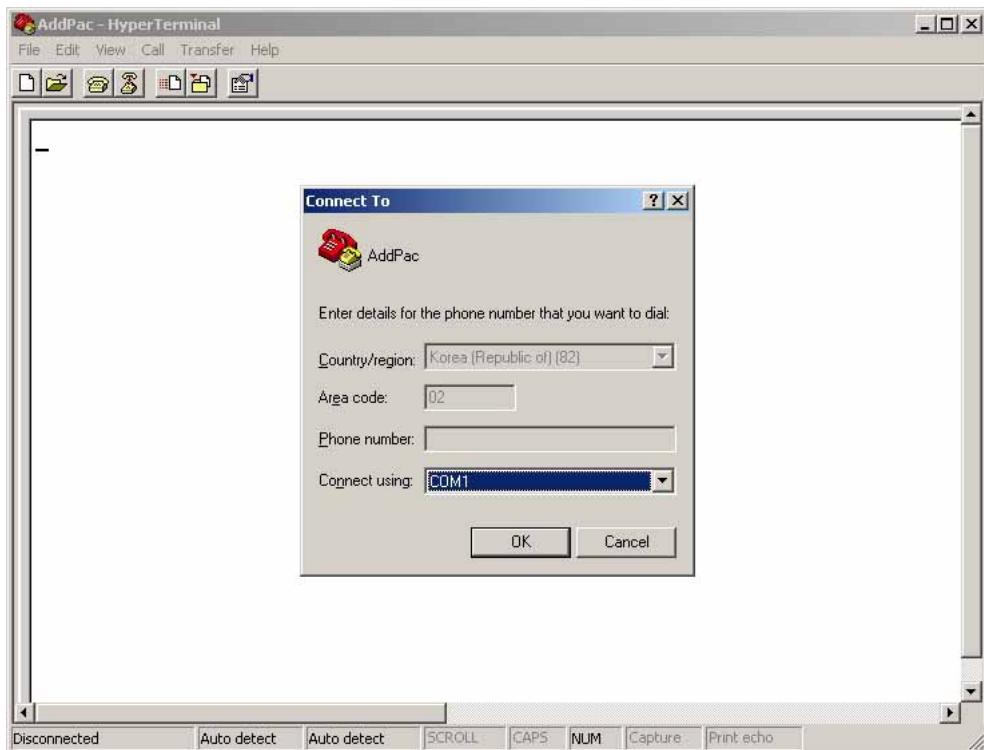
Figure 3-3 Settings for Connecting the Console Cable to Serial port

Specify each set point in the following registry information of the interface. The example sets to COM1.
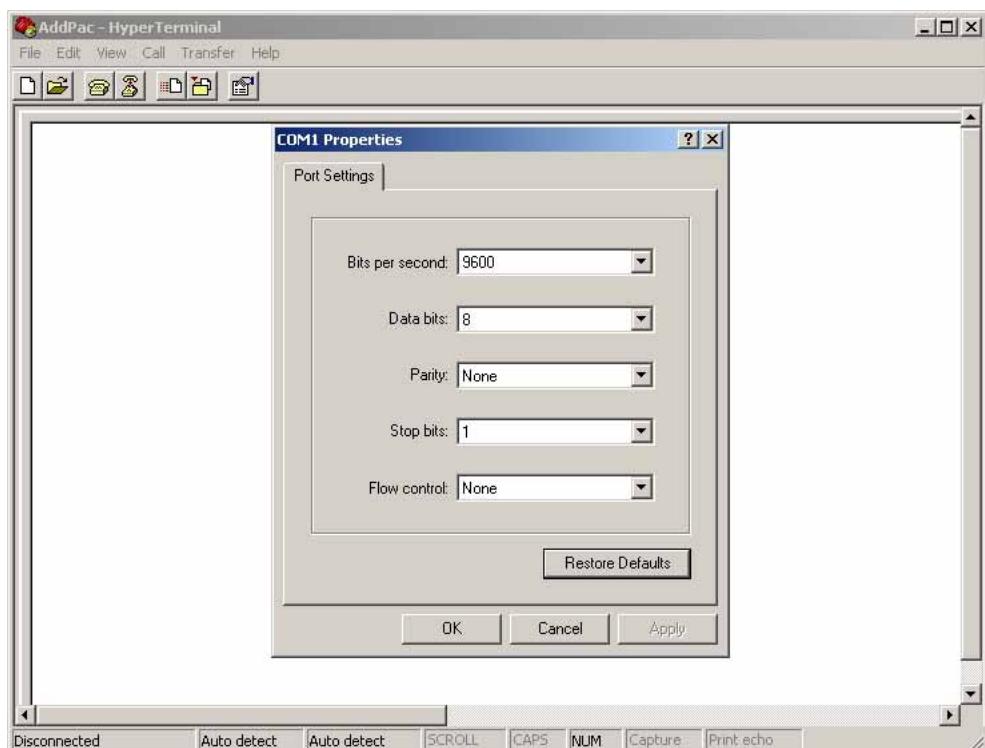
Figure 3-4 COM1 Setup Example

The booting message is displayed on HyperTerminal screen by pressing the enter key, after the setups.

APOS Command Instructions

NOTE	All the products of AddPac Technology is implemented with APOS(AddPac Operating System). So the basic CLI(Command Line Interface) settings are all same.

All the commands for configuring IPNext190 can be used by accessing to Console or Telnet terminal (VT-100 terminal).

In the commands, there is the user mode for accessing data network, administrator's mode for looking up the configuration status or debugging and the configuration mode for changing the environment settings or create the new ones.

The followings are the attributes of commands for configuring the IPNext190:

- You do not have to enter all the command letters and just entering a part of the command can be recognized automatically. For instance, if you want to enter 'show' command, just entering 'sh' or 'sho' can be automatically recognized as 'show'.

- On-line help provides the list of commands with usage sentences when a wrong command is entered.

- For the messages that can take more than one screen to be displayed, 'more' command is used to display the rest of messages in each additional screen.

- 'Help' and '?' command can used to see description of the command.

- The commands provide History: when you use the same commands again, you do not have to enter all the characters of command. The system prompt number allows you to enter the commands in a simple way.

- There are 3 different types of modes for the gateway commands. The commands for each mode can be described in the following pages.

User Mode Commands

The user mode command can be used by anybody who is logged into the gateway.

The prompt for the general use mode can be displayed as '**IP-PBX>**'.

Table 3-1 User Mode Commands

Command	Workflow Description
enable	Changes to the administrator mode
exit	Moves to the lower case of the prompt from the present
help	Displays APOS help screen
quit	Equals to exit command
show	The command for monitoring the configuration and operation status of the system
terminal	Determines a number of lines to be displays from the terminal
who	The command for displaying the users connected by vty
whoami	The command for displaying how the user is connected at the present

Administrator Mode Commands

Only the administrator, who logs into the gateway, can use the commands in the administrator mode. To use this command, you must log in to the gateway by the root account. An entrance to the configuration of the gateway is possible only when you log in as administrator mode.

At the administrator, all the commands in the user mode can be used.

The prompt for the administrator mode can be displayed as '**IP-PBX#**'.

Table 3-2 Administrator Mode Commands

Command	Description
clear	Initializes the initial counter and statistics
clock	Sets the present year, date and time
configure	Enters to the configuration mode
copy	Copies running config to startup config
debug	Debugs the overall system
disable	Enters to the user mode
disconnect	Closes VTY connection
dnsquery	Used for DNS Query test
dnsrv	Used for DNS SRV Record Test
end	Enters to the administrator mode
erase	Deletes config file
exit	Moves to a notch previous mode from the present
fsh	Enter File Shell
ftp	Displays APOS help screen
help	Deletes the present configuration
no	Transmits updated information to Name Server
nsupdate	Receives the clock information from ntp server
ntpdate	Checks the network connection (IPv4)
ping	Checks the network connection (IPv6)
ping6	Equals to exit
quit	Reboots the system
reboot	Checks the present status of the configuration
show	Connects remotely
telnet	Sets to display the terminal and debussing information

terminal	Transmits the file by tftp
tftp	Checks the route (IPv4)
traceroute	Checks the route (IPv6)
traceroute6	Displays a user's information who is currently connected
undebug	Displays a user's information for a terminal who is currently connected
who	Saves the present configuration
whoami	Initializes the initial counter and statistics
write	Sets the present year, date and time

System-Level Basic Configuration Settings

Login

You can create many user accounts to log in the IPNext190. Each account is limited for its access and APOS configuration settings depending on its level. The limitations of the user account, the '**roo**t', are listed as to follow:

- The user account 'root' can not be deleted.
- The entire account information can be verified by 'root' only.
- Even if the user's level is set to Admin and not the '**root**', the one can read one's account information.

Therefore, the privilege deleting and adding the account is given only to the '**root**'. Even though this can be done by Admin, the difference is recognized as the '**root**' and the Admin created by the '**root**'.

NOTE	At the factory default, the password of the IPNext PBX Series is set to '**router**'.

Table 3-3 Logging in as Root

Step	Command	Description

1	`Welcome, APOS(tm) Kernel Version 8.47.010.`
	 `Copyright (c) 1999-2008 AddPac Technology Co., Ltd.`
	 `Login:`
	 `Login: root`
		Log in root account

2	`Password: <password>`
	 `IP-PBX> enable`
	 `IP-PBX#`
		Get into APOS configuration command mode by entering the factory default password 'router' and enable at the IP-PBX mode and then b

Table 3-4 Verifying the User Account Information

Step	Command	Description
1	IP-PBX# **show username** username root password router ; password is clean text type administrator access username abc password abc ; password is clean text type administrator access username abcd password abcd ; password is clean text type operator access username abcde password abcde ; password is clean text type user access	Use APOS command to verify the user account information (The information above the account level is not displayed)

Table 3-5 Registering a New User

Step	Command	Description
1	IP-PBX# IP-PBX# configure terminal IP-PBX(config)#	Enter APOS command input mode
2	IP-PBX(config)# username ? WORD User name IP-PBX(config)# **username addpac ?** nopassword No password is required for the user to log in password Specify the password for the user	Set the login password for authentication nopassword : non-authentication mode password: authentication mode
3	IP-PBX(config)# username ? WORD User name IP-PBX(config)#**username addpac password ?** 0 Specifies an UNENCRYPTED password will follow 7 Specifies a HIDDEN password will follow WORD The UNENCRYPTED (cleartext) user password	Set the password to be displayed 0: Enter the password without encryption (displaying the password) 7: Enter the password with encryption (not displaying the password) WORD: Enter the password without encryption (displaying the password)

4	IP-PBX(config)# username ?	Set to the administrator's level
	WORD User name	Administrator: administrator's level
	IP-PBX(config)#**username addpac password**	
	router ?	Operator: operator's level
	administra System administrator	User: user's level
	tor	
	operator System operator and monitor	
	user System end-user	
5	IP-PBX(config)# username addpac password	The user ID is addpac and password is router.
	router operator ?	The level is set to operator
	<cr>	
	IP-PBX(config)# **username addpac password**	
	router operator	
	IP-PBX(config)#	

Table 3-6 Logging into General User Account

Step	Command	Description
1	IP-PBX# **exit**	Exit from the previous
	IP-PBX> **exit**	configuration to register to
	Welcome, APOS(tm) Kernel Version 8.41.008.	the user account
	Copyright (c) 1999-2006 AddPac Technology Co., Ltd.	
	Login:	
2	Login:	Enter the new user account
	Login: addpac	by using the registered
	Password: *<password>*	password 'addpac'
	IP-PBX> en	
	IP-PBX#	
3	IP-PBX# **show username**	The account information at
	username addpac password router ;	the level higher than the
	password is clean text type operator access	accessed account is not
	username abcde password abcde ;	displayed
	password is clean text type user access	

Table 3-7 Deleting User

Step	Command	Description
1	IP-PBX# configure terminal	Delete the user
	IP-PBX(config)# **no username *<user-name>***	
2	IP-PBX(config)# no username <user-name>	

Password

After the console connection, you have the privilege to execute only the show command. To get more privilege, you should enter the enable mode. If regular users enter the enable mode, the users will have all the privileges for allowing the users to change the system settings. Thus, you should set a password so that only the administrator is authorized enter the enable mode.

Table 3-8 Creating a Password

Step	Command	Description
1	# # **config t**	Enter APOS configuration command mode
2	(config)# enable password {password}	Create a password
3	**IP-PBX(config)# enable password 8 \<password>**	Enable the password
4	**IP-PBX(config)# enable password \<password>**	Disable the password

Table 3-9 Enable Mode Entry

Step	Command	Description
1	Login: Login: **root** Password: **\<password>** IP-PBX>	Log in root
2	IP-PBX> **enable** Password: **\<password>** IP-PBX#	Enter the password for Enable Mode Entry

Table 3-10 Verifying the Created Password

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 ! hostname IP-PBX **enable password 8 7N7KS8iqAThtDO7SODGdVw==**	Verify enable password which is the created password by using shown run command (Hidden)
2	IP-PBX# **show run** Building configuration...	Verify enable password which is the created password by using shown run

```
Current configuration:                              command

version 8.47.024

!

hostname IP-PBX

enable password abc
```

Table 3-11 Disabling Password

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	
2	IP-PBX(config)# **no enable password**	

hostname

You can change the prompt name in CLI that appears when you connect to the devices through a console or Telnet. If you manage multiple devices through Telnet connection, the host name is very important. It would be convenient to use the host name as the device name or location.

The following example shows to set the host name to 'IPNext190'.

