

SmartNode[™] 100 Series **Analog Telephone Adapter**

User Manual



This is a Class B device and can be used in residential locations.

Sales Office: +1 (301) 975-1000
Technical Support: +1 (301) 975-1007
E-mail: support@patton.com
WWW: www.patton.com

Part Number: 07MSN100-UM, Rev. A
Revised: October 27, 2017

Patton Electronics Company, Inc.

7622 Rickenbacker Drive
Gaithersburg, MD 20879 USA

Tel: +1 (301) 975-1000

Fax: +1 (301) 869-9293

Support: +1 (301) 975-1007

Web: www.patton.com

E-mail: support@patton.com

Trademark Statement

The term *SmartNode* is a trademark of Patton Electronics Company. All other trademarks presented in this document are the property of their respective owners.

Copyright © 2017, Patton Electronics Company. All rights reserved.

The information in this document is subject to change without notice. Patton Electronics assumes no liability for errors that may appear in this document.

Warranty Information

Patton Electronics warrants all SmartNode components to be free from defects, and will—at our option—repair or replace the product should it fail within one year from the first date of the shipment.

This warranty is limited to defects in workmanship or materials, and does not cover customer damage, abuse or unauthorized modification. If the product fails to perform as warranted, your sole recourse shall be repair or replacement as described above. Under no condition shall Patton Electronics be liable for any damages incurred by the use of this product. These damages include, but are not limited to, the following: lost profits, lost savings and incidental or consequential damages arising from the use of or inability to use this product. Patton Electronics specifically disclaims all other warranties, expressed or implied, and the installation or use of this product shall be deemed an acceptance of these terms by the user.

Summary Table of Contents

- 1 General information 15
- 2 Installation 22
- 3 Quick Start 29
- 4 SmartNode ATA Home 46
- 5 Network Settings 53
- 6 VoIP Settings 61
- 7 Security Settings 112
- 8 Maintenance Settings 119
- 9 Contacting Patton for assistance 133
- A Compliance Information 136
- B Specifications 139
- C Example Applications 143
- D FAQ List 146

Table of Contents

Summary Table of Contents	3
Table of Contents	4
List of Figures	8
List of Tables	10
About This Guide	11
Safety when working with electricity	12
Deutsch	13
General observations	14
1 General information	15
Overview	16
Features	16
Front Panel LED Indicators & Rear Panels	16
Front panel LEDs	16
Rear panel connectors	19
2 Installation	22
Introduction	23
Installing the SN101/1JS/E (1 FXS port) ATA	23
Package contents	24
Connecting the ATA to a computer	24
Connecting the ATA to a cable/DSL modem or router	25
Connecting the ATA to a telephone or fax machine	25
Connecting power to the ATA	25
Installing the SN102/2JS/E (2 FXS ports) ATA	25
Package contents	25
Connecting the ATA to a computer	26
Connecting the ATA to a cable/DSL modem or router	26
Connecting the ATA to telephones or fax machines	26
Connecting power to the ATA	26
Installing the SN102/1JS1JO/E (1 FXS port and 1 FXO ports) ATA	26
Package contents	27
Connecting the ATA to a computer	27
Connecting the ATA to a cable/DSL modem or router	27
Connecting the ATA to a telephone or fax machine	27
Connecting the ATA to the PSTN or a PBX	27
Connecting power to the ATA	27
3 Quick Start	29
Introduction	30
Configuring the SN100 to communicate with your computer	30
Wizard Setup window	31

WAN Port Type set up.....	34
VoIP set up	35
Configuring SN101/1JS/E (1 FXS) ATA VoIP settings	36
Configuring SN102/2JS/E (2 FXS) ATA VoIP settings	39
Configuring SN102/1JS1JO/E (1 FXS/1 FXO) ATA VoIP settings	42
4 SmartNode ATA Home	46
Introduction	47
Accessing the home window	47
System Status pane	49
Device information	50
System status	50
Interface status	51
Summary status	51
VoIP status	51
Network, VoIP, Security, and Maintenance Menu	52
5 Network Settings	53
Introduction	54
WAN Interface.....	54
Static IP	55
DHCP client	56
PPPoE	56
L2TP with WAN	57
LAN Interface	57
NAT Port Forwarding.....	59
6 VoIP Settings	61
Introduction.....	63
SIP	63
Configuring SN101/1JS/E (1 FXS) ATA SIP settings	63
Configuring SN102/2JS/E (2 FXS) ATA SIP settings	75
Configuring SN102/1JS1JO/E (1 FXS/1 FXO) ATA SIP settings	87
Phone.....	99
Analog Phone window	100
Common window	105
Region window	106
Phone Book.....	107
Speed Dial window	109
Dial Plan with URL window	109
PSTN Line.....	111
7 Security Settings	112
Introduction.....	113
Firewall.....	113
Configuring IP Filtering settings	113