Table 3-12 Creating a Hostname

Step	Command	Description
1	# # **config t**	Enter APOS configuration command mode
2	**(config)# hostname IPNext190**	Set the host name to 'IPNext190'
3	**IPNext190(config)# exit** **IPNext190#**	The hostname is set to IPNext190

Table 3-13 Initializing Hostname

Step	Command	Description
1	IPNext190# IPNext190# **configure terminal** IPNext190(config)#	
2	IPNext190(config)# **no hostname**	

```
        IP-PBX(config)#
```

clock

Use 'show clock' command to find out the system time and the present running time. This command displays the time logging and debugging on the present time basis. The clock should be set to the present time.

The following is an example for setting up clock to the present.

Table 3-14 Clock Configuration Settings

Step	Command	Description
1	# config t	Enter APOS configuration command mode
2	(config)# clock time 2008 08 07 15 50 00	Set the clock to the present time of **2005 06 07 15 50 00**

Table 3-15 Verifying clock Settings

Step	Command	Description
1	IP-PBX# **show clock** **System was started at Fri Dec 1 01:54:57 2008** **Current time is Fri Dec 1 07:35:11 2008** **Running time is 0 days 05:40:14** IP-PBX#	Use show clock command to verify the present time setting

Line vty/console

This command configures the settings for the remote user access and console. If no entry is made for a certain time period, this command configures the settings for the time to delete the corresponding terminal. If the setting is not entered, the default value is set to10 minutes. If you do not want to delete the terminal, set the time to 0.

Table 3-16 Line vty/console Configuration Settings

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command mode
2	IP-PBX(config)# **line vty**	Enter vty configuration mode
3	IP-PBX(config-line)# **exec-timeout < *minutes> <*****seconds>**	Set the time for ending the session of the terminal automatically if no entry is made for a certain time period.
4	IP-PBX(config-line)# **exec-timeout 0**	If no entry is made, the session of the terminal is not ended (Default: exec-timeout 10)
5	IP-PBX(config-line)# **session-limit *<1-8>***	Set the maximum number of vty sessions
6	IP-PBX(config-line)# **session-limit 5**	Set the limit on vty session to 5
7	IP-PBX(config)# **exit**	Exit from vty configuration mode
8	IP-PBX(config)# **line console**	Enter console configuration mode
9	IP-PBX(config-line)# **exec-timeout 0**	If no entry is made, the console terminal session is not ended (Default: exec-timeout 10)

Table 3-17 Verifying Line vty/console Settings

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX **!** **line console**	Use show run command to verify Line VTY/Console

```
      exec-timeout 0 0
      !
      line vty
       exec-timeout 0 0
       session-limit 5
```

Table 3-18 Initializing Line vty/console Settings

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	
2	IP-PBX(config)# **line vty**	
3	IP-PBX(config-line)# **no exec-timeout**	
4	IP-PBX(config-line)# **no session-limit**	
5	IP-PBX(config)# **exit**	
6	IP-PBX(config)# **line console**	
7	IP-PBX(config-line)# **no exec-timeout**	

Utilization

To configure the settings for checking the possible usage of CPU or a particular interface in a certain time interval, use utilization command. 1 minute is set at the default.

Use show utilization command to check the system usage by each Maximum, Minimum, Average, Last 30 seconds.

Table 3-19 Utilization Configuration Settings

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command mode
2	IP-PBX(config)# **utilization ?**	Set utilization (Default: disable)
	fastethernet FastEthernet IEEE 802.3	Choose the option for utilization Apply FastEthernet: Interface Utilization Apply CPU Utilization
	CPU CPU usage	
3	IP-PBX(config)# **utilization fastethernet**	Enable FastEthernet Utilization
4	IP-PBX(config)# **utilization cpu**	Enable CPU Utilization
5	IP-PBX# **clear utilization**	Initialize the information of utilization collected in the IP-PBX

Table 3-20 Verifying Utilization Settings

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX ! **utilization cpu** **utilization FastEthernet**	Use show rung command to verify utilization settings
2	IP-PBX # **show utilization** **CPU utilization** : enabled, Period : 30 seconds last 30 seconds : 11 % maximum:12%, time: Sun Jan 4 11:02:15 1970	Use show utilization command to verify the utilization information of CPU and interface.

```
    minimum : 12 %, time : Sun Jan  4 11:02:15 1970

    average : 12 %, duration : 0 days 00:03:50


FastEthernet0/0 utilization : enabled, Period : 30
seconds
    <TX>
    last 30 seconds : 6688 bps

    maximum :   0 % (     8216 bps), time : Sun Jan
4 11:04:25 1970

    minimum :   0 % (     5752 bps), time : Sun Jan
4 11:04:41 1970

    average :   0 % (      6432 bps), duration : 0
days 00:01:40
    <RX>
    last 30 seconds : 28288 bps

    maximum :   0 % (    31264 bps), time : Sun Jan
4 11:05:12 1970

    minimum :   0 % (    23744 bps), time : Sun Jan
4 11:05:03 1970

    average :   0 % (    27240 bps), duration : 0
days 00:01:40


FastEthernet0/1 utilization : enabled, Period : 30
seconds
    <TX>
    last 30 seconds :   0 bps
    maximum :  0 % (       0 bps), time :
    minimum :  0 % (       0 bps), time : Sun Jan  4
11:04:25 1970
    average :   0 % (       0 bps), duration : 0
days 00:01:40
    <RX>
    last 30 seconds :   0 bps
    maximum :  0 % (       0 bps), time :
    minimum :  0 % (       0 bps), time : Sun Jan  4
11:04:25 1970
    average :   0 % (       0 bps), duration : 0
days 00:01:40
```

```
IP-PBX#
```

Table 3-21 Disabling Utilization

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	
2	IP-PBX(config)# **no utilization fastethernet**	
3	IP-PBX(config)# **no utilization cpu**	

interface

For IPNext190 to communicate with other network devices, the IP Address must be configured. The duplex and the bandwidth for connecting with other AddPac devices are set automatically to the optimum value. However, the duplex for connecting with other vendor's devices may not fit to each other, In this case, the bandwidth and duplex should be set manually.

The following example shows configuring the IP address of 172.20.101.100 to the interface of Fastethernet 0/0 and then the link speed of 100Mbps and full duplex manually.

Table 3-22 Configuring Fastethernet

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS configuration mode
2	IP-PBX(config)# **interface fastethernet 0/0**	Enter interface configuration mode
3	IP-PBX (config-if)# **ip address 172.20.101.100 255.255.0.0**	Configure the IP address of 172.20.101.100 to the interface
4	IP-PBX (config-if)# **no speed auto**	If auto negotiation does not work, set to 100/full duplex manually (Default: auto)
5	IP-PBX (config-if)# **speed 100**	
6	IP-PBX (config-if)# **duplex full**	

3-23 Configuring IPv6 Interface

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **interface fastethernet 0/0**	Enter interface configuration mode
3	IP-PBX (config-if)# **ipv6 address 2001:e78:b01:19:114::50/64**	Set the IPv6 address of '2001:e78:b01:19:114::50/64' to the interface

Table 3-24 Configuring IPv4 Interface

Step	Command	Description
1	IP-PBX# **show run**	Use shown run command to verify the

```
Building configuration...                    specified settings of IP address, speed

Current configuration:                       and duplex

version 8.47.024

hostname IP-PBX!
```
interface FastEthernet0/0

 ip address 172.20.101.100 255.255.0.0

 full-duplex

 speed 100

Table 3-25 Configuring IPv6 Interface

Step	Command	Description
1	IP-PBX# **show run**	Use shown run command to verify the
	Building configuration...	specified settings of IPv6
	Current configuration:	
	version 8.47.024	
	hostname IP-PBX	
	!	
	interface FastEthernet0/0	
	ipv6 address 2001:e78:b01:19:114::50/64	

Table 3-26 Deleting IPv4 Interface

Step	Command	Description
1	IP-PBX#	
	IP-PBX# **configure terminal**	
	IP-PBX(config)#	
2	IP-PBX(config)# **interface fastethernet 0/0**	
3	IP-PBX (config-if)# **no ip address**	

Table 3-27 IPv6 Deleting Interface

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	
2	IP-PBX(config)# **interface fastethernet 0/0**	
3	IP-PBX (config-if)# **no ipv6 address**	

Default Route

To access a network in where a system is not configured, you should configure where to route. In the same way to configure the default gateway from PC, configure the IP of the device which has been connected already.

The following table presents an example to show configuring IPv4 to "172.20.1.1", IPv6 to "2001:e78:b01:19:1::1"

Table 3-28 Specifying IPv4 Default route

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS configuration mode
2	IP-PBX(config)# **ip route 0 0 172.20.1.1**	Specify IPv4 default route to 172.20.1.1

Table 3-29 Specifying IPv6 Default route

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **ipv6 route ::/0 2001:e78:b01:19:1::1**	Specify IPv6 Default router to "2001:e78:b01:19:1::1"

Table 3-30 Verifying IPv4 Default route

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX ! interface FastEthernet0/0 ip address 172.20.101.100 255.255.0.0 ! **ip route 0.0.0.0 0.0.0.0 172.20.1.1**	Use show run command to verify the specified IPv4 default router

---

```
        !
```

Table 3-31 Verifying IPv6 Default route

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX ! interface FastEthernet0/0 ipv6 address 2001:e78:b01:19:114::50/64 ! **ipv6 route ::/0 2001:e78:b01:17:1::1** !	Use show run command to verify the specified IPv6 default router

Table 3-32 IPv4 Default route Deleting

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	
2	IP-PBX(config)# **no ip route 0.0.0.0 0.0.0.0 172.20.1.1**	

Table 3-33 Deleting IPv6 Default route

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	
2	IP-PBX(config)# **no ipv6 route ::/0 2001:e78:b01:17:1::1**	

voip-interface

This configuration specifies VoIP service to a specific interface. VoIP service is provided by using the IP address specified to the VoIP interface, if the IP address is not specified to the VoIP interface, configuring the VoIP settings and searching the content are not possible.

Table 3-34 Configuring VoIP-Interface

Step	Command	Description

1	`IP-PBX#`
	`IP-PBX# `**`configure terminal`**
	`IP-PBX(config)#`
		Enter APOS command entry mode.

2	`IP-PBX(config)# `**`voip-interface ip fastethernet`** **`0/0 ?`**	Specify IPv4 Interface to VoIP interface

	`Preference         Set interface Preference`
	
	`<cr>`
		As preference value<1-255> gets lower, the priority gets higher.
		Preference <1>

3	`IP-PBX(config)# `**`voip-interface ip fastethernet`** **`0/0 preference 1`**	Configure VoIP service to IPv4 FastEthernet 0/0 (Default)
4	`IP-PBX(config)# `**`voip-interface       ipv6`** **`fastethernet 0/0`**	Configure VoIP service to IPv6 FastEthernet 0/0 (Default)

Table 3-35 Verifying the Settings of VoIP-Interface

Step	Command	Description

1	`IP-PBX# `**`show voip-interface`**
	`IP(Internet Protocol) VoIP Interface:`
	`  (*) `**`voip-interface  FastEthernet0/0  preference  1`**
	`link-up`
	`      voip-interface  FastEthernet0/1 `**`preference  2`**
	`link-down`
	`IPv6(Internet Protocol version 6) VoIP Interface:`
	`  (*) `**`voip-interface   ipv6   FastEthernet0/0`**
	`preference 1 link-up`
	`  !`
		Use show voip-interface command to verify the settings of voip-interface

Table 3-36 Initializing VoIP-Interface Settings

Step	Command	Description
1	IP-PBX#	
	IP-PBX# **configure terminal**	
	IP-PBX(config)#	
2	IP-PBX# **no voip-interface ip fastethernet 0/0**	
3	IP-PBX# **no voip-interface ipv6 fastethernet 0/0**	

dns

Domain Name Server (DNS) is used from Internet to change the name of network node to IP address. For specifying to DNS server, 5 addresses can be entered at maximum. Even if more than 5 addresses are entered, only 5 addresses can be applied.

Table 3-37 Configuring DNS

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **dns name-server ?**	Specify the address of Domain Name Server (Default: Disable)
	A.B.C.D Domain server IP address X:X::X:X Domain server IPv6 address	Specify the server to IPv4 address Specify the server to IPv6 address .
3	IP-PBX(config)# **dns name-server 172.17.10.10**	Enable DNS in IPv4 / IPv6 format, Priority level is determined by entry order.

Table 3-38 Verifying DNS Settings

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX ! **dns name-server 172.17.10.10** !	Use show run command to verify DNS configuration settings

Table 3-39 Disabling DNS

Step	Command	Description
1	IP-PBX# **no dns name-server**	

logging

Use logging command to manage devices and logs the operational status of the devices and determines the level of this information, provides the information to a specific host. All the settings of logging can be done in Global Configuration Mode.

Table 3-40 Configuring Logging

Step	Command	Description

1	`IP-PBX#`
	
	`IP-PBX# configure terminal`
	
	`IP-PBX(config)#`
		Enter APOS command entry mode

2	`IP-PBX(config)# logging host server ip` `172.17.10.20 515`	Specify the IP address and port of the remote host to which logging information is to be sent
3	`IP-PBX(config)# logging on`	Enable logging (Default: disable)
4	`IP-PBX(config)# logging command`	Transmit command entry through vty
5	`IP-PBX(config)# logging event ?`	Set the condition for logging event

	`0-emergency      System unusable`
	`1-alert          Immediate action needed`
	`2-critical       Critical condition`
	`3-error          Error condition`
	`4-warning        Warning condition`
	`5-notice         Normal, but significant,`
	`                 condition`
	`6-informational  Informational    messages`
	`                 only`
	`7-debug          debug-level messages`
		Using logging event 7-debug is recommended in general

Table 3-41 Verifying Logging Configuration Settings

Step	Command	Description
1	IP-PBX# **show run**	Use show run command to verify the
	Building configuration...	logging settings
	Current configuration:	
	version 8.47.024	
	!	
	hostname IP-PBX	
	!	
	logging command	
	logging event 7-debug	
	logging host server ip 172.17.10.10 515	
	logging default-level warn	
	logging category clog info	
	logging on	
	!	

Table 3-42 Disable Logging

Step	Command	Description
1	IP-PBX#	
	IP-PBX# **configure terminal**	
	IP-PBX(config)#	
2	IP-PBX(config)# **no logging host server ip** **172.17.10.20 515**	
3	IP-PBX(config)# **no logging on**	
4	IP-PBX(config)# **no logging command**	

System Service Configuration

telnet server

Telnet is used as one of the ways to manage a device in remote location far away. Telnet is enabled at the default setting. So unless it is disabled, you do not have to use another command to enable. Telnet has the default port called TCP 23. You can make a change depending on the environment.

Table 3-43   Telnet Configuration

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS configuration mode
2	IP-PBX(config)# **telnet server**	Enable telnet service
3	IP-PBX(config)# **telnet port 23**	(Optional) Use this command to change the default telnet port number 23

Table 3-44 Verifying Telnet Settings

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX ! interface FastEthernet0/0 ip address 172.20.101.100 255.255.0.0 ! ip route 0.0.0.0 0.0.0.0 172.20.1.1 ! **no telnet server**	Use show run command to verify the disabled tenet setting
2	IP-PBX# **show ip tcp port** Local Address / Port Remote Address / Port State **inet 0.0.0.0 23 0.0.0.0 0 LISTEN**	Use show ip tcp port command to verify the operational status of telnet port (enable)

Table 3-45 Disabling Telnet

Step	Command	Description
1	IP-PBX#	
	IP-PBX# **configure terminal**	
	IP-PBX(config)#	
2	IP-PBX(config)# **no telnet server**	

ftp server

FTP is enabled at the default setting and it can be enabled when it is necessary. ftp server command is enabled at TCP21.

FTP is disabled at the default setting and it can be enabled depending on its necessity. The ftp server command enables ftp on the port number TCP21. Use ftp allow anonymous command to configure the open ftp server. The user account for accessing ftp is configured by username command. The following example enables ftp server and allowing access for the anonymous account.

Table 3-46 FTP Server Configuration

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **ftp server**	Enable FTP server
3	IP-PBX(config)# **username root password router**	FTP user account. Create "root/router"
4	IP-PBX(config)# **ftp port 21**	(Optional) Configure to change the default ftp port 21
5	IP-PBX(config)# **ftp allow anonymous**	(Optional) Allowing the anonymous account

Table 3-47 Verifying FTP Settings

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX ! interface FastEthernet0/0 ip address 172.20.101.100 255.255.0.0 ! ip route 0.0.0.0 0.0.0.0 172.20.1.1 ! **ftp server**	Use show run command to verify the enabled FTP setting details
2	ideoPhone# **show ip tcp port** Local Address / Port Remote Address / Port	Use show ip tcp port command to verify the operational status of ftp port

```
State
```

`inet 0.0.0.0 21    0.0.0.0 0 LISTEN`

Table 3-48 Disabling FTP

Step	Command	Description

1	`IP-PBX#`
	
	 `IP-PBX#` **`configure terminal`**
	
	 `IP-PBX(config)#`	

2	`IP-PBX(config)#` **`no ftp server`**
	
	 `IP-PBX(config)#  Stop  File  Transfer  Protocol`
	
	 `Server`	

snmp

Enable snmp server and assign snmp community with a setting to monitor a device in a remote location by using SNMP.

The following example configures snmp community setting to 'public',

Table 3-49 snmp Configuration

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS configuration mode
2	IP-PBX(config)# **ip snmp server**	Enable logging (Default: Disable)
3	IP-PBX(config)# **snmp port 161**	(optional) Change the default snmp port number to161
4	IP-PBX(config)# **snmp community public ro 0.0.0.0**	Set the value of snmp community to public
5	IP-PBX(config)# snmp host 10.1.1.1 version v2c AddPac	Transmit Trap to SNMP Manager at 10.1.1.1, as String AddPac by SNMP v2c protocol

Table 3-50 Verifying snmp Settings

Step	Command	Description
1	IP-PBX# **show run**	Use show run command to verify the
	Building configuration...	enabled SNMP
	Current configuration:	
	version 8.47.024	
	hostname IP-PBX!	
	!	
	interface FastEthernet0/0	
	ip address 172.20.101.100 255.255.0.0	
	!	
	ip route 0.0.0.0 0.0.0.0 172.20.1.1	
	!	
	snmp community public ro 0.0.0.0	
	snmp host 10.1.1.1 version v2c AddPac	
	!	
	ftp server	
	snmp server	
2	IP-PBX# **show snmp**	Use show snmp command to verify
	snmp community public ro	SNMP settings
	snmp host 10.1.1.1 version v2c AddPac	

Table 3-51 Disabling snmp

Step	Command	Description
1	IP-PBX#	
	IP-PBX# **configure terminal**	
	IP-PBX(config)#	
2	IP-PBX(config)# **no snmp server**	

IP TCP Keep-alive

TCP Session is formed with the corresponding service To use variety of services of the IPNext PBX (Coloring Service, Voice Mail, Messenger, IVR). Use tcp keep-alive count and timeout settings to check TCP Session constantly.

It is recommended to use the same settings between the IPNext PBX and server.
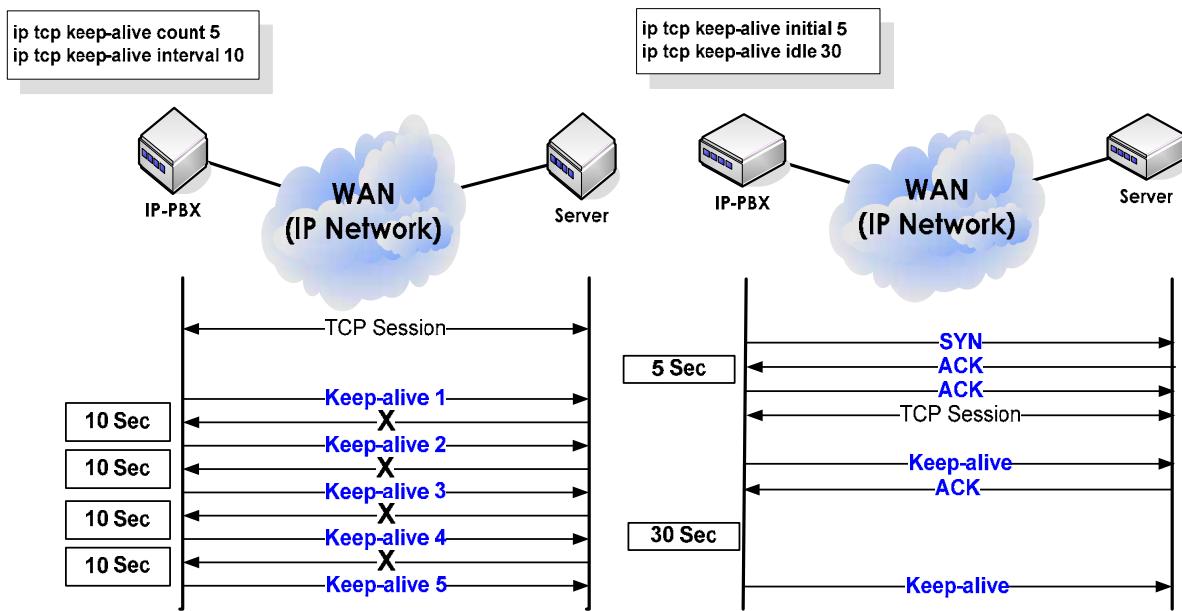
Table 3-52 IP TCP Keep-alive

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **ip tcp keep-alive count 5**	If there is no response for keep-alive message, the count for re-try (Default: count 8)
3	IP-PBX(config)# **ip tcp keep-alive idle 30**	After receiving a response for keep-alive message, this is the timeout setting until keep-alive message is received. (Default: idle 300)

4	IP-PBX(config)# **ip tcp keep-alive initial 5**	This is the timeout setting to wait for ACK message after TCP SYN is transmitted from the other party (Default: initial 25)
5	IP-PBX(config)# **ip tcp keep-alive interval 10**	If there is no response for keep-alive message, this is the setting for retry time interval. (Default: interval 25)

Table 3-53 Verifying IP TCP Keep-alive

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX ! **ip tcp keep-alive count 5** **ip tcp keep-alive idle 30** **ip tcp keep-alive initial 5** **ip tcp keep-alive interval 10** !	Use show run command to verify the settings of ip tcp keep-alive
2	IP-PBX# **show ip tcp config** ! ( ) ! Assume SO_KEEPALIVE on all TCP connections : 1 **tcp_keepcnt : 5 tcp_keepinit : 5 tcp_keepidle :** **30 tcp_keepintvl : 10** !	Use show ip tcp config command to verify the settings of ip tcp keep-alive

Table 3-54 Initializing IP TCP Keep-alive

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	
2	IP-PBX# **no ip tcp keep-alive count**	
3	IP-PBX# **no ip tcp keep-alive idle**	
4	IP-PBX# **no ip tcp keep-alive initial**	
5	IP-PBX# **no ip tcp keep-alive interval**	

call-manager sscp store-event

call-manager sscp store-event configuration settings are used to set the interval of notification message between call-manager and presence server.

For changing the user status information, the notification message is sent to the presence server from the call manager first, the presence server is used to deliver the changed information to PSClient and the Messenger registered to itself.
The notification message is sent if one of the conditions of sscp store-event count / time is matched.

If store-event-count is set to 1 in the environment where the registered user to the IPNext PBX changes one's status very often, the notification message is sent whenever each user status is changed. So the IPNext PBX may take a heavy load as a result. Therefore, the administrator needs to configure the settings suitable to the environment settings accordingly.

Table 3-55 call-manager sscp store-event Settings

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **call-manager sscp store-event**	Configure the settings of call-manager sscp store-event
	count set store event count value	Create notification depending on the number of changes in the user status
	time set store event timeout value	Create notification in a certain time interval
3	IP-PBX(config)# **call-manager sscp store-event-count 1**	Create notification message when a change takes place in the user status once. (Default: count 10)
4	IP-PBX(config)# **call-manager sscp store-event-time 1**	Notification is created every second. (Default: time 3)

Table 3-56 Verifying call-manager sscp store-event Settings

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX ! **call-manager sscp store-event-time 1** **call-manager sscp store-event-count 1** !	Use shown run command to verify the settings of call-manager sscp store-event

2	IP-PBX# **show call-manager sscp**
	
	!
	
	(skipped)
	
	!
	
	SSCP Policy Information.
	
	    cm service status = On
	
	    signaling-port = 8855
	
	    packet-size = 1472
	
	    client-session logging count = 0
	
	    client-session registering count = 0
	
	    event store time = 1(sec)
	
	    event store count = 1
	
	    event total store count = 0
	
	!
		Verify the settings of call-manager sscp store-event time/count by using show call-manager sscp command.

Table 3-57 Initializing call-manager sscp store-event Settings

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	
2	IP-PBX# **no call-manager sscp store-event-time**	
3	IP-PBX# **no call-manager sscp store-event-count**	

Call-Manager Service Configuration

http server

http server is enabled at default. If it is disabled, it should be enabled for configuring the settings of the IPNext PBX, this command is to check the status of Call Manager and use Auto Upgrade Server.

Table 3-58 Configuring http

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **http server**	Enable HTTP server. (default)
3	IP-PBX(config)# **no http authentication**	(Optional) Access to the server without http authentication. http authentication is recommended. (Default: enable)
4	IP-PBX(config)# **http document-root /hd**	Configure the default directory for accessing Web-based SMM (the default setting for the version lower than v8.47.024 is /hd) *When you upgrade to higher version than v8.47.024, change the setting of http document–root to /hd (the default setting for the version lower than v8.47.024 is /hd/smartclient)

Table 3-59 Verifying http Configuration Settings

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX! interface FastEthernet0/0	Use show run command to verify http configuration settings

```
 ip address 172.20.101.100 255.255.0.0

ip route 0.0.0.0 0.0.0.0 172.20.1.1

ftp server

http server

no http authentication

http document-root /hd
```

2	IP-PBX# **show http** **http server is enabled** **no http authentication** **http document-root /hd** IP-PBX#	Use show http command to verify http server configuration settings (enable).
3	IP-PBX# **show http** **http server is disabled** **http document-root /hd**	Use show http command to verify http server configuration settings (disable).

Table 3-60 Disabling http

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	
2	IP-PBX(config)# **no http server**	

network-domain interface

network-domain interface is used to configure the physical interface and multi-domain for Call Manager Service. Domain public is specified to the interface of FastEthernet0/0 and domain private is specified to the interface of FastEthernet0/1.

For interworking with the remote server (PS2000, RBT1000, UMS1000, IVR1000, MC3000 and others), the network domain name should be set same as the one in Call Manager.