	Configuring MAC Filtering settings	114
	Configuring Port Filtering settings	115
	Content Filter.....	116
	ACL Setting	117
8	Maintenance Settings	119
	Introduction.....	120
	System.....	120
	Configuring General System settings	120
	Configuring Administrator Account's user name and password	121
	Configuring User Account's user name and password	122
	Configuring Time settings	122
	Setting the time manually	123
	Configuring Auto Provision settings	123
	Configuring Dynamic DNS settings	124
	Configuring TR069 settings	125
	Tools.....	127
	Configuration settings	127
	Upgrading SN100 firmware	129
	Running a Ping Test	130
	Performing an SN100 software restart	130
	Logs.....	131
9	Contacting Patton for assistance	133
	Introduction.....	134
	Contact information.....	134
	Warranty Service and Returned Merchandise Authorizations (RMAs).....	134
	Warranty Coverage	134
	Out-of-Warranty Service	134
	Returns for Credit	134
	RMA Numbers	135
	Shipping Instructions	135
A	Compliance Information	136
	Regulatory Information.....	137
	EMC Directive	137
	Low-Voltage Directive (Safety)	137
	PSTN	137
	Radio and TV Interference (FCC Part 15)	137
	CE Declaration of Conformity.....	137
	Authorized European Representative	137
	Service.....	138
B	Specifications	139
	Telephone features.....	140
	DTMF Function	140

Fax Modes.....	140
IP Specifications	140
Call Features.....	141
Network and Security.....	141
Configuration/Management.....	141
Interfaces	141
Operating Temperature.....	141
Power	142
Dimensions and Weight.....	142
Certifications.....	142
C Example Applications	143
ATA with SIP Server Application	144
ATA Peer to Peer Call (IP Domain Call) Application.....	145
D FAQ List	146
Q: What is the default administrator username and password to log in to the SN100?.....	147
Q: I forgot the administrator password. What should I do?	147
Q: Why is it that I can ping outside hosts, but not access Internet Web sites?.....	147
Q: What is the maximum number of IP addresses that the DHCP server of the gateway can assign to local PCs?	147
Q: Why can't I call out from the SN100?.....	147
Q: Why can't I use the Web Interface to configure the SN100?	147
Q: Why does one-way talk happen?.....	147
Q: Why can't I call out when the SN100 under the NAT?.....	147

List of Figures

1	SN101/1JS/E ATA front panel	17
2	SN102/2JS/E ATA front panel	17
3	SN102/1JS1JO/E ATA front panel	18
4	SN101/1JS/E ATA rear panel	19
5	SN102/2JS/E ATA rear panel	20
6	SN102/1JS1JO/E ATA rear panel	20
7	Typical SN100 Series applications	23
8	SN100 ATA cables and 12VDC/1A power adapter	24
9	Login window	30
10	Please select Wizard or Advanced mode window	31
11	Wizard Setup window	31
12	Welcome to the Connection Wizard window	32
13	Time Zone Setting window	33
14	WAN Interface Setting window	34
15	Setting Internet interface message window	35
16	VoIP Configuration window	36
17	Congratulations! window	37
18	REG Status table	37
19	SN101/1JS/E ATA home window	38
20	VoIP Configuration - Phone 1 window	39
21	VoIP Configuration - Phone 2 window	40
22	Congratulations! window	41
23	REG Status table	41
24	SN102/2JS/E ATA home window	42
25	VoIP Configuration - Phone 1 window	43
26	Congratulations! window	44
27	REG Status table	44
28	SN102/1JS1JO/E ATA home window	45
29	SmartNode ATA home window	47
30	Login window	48
31	Please select Wizard or Advanced mode window	48
32	System Status pane	49
33	Device Information window	50
34	System Status window	50
35	Interface Status window	51
36	Summary Status window	51
37	VoIP Status window	51
38	Network, VoIP, Security, and Maintenance Menu	52
39	Displaying sub-categories	52
40	Network sub-categories	54
41	Internet Connection window	54
42	LAN setup window	58
43	DHCP Table window	59
44	Port Forwarding window	60
45	SN101/1JS/E VoIP sub-categories	63
46	SN101/1JS/E SIP Settings window	64
47	QoS window	64