Table 3-61 Configuring the Settings of network-domain interface

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **network-domain interface ip fastethernet 0/0 domain public**	Set network-domain interface to FastEthernet 0/0 at5 IPv4 and domain name to public(Default)
3	IP-PBX(config)# **network-domain interface ip fastethernet 0/1 domain Private**	Set network-domain interface to FastEthernet 0/0 at5 IPv4 and domain name to private(Default)
4	IP-PBX(config)# **network-domain interface ipv6 fastethernet 0/0 domain public**	(Optional) Set network-domain interface to FastEthernet 0/0 at5 IPv6 and domain name to public(Default)
5	IP-PBX(config)# **network-domain interface ipv6 fastethernet 0/1 domain Private**	(Optional) Set network-domain interface to FastEthernet 0/0 at5 IPv6 and domain name to private (Default)

Table 3-62 Verifying network domain interface Configuration Settings

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX ! Network Domain interface configuration. ! **network-domain interface ip FastEthernet0/0** **domain public** **network-domain interface ip FastEthernet0/1** **domain private** !	Use show run command to verify the settings of network-domain

Table 3-63 Initializing network-domain interface Settings

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	
2	IP-PBX(config)# **no network-domain interface ip fastethernet 0/0 domain public**	
3	IP-PBX(config)# **no network-domain interface ip fastethernet 0/1 domain Private**	
4	IP-PBX(config)# **no network-domain interface ipv6 fastethernet 0/0 domain public**	
5	IP-PBX(config)# **no network-domain interface ipv6 fastethernet 0/1 domain Private**	

LDAP

Light-weight Directory Access Protocol (LDAP) is a software protocol which finds and locates a resource such as a file or device in a network of an organization, individual, internet or intranet of an enterprise. As a light-weighted version of DAP, LDAP is a part of X.500 which is a direcctory service standard

The AddPac Ipnext190 uses LDAP to store the necessary data for its operation. The followings show how to configure the setting of LDAP:

Table 3-64 Configuring LDAP

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **ldap**	Enter ldap configuration mode
3	IP-PBX(config-ldap)# **slapd**	Enable ldap service (Default: 389)

Table 3-65 Configuring LDAP Notification Server

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **ldap**	Enter ldap configuration mode
3	Router(config-ldap)# **notification 5389**	Configure ldap notification server and its port (Default TCP Listen Port: 5389)

Table 3-66 Changing LDAP Port

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **ldap**	Enter ldap configuration mode
3	IP-PBX(config-ldap)# **no slapd** Waiting for cache to release all entries. IP-PBX(config-ldap)# LDAP daemon is now inactive.	Disabling ldap service
4	IP-PBX(config-ldap)# **slapd 9389** LDAP LDBM backend cache entry size is 5000 LDAP daemon is now active	Set ldap port to 9389 (Range: 1-65535)
5	IP-PBX(config-ldap)# **exit**	Exit from ldap configuration mode
6	IP-PBX(config)# **ldapclient**	Enter ldapclient configuration mode
7	IP-PBX(config-ldapclient)# **host 127.0.0.1 9389**	Change ldap server port to 9389
8	IP-PBX(config-ldapclient)# **end**	Exit from ldapclient configuration mode
9	IP-PBX# **write** Proceed with write? [confirm] Building configuration... [OK] Configuration saved to flash:/flash/apos.cfg	Save the settings
10	IP-PBX# **reboot**	Reboot the system

Table 3-67 Verifying LDAP and Notification Server Configuration Settings

Step	Command	Description
1	IP-PBX# **show run** Building configuration… Current configuration: version 8.47.024 hostname IP-PBX ! ldap data-dir /hd/ldap suffix "dc=addpac,dc=com"	Use show run command to verify ldap and notification server configuration settings

```
rootdn "cn=Manager,dc=addpac,dc=com"

rootpw secret

include /hd/ldap/schema/core.schema

include /hd/ldap/schema/cosine.schema

include /hd/ldap/schema/inetorgperson.schema

include /hd/ldap/schema/addpac.schema

include /hd/ldap/schema/apcm.schema

include /hd/ldap/schema/apglobal.schema

include /hd/ldap/schema/apmessage.schema

include /hd/ldap/schema/apms.schema

include /hd/ldap/schema/apmd.schema

include /hd/ldap/schema/apums.schema

slapd 389

notification 5389

!
```

2	IP-PBX# **show ip tcp port**					Show ip tcp port
	Local Address	/ Port	Remote Address	/		ldap ldap
	Port State					Notification Server
	inet 127.0.0.1	**5389**	**127.0.0.1**	**2048**		.
	ESTABLISHED					
	inet 127.0.0.1	2048	127.0.0.1	5389		
	ESTABLISHED					
	inet 0.0.0.0	5081	0.0.0.0	0		
	LISTEN					
	inet 172.17.113.50	1721	0.0.0.0	0		
	LISTEN					
	inet 0.0.0.0	23	0.0.0.0	0		
	LISTEN					
	inet 0.0.0.0	5389	0.0.0.0	0		
	LISTEN					
	inet 0.0.0.0	**389**	**0.0.0.0**	**0**		
	LISTEN					
	inet 0.0.0.0	80	0.0.0.0	0		
	LISTEN					
	inet 0.0.0.0	21	0.0.0.0	0		
	LISTEN					
	IP-PBX# **show call-manager ldap**					Verify the enbled ladap port
	--					settings by using show call-

```
manager enable : TRUE                                  manager ldap command

base dn        : dc=addpac,dc=com

cluster base(*) : ou=APCM_C1,dc=addpac,dc=com

main           : ldap://127.0.0.1:389

manager id     : Manager

manager dn(*)  : cn=Manager,dc=addpac,dc=com

manager pw     : secret

global user id  : ga

global user pw  : secret

-------------------------------------------

Directory server last connection          TRUE

Directory Max Queue Size =  300

-------------------------------------------

Directory server ip    Port    Mode    Priority

-------------------------------------------

127.0.0.1              389     M       1
```

Table 3-68 Disabling LDAP and Notification Server Configuration Settings

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	
2	IP-PBX(config)# **ldap**	
3	IP-PBX(config-ldap)# **no slapd**	
4	IP-PBX(config-ldap)# **no notification**	

Presence Server

Presence Server is disabled at default and it can be enabled if necessary. Presence Server is the server for Smart Messenger and Presence Client Service. Smart Messenger interworks with the AddPac IP Phone product series and takes many additional services such as IP Phone Control, User Presence Status and Voice Mail. Presence Client Service provides User Presence Status and Speed Button Service to the IP Phone (To use Presence Server, the IP-PBX should have Presence Server (Max Messenger Session) License.

Table 3-69 Enabling Presence Server

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **presence**	Enter Presence Server configuration mode
3	IP-PBX(config-ps)# **service enable**	Enable Presence Server (Default: Disabled)

Table 3-70 Verifying Presence Server Configuration Settings

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX ! presence server configuration. ! **presence** **service enable** sscp store-event-time 1 sscp store-event-count 1 logger disable logger level error	Use show run command to verify Presence Server configuration settings

Table 3-71 Disabling Presence Server

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	
2	IP-PBX(config)# **presence**	
3	IP-PBX(config-ps)# **service disable**	

Media Server

Media Server is disabled at default and it can be enabled if necessary. Media Server interworks with the AddPac IP Video Phone and IP Phone provides the variety of services including Ring Back Tone (RBT), Music On Hold (MoH) and Caller ID (CID).

Table 3-72 Media Server Configuration Settings

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **media**	Enter Media Server Configuration Mode
3	IP-PBX(config-media)# **rbt enable**	Enabling Media Server (Default: Disabling)

Table 3-73 Verifying Media Server Configuration Settings

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX ! ! media server configuration. ! **media** **rbt enable** !	Use show run command to verify the configuration settings of Media Server

Table 3-74 Disabling Media Server

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	
2	IP-PBX(config)# **media**	
3	IP-PBX(config-media)# **rbt disable**	

LDAP Client

LDAP Client must be configured for Call Manager service. After LDAP Client is configured, Device is automatically registered to Call Manager LDAP.

Table 3-75 LDAP Client Configuration Settings

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **ldapclient**	Enter ldapclient configuration mode
3	IP-PBX(config-ldapclient)#**name IPNext190_test**	Create a device name for registering ldap.
4	IP-PBX(config-ldapclient)#**host 127.0.0.1 389**	Configure ladap server IP and port Default IP 127.0.0.1 Default Port 389
5	IP-PBX(config-ldapclient)# **ldap enable**	Enable ldapclient service (Default: Disable)
6	IP-PBX(config-ldapclient)# **autoreg** **start**	(optional) Use this command to reregistering the device automatically if the device is deleted

Table 3-76 Verifying LDAP Client Configuration Settings

Step	Command	Description
1	IP-PBX# **show run** Building configuration... Current configuration: version 8.47.024 hostname IP-PBX ! **ldapclient** **name IPNext190_test** **host 127.0.0.1 389** **ldap enable** ! !	Use show run command to verify the configuration settings of ldap client.
2	IP-PBX# **show call-manager domain cluster**	Use show call-manager domain cluster

```
Device pool

--------------------------

DevicePool 1

  Name = default

  Region = 1

  CallManagerGroup Information

  - N/A


CallManager Status Summary

-----------------------------------------------

-----------------------

- Cluster Mode                   : Active

- Monitoring Link Status          : Disabled

- Link Status                   : UP

- Monitoring LDAP Connection Status : Enabled

- LDAP Connection Status          : UP

- On Trunk Initiating           : Yes

- Trunk Initiating Ready         : No

- CallManager Status            : In Service


- Binding Status


- My CallManagerProfile = 1


- CallManagerProfile 1

 * Name = autoreg1

 * KeepAlive Interface = 3


IP-PBX#
```

command to verify the connection status. If the connection sttus is up ldap client is regtered normally. If the connect status is down, it is not registered normally.

Table 3-77 Disabling LDAP Client

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **ldapclient**	Enter ldapclient configuration mode
3	IP-PBX(config-ldapclient)#**no name**	Cancel the device name
4	IP-PBX(config-ldapclient)#**no host**	Cancel the IP and port settings of ldap server Default IP 127.0.0.1 Default Port 389
5	IP-PBX(config-ldapclient)# **ldap disable**	Disabling ladapclient service

Verifying Network Configuration Settings

Displaying the Status of Configuration Settings

The following basic network configuration by the command displays the default-config status of the Ipnext190.

Table 3-78 show running-config Command

```
Welcome, APOS(tm) Kernel Version 8.47. .024.

Copyright (c) 1999-2008 AddPac Technology Co., Ltd.

IP-PBX# show run

Building configuration...

Current configuration:

!

version 8.47.010

!

hostname IP-PBX

!

username root password router administrator

!

interface Loopback0

 ip address 127.0.0.1 255.0.0.0

!

interface FastEthernet0/0

 no ip address

 speed auto

 no qos-control

!

interface FastEthernet0/1

 no ip address

 speed auto

 no qos-control

!

ftp server

http server

http document-root /hd

! VoIP configuration.
```

```
!!
! Voice service voip configuration.
!
voice service voip
 fax protocol t38 redundancy 0
 fax rate 9600
 h323 call start fast
 h323 call tunnel enable
!
! Voice port configuration.
!
! FXO
voice-port 0/0
 no caller-id enable
!
! FXO
voice-port 0/1
 no caller-id enable
!
! Pots peer configuration.
!
! Voip peer configuration.
!
dial-peer voice 1000 voip
 destination-pattern T
 session target sip-server
 session protocol sip
 no vad
 dtmf-relay dual-mode
 huntstop
!
! Gateway configuration.
!
gateway
 h323-id
 signalling-port 1721
 no ignore-msg-from-other-gk
SIP UA configuration.
```

```
!
sip-ua
 signaling-port 5070
 rport enable
!
! MGCP configuration.
!
mgcp
 codec  g711ulaw
 vad
!
Tones
!
call-manager sip
!
call-manager sscp store-event-time 3
call-manager sscp store-event-count 10
!
call-manager logger disable
call-manager logger level info
!
call-manager h323
 signalling-port 1720
!
! CallManager interface configuration.
!
call-manager interface ip FastEthernet0/0 domain public
call-manager interface ip FastEthernet0/1 domain private
!
rtp-proxy
!
line console
!
line vty
!
character-set encoding usa ascii
mount mem 8192 /apcm
! mount mem 1024 /tmp
```

```
!
ldap
 data-dir /hd/ldap
 suffix "dc=addpac,dc=com"
 rootdn "cn=Manager,dc=addpac,dc=com"
 rootpw secret
 include /hd/ldap/schema/core.schema
 include /hd/ldap/schema/cosine.schema
 include /hd/ldap/schema/inetorgperson.schema
 include /hd/ldap/schema/addpac.schema
 include /hd/ldap/schema/apcm.schema
 include /hd/ldap/schema/apglobal.schema
 include /hd/ldap/schema/apmessage.schema
 include /hd/ldap/schema/apms.schema
 include /hd/ldap/schema/apmd.schema
 include /hd/ldap/schema/apums.schema
!
!  presence server configuration.
!
presence
 service disable
 sscp store-event-time 1
 sscp store-event-count 1
 logger disable
 logger level info
!
! media server configuration.
!
media
 rbt disable
!
ldapclient
 ldap disable
!
end
IP-PBX#
```

Verifying IP, Default Route Configuration Settings

The followings display the network configuration for the basic communication. Use ping test to the default Ipnext190 to check the network connection

Table 3-79 IP, Default Route Configuration Settings

```
IP-PBX# configure terminal
IP-PBX(config)# interface Fastethernet 0/0
IP-PBX(config-if)# ip address 172.17.201.115 255.255.0.0
IP-PBX(config-if)# exit
IP-PBX(config)# ip route 0.0.0.0 0.0.0.0 172.17.1.1
IP-PBX(config)# end
IP-PBX#
IP-PBX#
IP-PBX# write
Proceed with write? [confirm]
Building configuration...
[OK] Configuration saved to flash:/apos.cfg
IP-PBX#
IP-PBX# ping 172.17.1.1
PING 172.17.1.1 (172.17.1.1): 56 data bytes
64 bytes from 172.17.1.1: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 172.17.1.1: icmp_seq=1 ttl=255 time=0 ms
64 bytes from 172.17.1.1: icmp_seq=2 ttl=255 time=0 ms
64 bytes from 172.17.1.1: icmp_seq=3 ttl=255 time=0 ms
64 bytes from 172.17.1.1: icmp_seq=4 ttl=255 time=0 ms

--- 172.17.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss'
round-trip min/avg/max = 0/0/0 ms
IP-PBX#
```

Verifying LDAP Configuration Settings

Table 3-80 Running and Verifying LDAP

* Verifying LDAP Configuration Settings by show run command

```
IP-PBX#
IP-PBX# show run
Building configuration...
Current configuration:
!
hostname IP-PBX
!
username root password router administrator
!
interface Loopback0
 ip address 127.0.0.1 255.0.0.0
!
interface FastEthernet0/0
 ip address 172.17.201.79 255.255.0.0
 speed auto
!
interface FastEthernet0/1
 speed auto
!
-------------------------------skipped--------------------------------
!
! APOS File System
!
mount hdd 0 /hd
mount mem 8192 /apcm
! mount mem 512 /tmp
!
share global
 workgroup WORKGROUP
 encrypt-passwords
 !
```

```
character-set encoding usa ascii

mount mem 8192 /apcm

! mount mem 1024 /tmp

!

ldap

 data-dir /hd/ldap

 suffix "dc=addpac,dc=com"

 rootdn "cn=Manager,dc=addpac,dc=com"

 rootpw secret

 include /hd/ldap/schema/core.schema

 include /hd/ldap/schema/cosine.schema

 include /hd/ldap/schema/inetorgperson.schema

 include /hd/ldap/schema/addpac.schema

 include /hd/ldap/schema/apcm.schema

 include /hd/ldap/schema/apglobal.schema

 include /hd/ldap/schema/apmessage.schema

 include /hd/ldap/schema/apms.schema

 include /hd/ldap/schema/apmd.schema

 include /hd/ldap/schema/apums.schema
```

=> Execute slapd and notification server if 'notification' configuration

is not found

```
!

End
```

* Enable LDAP and Execute Notification Server

```
IP-PBX #

IP-PBX # con t

IP-PBX (config)#

IP-PBX (config)# ldap

IP-PBX (config-ldap)#

IP-PBX (config-ldap)# slapd
```

LDAP daemon is now active.   => Check LDAP active

```
IP-PBX(config-ldap)# notification 5389

IP-PBX(config-ldap)#
```

Start Ldap Notification Server (listen tcp/5389)   => Check the status of LDAP Notification

Server

```
IP-PBX #

IP-PBX #

IP-PBX # show run


--------------------- skipped ----------------------

! !

ldap

 data-dir /hd/ldap

 suffix "dc=addpac,dc=com"

 rootdn "cn=Manager,dc=addpac,dc=com"

 rootpw secret

 include /hd/ldap/schema/core.schema

 include /hd/ldap/schema/cosine.schema

 include /hd/ldap/schema/inetorgperson.schema

 include /hd/ldap/schema/addpac.schema

 include /hd/ldap/schema/apcm.schema

 include /hd/ldap/schema/apglobal.schema

 include /hd/ldap/schema/apmessage.schema

 include /hd/ldap/schema/apms.schema

 include /hd/ldap/schema/apmd.schema

 include /hd/ldap/schema/apums.schema
```
 slapd   **=> Check LDAP status**

 notification 5389   **=> Check LDAP Notification Server status**
```
IP-PBX #

IP-PBX #
```

* The details to be Checked when LDAP does not operate normally

```
IP-PBX #

IP-PBX # fsh

fsh:/>

fsh:/> ll

total(bytes) 33552

drwxrwxrwx 1 root  apos   752 Sep 13  9:10 apcm/

d--------- 1 root  apos     0 Sep 13  9:09 flash/
```
drwxrwxrwx 1 root apos 32768 Sep 13 9:09 hd/
```
drwxrwxrwx 1 root  apos    32 Sep 13 11:36 tmp/

fsh:/>
```

```
fsh:/> cd hd
```

> => For LDAP Recovery, please refer to Smart Multimedia Manager) Check whether ladap data exists in hdd (It is normal when all the settings below exist, but if any setting is missing, LDAP Recovery should be performed)

```
fsh:/hd>
fsh:/hd> ll
d--------- 1 root  apos  2048 Jan 01 12:04 addpac/
d--------- 1 root  apos  2048 Jan 01 12:05 cdr/
d--------- 1 root  apos  2048 Jan 01 12:05 en/
d--------- 1 root  apos  2048 Jan 01 12:06 ko/
d--------- 1 root  apos  2048 Jan 01 12:08 ldap/
drw-rw-rw- 1 root  apos  2048 Aug 21 09:01 lost+found/
d--------- 1 root  apos  2048 Jan 01 12:08 mbox/
d--------- 1 root  apos  2048 Jan 01 12:08 music/
d--------- 1 root  apos  2048 Jan 01 12:08 scenario/
d--------- 1 root  apos  2048 Jan 01 12:08 smartclient/
d--------- 1 root  apos  2048 Jan 01 12:09 storage/
d--------- 1 root  apos  2048 Jan 01 12:12 tone/
d--------- 1 root  apos  2048 Jan 01 12:12 voice/
fsh:/hd> exit
IP-PBX #
IP-PBX #
```

* Configuring and Executing LDAP Client

```
IP-PBX# con t
IP-PBX(config)# ldapclient
IP-PBX(config-ldapclient)# name ipnext190_ldap
IP-PBX(config-ldapclient)# host 127.0.0.1 389
IP-PBX(config-ldapclient)# ldap enable
IP-PBX(config-ldapclient)#
[LDAP_CLIENT] Auto-Registration Complete.device id(56) => Check LDAP Client
```

Upgrading APOS

AddPac Ipnext190 allows connections using the following methods to transfer APOS image files in binary codes. Each network protocol can process or stop providing the features

The network of uploading or downloading the APOS image file saved in the PC to or from AddPac Ipnext190 is configured as follows:
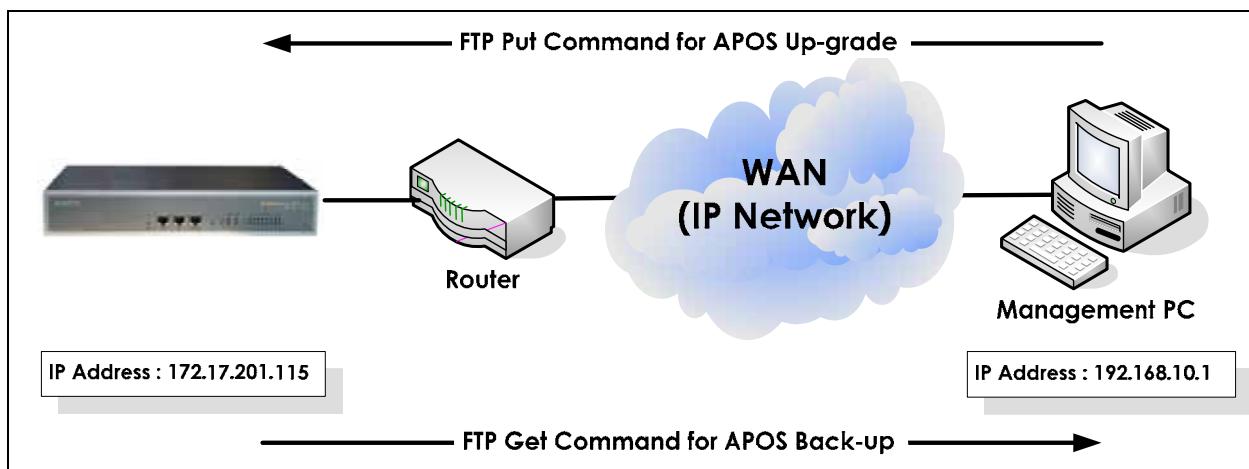

Figure 3-5 APOS Image File Upgrade Using FTP

Enabling FTP Service

Enable FTP from IPNext PBX first to upload/download APOS by using FTP.

Table 3-81 Running FTP

```
IP-PBX# configure terminal

IP-PBX(config)#

IP-PBX(config)# ftp server

IP-PBX(config)# Start File Transfer Protocol Server (listen tcp/21)

IP-PBX(config)#
```

Uploading APOS

Use ftp from DOS window of PC to upload APOS for the Ipnext190. Press 'Start' of the window and enter 'cmd' in Run widow, then DOS window opens up.

Table 3-82 APOS Upgrade (DOS Screen)

```
D:\ >dir

2008-08-14  15:21p     <DIR>          .

2006-08-14  15:21p     <DIR>          ..

2008-08-14  15:21p         5,229,160 ipnext190_g2_v8_47_024.bin


D:\>

D:\> ftp 172.17.113.50     => Access to the server

Connected to 172.17.113.50.

220 IP-PBX FTP server (Version 8.47.010) ready.

User (172.17.113.50:(none)): root

331 Password required for root.

Password:

230 User root logged in.

ftp> binary                => Change to binary mode

200 Type set to I.

ftp> hash                  => Display Hash mark

Hash mark printing On  ftp: (2048 bytes/hash mark) .

ftp> put ipnext190_g2_v8_47_024.bin => ipnext190_g2_v8_47_024.bin  => Upload the file

200 PORT command successful.

150 Opening BINARY mode data connection for 'ipnext190_g2_v8_47_010.bin'.

###########################################################################

------------     -----------

#########################################################################

226 Transfer complete.

ftp: 5229160 bytes sent in 1.92Seconds 2720.69Kbytes/sec.

ftp> quit

221 Goodbye. => Do not reboot the IPNext PBX until the message is displayed as 'The system software is
updated' at the console connected to the IPNext PBX, even after the message of 'Goodbye' is displayed.

D:\>
```

Table 3-83 APOS Upgrade (Console Screen)

```
IP-PBX#
5229160(0x4fca68) bytes are received and version is "8.47.024"    => upgrade
in process
IP-PBX#
IP-PBX#
The "system software" is updated.  => upgrade is completed
```

Chapter 4.   Initializing

When you execute the data initialization of the IPNext190 for the first time or HDD or Flash Memory is damaged by an unexpected failure during its operation, the data needs to be initialized (Call Manager, Announcement File, Database Schema and other basic files).

The following details describe the data initialization process of the IPNext190.

This procedure initializes the entire data and is used when Smart Directory Server is damaged during its operation or a new version needs to be upgraded. Therefore, a precaution is required.

Basic System Configuration

Step1. Initialize

This command initializes all the configuration settings of the IPNext190. Use erase startup-config command to initialize the settings and then reboot the system, so you may enter the initial mode

Table 4-1 Initializing

Step	Command	Description

1	```IP-PBX#```
	
	```IP-PBX# erase startup-config```
	
	```IP-PBX# reboot```
	
	```Proceed with reboot? [confirm]```
	
	```Reboot System ..```
	
	```Please wait few seconds```
	
	```IP-PBX(config)#```
		Use erase startup-config command to initialize
		
		.

Step2. Configure the interface

This example specifies the interface of Fastethernet 0/0 to the IP address of '172.17.111.20'.

Table 4-2 Configuring the interface

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter the APOS command mode
2	IP-PBX(config)# **interface fastethernet 0/0**	Enter the interface configuration mode
3	IP-PBX(config)# **ip address 172.17.111.20 255.255.0.0**	Specify the interface to the IP address of 172.17.111.20

Step3. Configure Default Route

This example specifies the Default Router to the IP address of 172.17.1.1.

Table 4-3 Configuring Default Route

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter the APOS command mode
2	IP-PBX(config)# **ip route 0.0.0.0 0.0.0.0 172.17.1.1**	default route "172.17.1.1"

Configuring System Service

http server

This example enables HTTP Server and Http document-root Directory.

(Default: http server, http document-root /hd)

Table 4-4 Configuring HTTP Server

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter the APOS command mode
2	IP-PBX(config)# **http server**	Enable HTTP server (default)
3	IP-PBX(config)# **no http authentication**	Configure the server to be accessed without HTTP authentication(optional)
4	IP-PBX(config)# **http document-root /hd**	Configure the Default Directory for accessing the web-based SMM. (the default version higher than IPNext190 v8.47.024: /hd) * Change the setting of http document–root to /hd if you need to upgrade a version lower than v8.47.024 to a version higher than v8.47.024 (The default setting of the version older than IPNext50 v8.47.024 : /hd/smartclient)

ftp server

This example enables FTP Server (Default: ftp server, ftp port 21).

Table 4-5 Configuring ftp server

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter the APOS command mode.
2	IP-PBX(config)# **ftp server**	Enable FTP server. (default)

Initializing File System (Optional)

This section presents some examples of the file system for the IPNext190. The configuration settings of this file system, which have been saved in the IPNext190, are completely initialized. So you should backup the data and files to SMM and SMM separately prior to initialization (For backing up to SMM, refer to Smart Multimedia Manager Installation and Operation Guide. For backing up to SMT, refer to IPNext System Maintenance Tool Guide).

Table 4-6 Initializing File System

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter the APOS command mode
2	IP-PBX(config)# **hdd nand format**	Initialize the file system used for the IPNext190 It may take some time to initialize the file system.

Initializing Call-Manager

Step4. Execute and Process Initialization of System Maintenance Tool

For initializing Call Manager, execute the initialization process of System Maintenance Tool (For installation and initialization methods of System Maintenance Tool, please refer to System Recovery and System Initialize in Chapter 2 of the IPNext System Maintenance Tool).

Step5. Configure Presence Server

Enable the service to use Presence Server. Presence Server is disabled at default (To use Presence Server, the IPNext PBX should have (Max Messenger Session) License).

Table 4-7 Configuring Presence Server

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **presence**	Enter Presence Server configuration mode
3	IP-PBX(config)# **presence server**	Enable Presence Server

Step6. Configure Media Server

Enable the service to use Media Server. Media Server is disabled at default.

Table 4-8 Configuring Media Server

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter APOS command entry mode
2	IP-PBX(config)# **media**	Enter Media Server configuration mode
3	IP-PBX(config-media)# **rbt enable**	Enable Media Server service

Step7. Configure Idapclient

When initialization of Call Manager and rebooting are completed by System Maintenance Tool, you are ready to configure Ldapclient for Call-Manager Service.

Table 4-9 Configuring Ldap Client

Step	Command	Description
1	IP-PBX# IP-PBX# **configure terminal** IP-PBX(config)#	Enter the APOS command mode
2	IP-PBX(config)# **ldapclient**	Enter ldapclient configuration mode
3	IP-PBX(config-ldapclient)# **name IPNext190_test**	Configure device name to be registered to ldap
4	IP-PBX(config-ldapclient)# **host 127.0.0.1 389**	Specify the IP and port of ldap server Default IP (127.0.0.1) Default Port (389)
5	IP-PBX(config-ldapclient)# **ldap enable**	Enable ldap Client service

Step8. Verify the Status of Call Manager Service

After the settings of ladapclient is completed, use show call-manager domain cluster command to verify the status of Call Manager service (If CallManger Status is In Service and Monitoring LDAP Connection Status is Enable, the service is in normal operational status).

Table 4-10 Verifying the Status Call-Manager Service

Step	Command	Description
1	IP-PBX# **show call-manager domain cluster** Device pool -------------------------- DevicePool 1 Name = default Region = 1 CallManagerGroup Information - N/A CallManager Status Summary	If CallManager Service is In Service and ldap connection is UP, the service is in the normal operational status

```
--------------------------------------------
----------------------
- Cluster Mode                 : Active
- Monitoring Link Status        : Disabled
- Link Status                  : UP
- Monitoring LDAP Connection Status : Enabled
- LDAP Connection Status        : UP
- On Trunk Initiating          : Yes
- Trunk Initiating Ready        : No
- CallManager Status           : In Service
- Binding Status
…
```

Step9. Access to Web-based SMM

1) Open Internet Explorer and then enter the IP address of the IPNext 190 then press 'Enter' key.
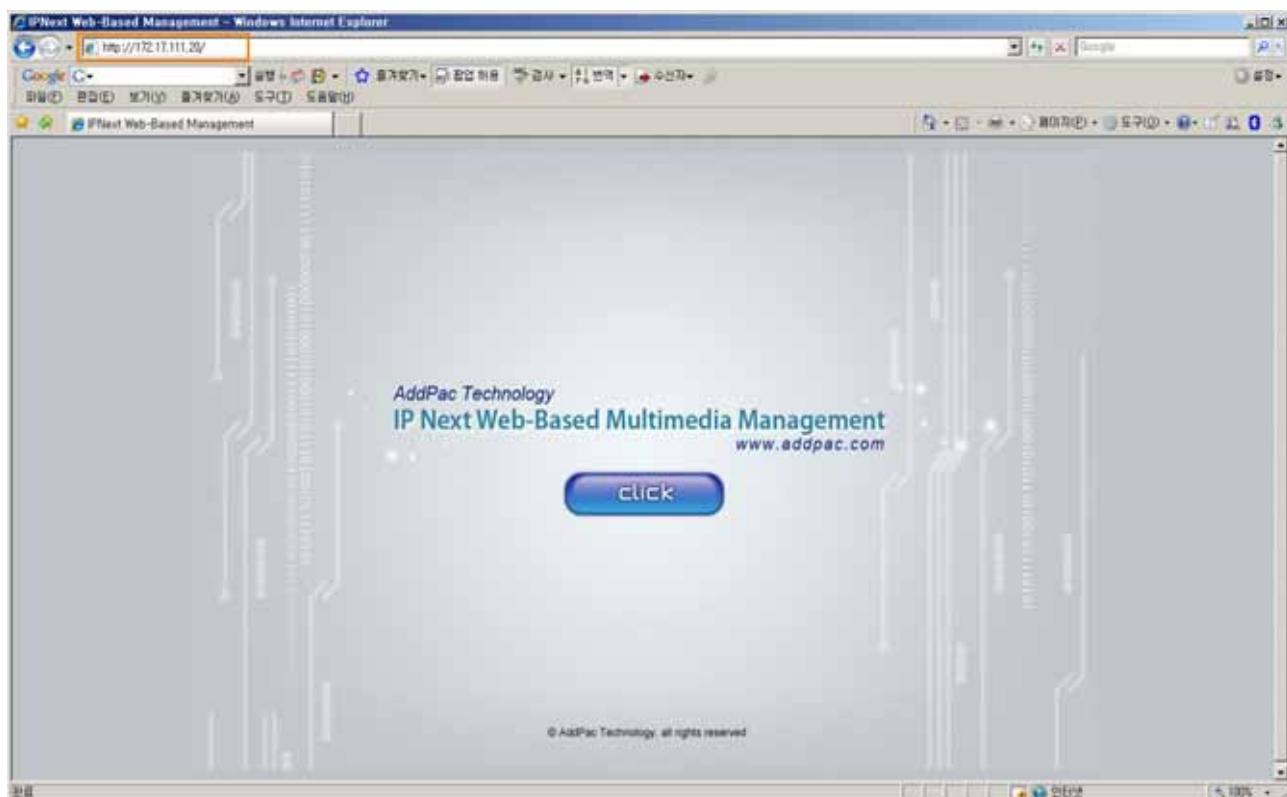
Figure 4-1 Web Based SMM Access Screen 1

2) Press 'Click' to move to LDAP entry screen.
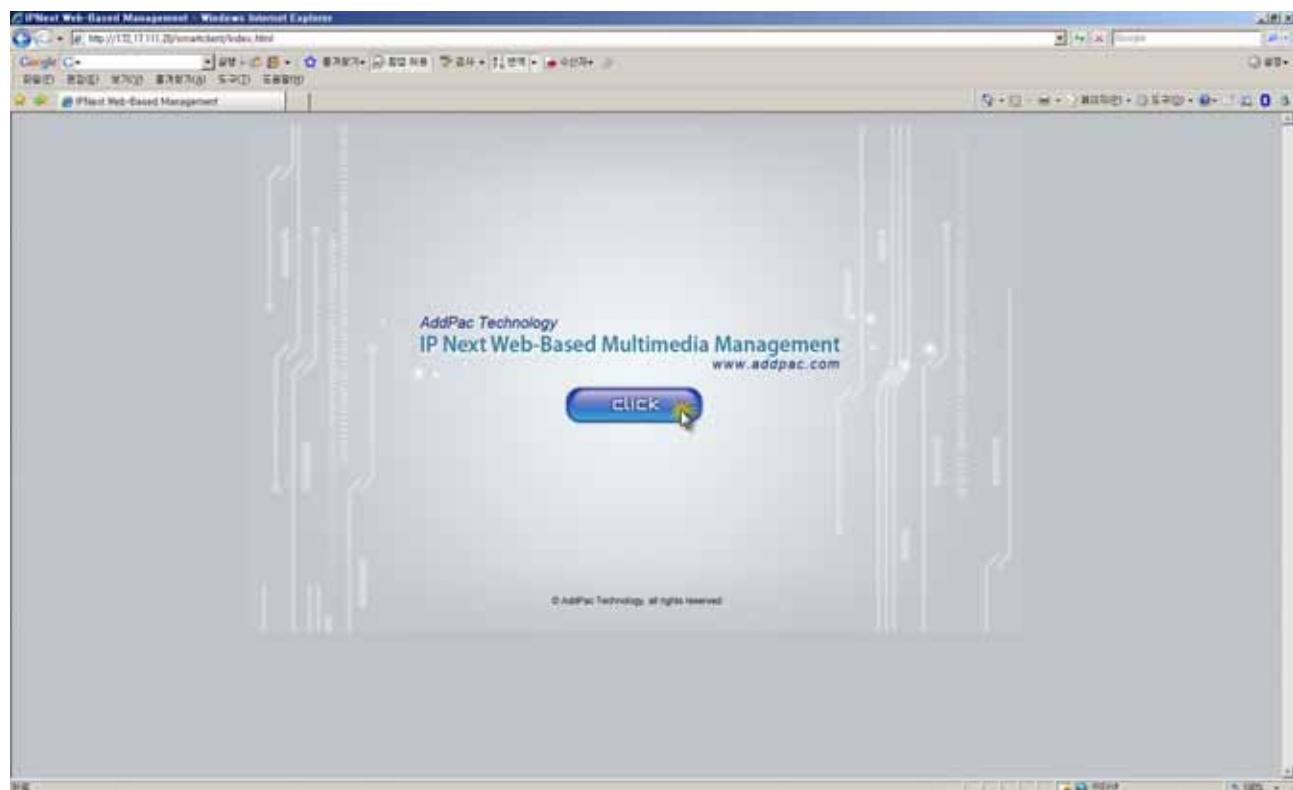
Figure 4-2 Web Based SMM Access Screen 2

3) Enter the ID, Password and Port for accessing to the IPNext190 and click the Login icon (Default ID:root, Default Password: router, Default Port: 389).
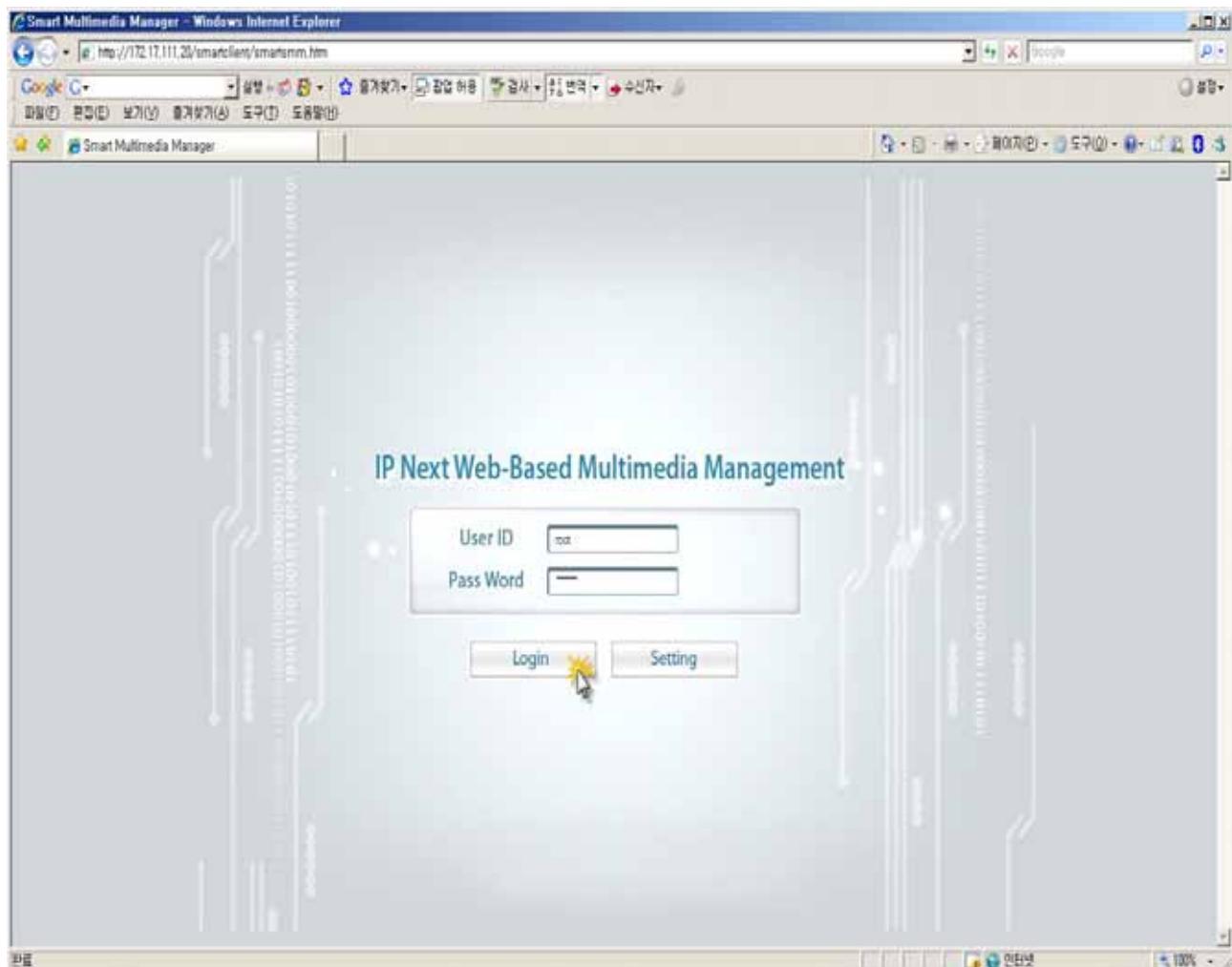

Figure 4-3 Web Based SMM Access Screen 3

4) When the access is completed, the initial main screen is displayed in the following:
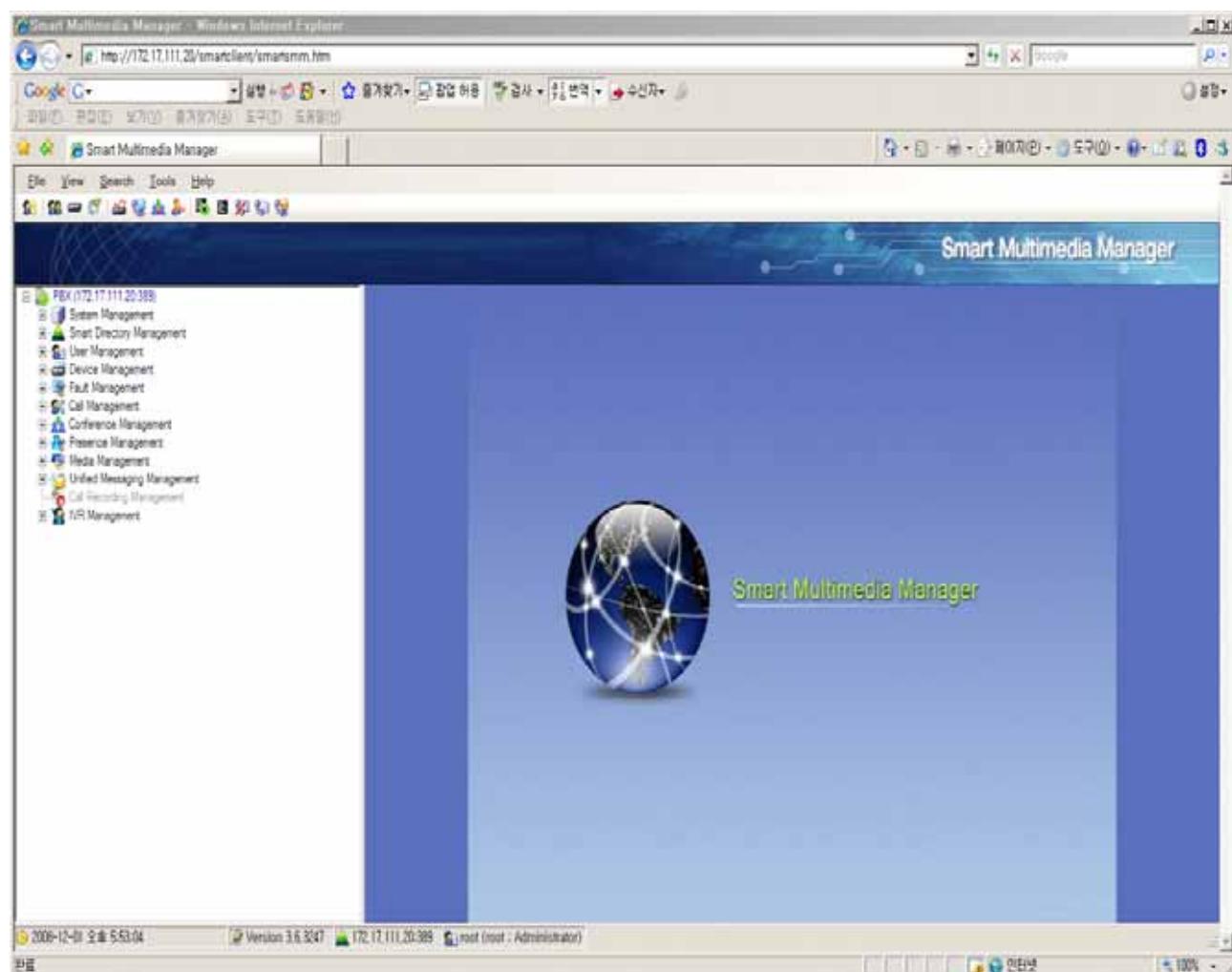

Figure 4-4 Web Based SMM Access Screen 4

Chapter 5.   Appendix

Console Port Signal and Pinout

This Appendix describes the pinout specification of the following cables used for AddPac IP-
PBX:

- Console port signals and pinout (RJ-45 to DB9)
- Pinout of UTP cable assembly (RJ-45 to RJ-45)

The built-in RJ-45 to DB9 (Female DTE Connector) cable is used to connect the console port
of the Ipnext190 system with the PC where the terminal emulation software operates.

Table 5-1 Console Port Pinout

Console Port (DTE)	RJ-45	DB-9	Console Device (PC)
Signal	RJ-45 Pin	DB-9 Pin	Signal
RTS	1	8	CTS
DTR	2	6	DSR
TxD	3	2	RxD
GND	4	5	GND
GND	5	5	GND
RxD	6	3	TxD
DSR	7	4	DTR
CTS	8	7	RTS

Pinout of UTP Cable (RJ-45 to RJ-45)

The RJ-45 to RJ-45 Ethernet cable is used to connect the Ipnext190 with another device (typically hub). The sequence of the RJ-45 connector pins is shown in below figure. For the signals between the IPNext190 with another device and pinout specification, refer to Figure 4-1, "Signals and Pinout of Serial Ethernet Cable".
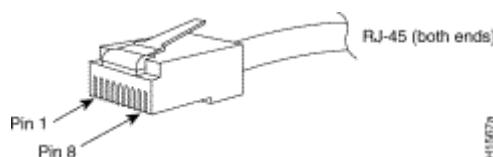

Figure 5-1 100Base-TX RJ-45 Connector

**Table 5-2 Signals and Pinout of Serial Ethernet Cable**

RJ-45	Signal	Direction	RJ-45 Pin
1	**Tx +**	→	1
2	**Tx -**	→	2
3	**Rx +**	←	3
4	**-**	**-**	4
5	**-**	**-**	5
6	**Rx -**	←	6
7	**-**	**-**	7
8	**-**	**-**	8

1. The table above shows the specification of serial cables that connect the IPNext190 with the hub.

2. If you want to connect an IP-PBX with another IP-PBX or the gateway with the PC, you should use cross cables.

Pinout of E1/T1 Cable (RJ-45 to PBX)

The AddPac E1/T1 module can be connected by RJ-45 cable. As the pinout of RJ-45 shown below, connect RX of the PBX to the pin 1 and 2 and TX to the number 3, 4.

TX_RING(pin 5)
TX_TIP(pin 4)
RX_RING(pin 2)
RX_TIP(pin 1)
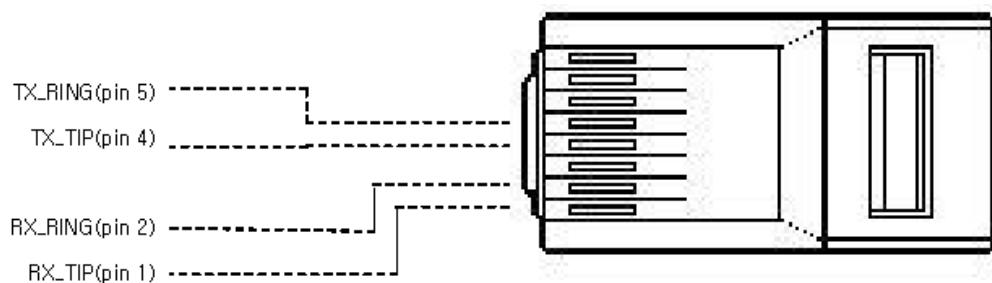
Figure 5-2 Digital E1/T1 RJ-45 Pinout

Abbreviation and Glossary

Glossary and Abbreviation	Definition
ADSL	Stands for Asymmetric Digital Subscriber Line. If you use ADSL, the central office will be connected to each home directly in a 1:1 method. In a down-link where data is transferred downward from the central office to the users, high-speed data communications of at least 1.5 Mb can be made. On the contrary, in an up-link from the users to the central office, communications are made very slowly. Thus, this service is called an asymmetrical service not a symmetrical service.
AP-VPMS	Stands for VoIP Plug & Play Management Software. This integrated management software developed by AddPac Technology enables VoIP products to be installed in a GUI environment, be monitored in real-time, or to be upgraded. This software also enables network administration.
API	Stands for Application Programming Interface. API is a function call legend standard that defines service interfaces.
APOS	Stands for AddPac Internetworking Operation System. This is an operating system that supports the network products developed by AddPac Technology.
ATM	Stands for Asynchronous Transfer Mode. This is an international cell relay standard for providing a variety of services such as voice, video, and data in the form of a cell of a fixed length (53 bytes). If you use a fixed-length cell, cell processing will be performed in the hardware; thus, transmission delay can be reduced. ATM is designed to make use of high-speed transmission media such as E3, SONET, and T3.
ATM High-Speed National Network	This network has been commercialized by the Korean government since 1993. The high-speed national network designed for governmental offices provides data services (transport network services) and Internet services. Data services are categorized into ATM, dedicated lines, packet exchange, and frame relay services. Internet services are categorized into Internet multi-services provided through ATM connection circuits and simple Internet services.
ATM Forum	This is an international organization founded by Cisco Systems, NET/ADAPTIVE, Northern Telecom, and Sprint in 1991 to reach the agreement of a standard for ATM technologies. ATM Forum expands the formal standards developed by ANSI and ITU-T and the agreements on the implementation of technologies.

Authentication	Operation of verifying the identification of a person or a process. This is a security feature.
BNC Connector	This is a standard connector used to connect IEEE 802.3 10Base-2 coaxial cables to Media Access Unit (MAU).
Boot Loader	This is a chip installed into a printed circuit board used to send executable boot commands to a network device.
Bps	Stands Bits per second. Typically called bps. Refer to bit rate.
Cable Modem	This device converts analog signals to digital signals in order to enable the Internet through a cable network. Since telephone networks are made of copper wires and cable networks are made of coaxial and optical cables, the bandwidth of cable networks are much wider than that of telephone networks. However, the modulation/demodulation technology, which converts digital to analog and vice versa, is required for cable networks when data is transferred.
Call Center	Call Center is a central place where calls from customers and other people are processed systematically. Computer automation is implemented in Call Center to some degree. Typically, Call Center processes many calls simultaneously, categorizes calls, connects the calls to personnel, and records calling logs automatically. Call Center is typically used for mail order catalog firms, telemarketing firms, customer centers for PC products, and large enterprises that sell products or provide services.
Caller ID	Caller ID is a call service that enables the phone number of the caller to be sent to the recipient. To see the phone number, a digital reader should be installed into the phone.
Category 5 cabling	One of the five-level UTP cable connection methods specified by the EIA/TIA-586 standard. Category 5 cabling enables data to be transferred at a rate of up to 100Mbps.
CBR	Stands for Constant Bit Rate. The ATM network QoS class CBR defined by ATM Forum is used for a connection device that is based on a precise clock processing method to ensure untwisted data transfer.
CES	Stands for Circuit Emulation Service. This service allows you to multiplex multiple line emulation streams for voice and video with packet data through a single high-speed ATM link without using a separate ATM access multiplexer.
Checksum	This is a method for checking the integrity of transferred data. Checksum is an integer calculated from the octet sequence obtained by a series of operations. This value is calculated by the recipient again for verification.
Coaxial cable	This coaxial cable is made of an external cylinder-type conductor that wraps an internal wire conductor. Examples of the coaxial cables used for LAN include 50Ω cables used for digital signal processing and 75Ω cables used for high-speed digital signal processing.

CODEC	Stands for COder-DECoder. CODEC is: 1. A built-in circuit device that converts analog signals to digital bit streams and vice versa based on a pulse code modulation method; 2. A DSP software algorithm that compresses or decompresses voice or audio signals over Voice over IP, Voice over Frame Relay, or Voice over ATM.
Console	A DTE interface through which a command enters a host
CoS	Stands for Class of Service. CoS refers to the standard method that enables a higher-level protocol to make a lower-level protocol process messages. For the SNA lower-level area routing, CoS is used to determine the optional path for lower-level area nodes to set a given session. CoS consists of a virtual path number and a transmission priority field. Also called ToS
Decryption	Decryption means restoring data to the original non-encrypted state by applying the encryption algorithm to the encrypted data in reverse.
DHCP	Stands for Dynamic Host Configuration Protocol. DHCP has a mechanism that reassigns an IP address dynamically in order for the host to recycle unnecessary IP addresses.
DNS	Stands for Domain Name Server. This is a server system used for the Internet to convert the name of a network node name to an address.
DS-3	Stands for Digital Signal level 3. This is a frame processing standard used to transmit digital signals at a rate of T3 (44.736Mbps).
DSP	Stands for Digital Signal Processor. This is a dedicated processor that processes only digital signals. DSP is used as a sub-processor for voice processing in NEXT.
DTMF	Stands for Dual Tone MultiFrequency. Two voice-band tones are simultaneously used for dialing (just like touch tones).
E&M	Stands for either recEive and transmit or Ear and Mouth. Typically, this is a trunking device used for switch-to-switch or switch-to-network two-way communications. The analog E&M interface of Cisco is a RJ-48 connector for PBX trunk lines. E&M is available for E1/T1 digital interfaces.
E1	This is a wide area digital transmission technique used mainly in Europe. E1 enables data transfer at a rate of 2,048Mbps. E1 can be lent by regular service providers for a private use.
Encryption	Encryption means that a specific algorithm is applied to data in order to convert data to a form that unauthorized users cannot identify.
Ethernet	Baseband LAN standard initiated by Xerox Corporation and co-developed by Xerox, Intel, and DEC. CSMA/CD is used for Ethernet networks, which operate through a variety of cables at a rate of 10Mbps. Ethernet is similar to the IEEE 802.3 standard. Refer to 10Base-

	2, 10Base5, 10Base-F, 10Base-T, 10Broad-36, Fast Ethernet, and IEEE 802.3.
FAX	Abbreviation of Facsimile. FAX refers to the transmission of scanned texts or images to a printer or an output device connected to another phone number by using a telephone line. Once the original document is read by a facsimile, the facsimile treats the document as a fixed graphic image, and converts it to bitmap. In this digital form, data is transferred in the form of an electrical signal through a phone system. The receiving facsimile restores the data to a encoded image, and prints it on a sheet of paper.
Frame	Logical group of data transferred to a data link layer unit through a transmission medium. From frames, the header and trailer that include user data are important. Headers and trailers are used for synchronization and error control. Cells, datagrams, messages, packets, and segments are used to describe logical data groups in various layers of OSI or based on various technologies.
Frame-Relay	This is an industry-standard switching-type data link layer protocol that processes multiple virtual lines in inter-connected devices by using the HDLC encapsulation. Frame-Relay is more efficient than X.25.
FTP	Stands for File Transfer Protocol. FTP, which is an application protocol, is part of the TCP/IP protocol stack used for file transfer between network nodes. FTP is defined in RFC 959.
FXO	Stands for Foreign Exchange Office. The FXO interface is connected to the switching center of Public Switched Telephone Network (PSTN), and is provided by a regular phone. The FXO interface of Cisco is a station interface of the switching center or PBX on PSTN, and is a RJ-11 connector for analog connection devices.
FXS	Stands for Foreign Exchange Station. The FXS interface is directly connected to a standard phone, and provides a ring-back tone, voltage, and a dial tone. The FXS interface of Cisco is a RJ-11 connector for basic telephone service devices, keyset, and PBX.
G.711	This specifies the PCM voice coding technique of 64Kbps. Voice is encoded under G.711 in an appropriate format that enables digital voice transmission over either PSTN or PBX. G.711 is specified under the ITU-T standard of G-series recommendation.
G.723.1	This is one of the H.324 standards, and specifies a compression technique that enables voice or audio signal elements to be compressed at a very low bit transmission rate. This CODEC is related to the bit transmission rates of 5.3Kpbs and 6.3Kpbs. The high bit transmission rate is based on the MLMLQ technology, and provides high quality sounds. The low bit transmission rate is based on CELP, and ensures high flexibility for system designers. This standard is specified under the G-series ITU-T standard.

G.726	This standard specifies ADPCM coding performed at a rate of 40Kbps, 32Kbps, 24Kbps, or 16Kbps. If the PBX network is configured to support ADPCM, you can exchange ADPCM encoding voice with packet voice networks, PSTN, or PBX networks. This standard is specified under the ITU-T standard of G-series recommendation.
G.728	This standard specifies variations that ensure low delay of CELP voice compression performed at 16Kbps. The CELP voice coding should be converted to a public telephony format for transmission over either PSTN or PSTN. This standard is specified under the ITU-T standard of G-series recommendation, and defines the CELP compression that encodes G.729 voice to a stream of 8Kbps. G.728 has two variations (G.729 and G.729 Annex A), and the variations are different in terms of calculation complexity. The two variations have voice quality similar to ADPCM of 32Kbps. G.728 is specified under the ITU-T standard of G-series recommendation.
Gatekeeper	This is the component of the H.323 video conference system that analyzes a caller ID, controls access authorization, and manages the subnet bandwidth. A gatekeeper is H.323 entity that provides the features that enable address conversion and LAN access control to the H.323 terminal and gateway on LAN. Gatekeepers can provide other services such as bandwidth control and search for a gateway to the H.323 terminal and gateway. This device manages a device registry on a multimedia network. The devices are registered with the gatekeeper, and they request the gatekeeper to authorize a call.
H.225	This ITU standard is applied to the session setting and packetization of H.225.0. H.225.0 specifies a variety of protocols such as RAS, Q.931, and RTP.
H.245	This ITU standard is applied to H.245 endpoints control.
H.323	This standard is an extension of the ITU-T standard H.320 that enables voice conferences over LAN or another packet switching network as well as video transmission over the Internet.
HBD3	This is a type of line codes used for E1.
HDLC	Stands for High-Level Data Link Control. HDLC is a transmission protocol used in the data link layer, which is the second layer of the 7-layer OSI model. HDLC is used in the X.25 packet switching network. Data consists of frames in HDLC, and frames are transmitted through a network. The destination verifies if the frames have been successfully transmitted. The HDLC protocol includes data for controlling data flow and troubleshooting errors in a data frame.
Hookflash	This is a short on-hook duration of a device such as phones during a call. Hookflash means that a phone attempts to make a dial tone recall through PBX. This is usually used to

	perform call transfer.
HTTP	Stands for Hypertext Transfer Protocol. This protocol enables a Web browser or a Web server to transfer files such as text files and graphic files.
IPSec	Stands for Internet Protocol Security protocol. IPSec is a still developing standard for the security of networks or the packet processing layer of network communications. In the previous security techniques, security has been included in the application layers of a communication model. IPSec is particularly useful for the implementation of remote user access through dial-up access to Virtual Private Networks (VPN) and regular private networks. The main advantage of IPSec is that security can be ensured without replacing an individual user PC with a new one. Cisco takes the initiative of suggesting IPSec as the standard, and has embedded support to this feature into its network router.
IPv6	IPv6 is the latest IP, and has been embedded into part of IP support into many products including the operating systems of PC. IPv6 is called IP Next Generation (IPng), that is the next-generation IP. IPv6 is the formal IETF standard. IPv6 is designed as an evolutional version of the currently used IP version 4. Network hosts or intermediate nodes that adopt either IPv4 or IPv6 can process any packets formulized by either IPv4 or IPv6; thus, the users and service provides can upgrade their IP to IPv6 individually without collaboration.
ISP	Stands for Internet Service Provider. ISP refers to service providers that provide Internet access services, Web site construction and Web hosting services to individuals or enterprises. ISP has devices and communication lines required for Internet access, and large ISPs have their own high-speed dedicated lines in order to provide services that have better quality and are less dependent on telephone network service providers to their customers. The large nationwide ISPs of the U.S. are AT&T WorldNet, IBM Global Network, MCI, Netcom, UUNet, and PSINet. Those of Korea are INet, Channeli, Netsgo, and Netian. The users access the Internet through online service providers. The main online service providers of the U.S. are America Online and Compuserve, and those of Korea are Chollian, Unitel, and Hitel.
ITU-T	Stands for International Telecommunication Union Telecommunication Standardization Sector. This is an international organization that develops global standards on communication technologies. ITU-T performs the previous tasks of CCITT.
IVR	Stands for Interactive Voice Response. IVR refers to a system that provides data in the form of recorded messages through phone lines as a response to user input in the form of human voice or mainly DTMF signal processing. Examples are banks that allow you to check balance by using a phone or automated stock quotations system.

LAN	Stands for Local Area Network. This is a low-error, high-speed data network that covers relatively small geographical areas of up to several thousand meters. LAN inter-connects workstations, peripherals, terminals, and other devices in a building or a geographically limited area. The LAN standard specifies a cable connection and signal processing method in the physical layer and data link layer of the OSI model. Reference: MAN, WAN.
Link	This is a network communication channel configured with lines or a transmission path between the transmitter and receiver and related devices. A link mainly refers to WAN connections, and is sometimes called a line or a transmission link.
Loopback Test	This test is performed as follows: Transmit a signal or return it to the transmitter at a location on the communication path. This loopback test is usually performed to test the availability of network interfaces.
MAC Address	Stands for Media Access Control Address. This is a standard data link layer address required for any and all ports and devices connected to LAN. Other devices on a network use this address to locate a specific port within the network and to create or update a routing table and data structure. A MAC address is 6 bytes long, and is managed by IEEE. A MAC address is called as a hardware address, a MAC-layer address, or a physical address. Compare to: Network Address
MAN	Stands for Metropolitan-Area Network. This network covers the entire area of a large city. The operation area of MAN is geographically larger than that of LAN; however, is smaller than that of WAN. Compare to: LAN, WAN.
MGCP	MGCP, which is also known as H.248 or Megaco, is a standard protocol required to operate signals required during a multimedia conference or to manage sessions. This protocol defines a method of communications between the media gateway that converts the data format required for a circuit switching network to the one required for a packet switching network and the media gateway control device. MGCP may be used to set up, manage, and complete calls among multiple endpoints. Megaco and H.248 are the improved version of MGCP.
NAT	Stands for Network Address Translation. NAT is a mechanism for reducing the need for globally unique IP addresses. NAT allows you to access the Internet as an organization whose address is not globally unique converts the address to an address space where the address can be globally routed. NAT is also called Network Address Translator.
NTP	Stands for Network Time Protocol. NTP, which is built based on TCP, sets a local time accurately based on a wireless clock and an atomic clock on the Internet. NTP can synchronize a distributed clock in the unit of milliseconds for a long time.

PABX	Stands for Private Automatic Branch eXchange. PABX is a switch for phones used at enterprises. PABX is used in Europe, while PBX is used in the U.S.
Packet	A packet is a group of logical data that contains user data and a header where control data is contained. A packet mainly refers to the unit of network layer data.
PBX	Stands for Private Branch eXchange. PBX, which is located in a subscriber building, is a digital or analog phone switchboard used to connect private networks to public phone networks.
PING	Stands for Packet INternet Groper. ICMP echo-processes a response between messages. PING is used for an IP network to test the accessibility of network devices.
Point to Point Connection	One of the two basic connection types. In ATM, the point to point connection may be either a one-way connection or a two-way connection between two ATM end systems.
Pont to Multipoint Connection	One of the two basic connection types. In ATM, the point to multipoint connection is a one-way connection method that enables a transmitting end-system (root node) to be connected to multiple receiving end-systems (riff). Compare to: Point to Point Connection
POTS	Stands for Plain Old Telephone Service. Reference: PSTN.
PPP	Stands for Point-to-Point Protocol. This protocol is the advanced version of SLIP that enables a router-to-router connection or a host-to-network connection through synchronous or asynchronous lines. SLIP is designed to be used on an IP, while PPP is used along with network layer protocols such as IP, IPX, and ARA. PPP has a bulletin board security mechanism such as CHAP and PAP. PPP has two sub-protocols, LCP and NCP. Reference: CHAP, LCP, NCP, PAP, and SLIP
Protocol Stack	This is a collection of communication protocols that inter-work with one another and that process communications in part or all of the seven layers of the OSI reference model. All protocol stacks are not related to each layer of the OSI model, and one protocol of a stack can process multiple layers at one time. TCP/IP is a typical protocol stack.
PSTN	Stands for Public Switched Telephone Network. PSTN is a general term that refers to various telephone networks and services used worldwide. PSTN is also called POTS.
PVC	Stands for either Permanent Virtual Circuit or Permanent Virtual Connection. PVC is a virtual circuit installed permanently. PVC allows you to reduce a bandwidth for setting up or releasing a circuit when a specific virtual circuit must always exist. As an ATM term, PVC is called Permanent Virtual Connection.
Q.931 Signaling	This is an ITU standard that specifies ISDN signal processing methods. The H.225.0 standard uses a variation of Q.931 to set up or disconnect the session of H.323.
QoS	Stands for Quality of Service. QoS is the criterion of measuring the performance (e.g.

	transmission quality and service availability) of a transmission system.
RAM	Stands for Random-Access Memory. RAM is a volatile memory that can be read or written by a microprocessor.
RAS	RAS refers to a protocol for registration, connect acknowledgement, and status protocol. RAS is used for H.323 to find or have a conversation with a gateway.
RISC	Stands for Reduced Instruction Set Computing.
Router	This is a network layer device that determines the optional route to which network traffic is delivered by using one or more metrics. A router forwards packets from a network to another network based on the network layer information. A router is sometimes called a gateway. (A gateway in this meaning is getting older.) Compare to: Gateway; Reference: Relay
RS-232	This is a frequently used physical layer interface, and is known as EIA/TIA-232 nowadays.
RTCP	Stands for RTP Control Protocol. This protocol monitors the QoS of IPv6 RTP connections, and transfers data on sessions in operation. Reference: Real-Time Transport Protocol (RTP)
RTP	1. Stands for Routing Table Protocol. This VINES routing protocol based on RIP distributes network topology data, and helps the VINES server that searches for adjoining clients, servers, and routers. A delay time is used as a routing metric. Reference: SRTP 2. Stands for Rapid Transport Protocol. RTP provides facing and error recovery services to the APPN data when the data passes the APPN network. RTP allows you to check error recovery and flow control synthetically. RTP does not recover but prevents traffic congestion. 3. Stands for Real-Time Transport Protocol. This is one of the IPv6 protocols. RTP is designed to enable the synthetic network transmission feature in the application that transfers real-time data such as audio, video, and simulation data through multicast or unicast network services. RTP enables the real-time application to identify a payload type, specify a sequence number, perform time-stamping, and to monitor a transmission procedure.
SIP	Stands for Session Initiation Protocol. SIP is an application layer control protocol based on very simple texts, and allows more than one user to make, correct, or complete a session. Examples of sessions include remote conferences, phones, meetings, event notifications, and instant messaging on the Internet. SIP is independent to lower-level packet protocols (e.g. TCP, UDP, ATM, and X.25).
SmartViewer	This is software that allows you to monitor AP-GK1000, AP-GK2000, and AP-GK3000, which are the gatekeeper series of AddPac Technology, in a Graphical User Environment

	(GUI) environment in real-time and to search or manage statistical data.
SNMP	Stands for Simple Network Management Protocol. This is a network management protocol almost dedicated to TCP/IP networks. SNMP monitors and controls network devices, and manages setup, collection of statistical data, operation performance, and security features. Reference: SGMP and SNMP2

AddPac Technology Co., Ltd.
Floors # 2 and 3, Jeong Am Bldg., 769-
12, Yoksam-dong, Kangnam-ku, Seoul
Phone (02) 568-3848 (Rep.)
Facsimile (02) 568-3847
E-mail Address: info@addpac.com
http://www.addpac.com