48	Edit SIP Settings window	66
49	Advanced Edit SIP Settings window	69
50	SN102/2JS/E VoIP sub-categories	75
51	SN102/2JS/E SIP Settings window	75
52	QoS window	76
53	Edit SIP Settings window	78
54	Advanced Edit SIP Settings window	81
55	SN102/1JS1JO/E VoIP sub-categories	87
56	SN102/1JS1JO/E SIP Settings window	87
57	QoS window	88
58	Edit SIP Settings window	90
59	Advanced Edit SIP Settings window	93
60	Phone sub-category	99
61	Analog Phone window	99
62	Common window	99
63	Region window	100
64	Phone Advanced Setup window	101
65	Phone Book sub-category	107
66	Speed Dial window	108
67	Dial Plan with URL window	108
68	PSTN sub-category	111
69	PSTN Line General window	111
70	Security sub-categories	113
71	IP Filtering window	114
72	MAC filtering window	115
73	Port filtering window	116
74	Content Filter Window	117
75	ACL Setting window	118
76	Maintenance sub-categories	120
77	General System settings window	121
78	Time Setting window	122
79	Auto Provision window	123
80	Dynamic DNS window	125
81	TR069 window	126
82	Tools Configuration window	128
83	Upgrade Firmware window	129
84	Ping Test window	130
85	Restart window	131
86	System Log window	132
87	ATA with SIP Server Application	144
88	ATA Peer to Peer Call (IP Domain Call)	145

List of Tables

1	SN101/1JS/E ATA front panel LED functions	17
2	SN102/2JS/E ATA front panel LED functions	18
3	SN102/1JS1JO/E ATA front panel LED functions	18
4	Function/description of SN101/1JS/E ATA rear panel connectors/button	19
5	Function/description of SN102/2JS/E ATA rear panel connectors/button	20
6	Function/description of SN102/1JS1JO/E ATA rear panel connectors/button	20

About This Guide

This guide describes the SmartNode 100 Series Analog Telephone Adapter (ATA) hardware, installation, and basic configuration.

Audience

This guide is intended for the following users:

- Operators
- Installers
- Maintenance technicians

Structure

This guide contains the following chapters and appendices:

- [Chapter 1](#) on page 15 provides information about SN100 features and capabilities.
- [Chapter 2](#) on page 22 provides information about installing the SN100.
- [Chapter 3](#) on page 29 describes how to quickly configure the SN100 for basic operation.
- [Chapter 4](#) on page 46 describes using the SmartNode ATA home window to monitor ATA status or to use the advanced settings to configure the ATA.
- [Chapter 5](#) on page 53 describes how to modify network settings.
- [Chapter 6](#) on page 61 describes how to modify VoIP settings.
- [Chapter 7](#) on page 112 describes how to modify security settings.
- [Chapter 8](#) on page 119 describes using maintenance tools.
- [Chapter 9](#) on page 133 describes how to contact Patton for assistance
- [Appendix A](#) on page 136 provides compliance information for the SN100
- [Appendix B](#) on page 139 provides specifications for the SN100
- [Appendix C](#) on page 143 provides example application scenarios
- [Appendix D](#) on page 146 is a frequently asked questions.

For best results, read the contents of this guide *before* you install the SmartNode 100.

Precautions

Notes and cautions, which have the following meanings, are used throughout this guide to help you become aware of potential ATA problems. **Warnings** relate to personal injury issues, and **Cautions** refer to potential property damage.

Note A note presents additional information or interesting sidelights.



The alert symbol and IMPORTANT heading calls attention to important information.



The alert symbol and CAUTION heading indicate a potential hazard. Strictly follow the instructions to avoid property damage.



The shock hazard symbol and CAUTION heading indicate a potential electric shock hazard. Strictly follow the instructions to avoid property damage caused by electric shock.



The alert symbol and WARNING heading indicate a potential safety hazard. Strictly follow the warning instructions to avoid personal injury.



The shock hazard symbol and WARNING heading indicate a potential electric shock hazard. Strictly follow the warning instructions to avoid injury caused by electric shock.

Safety when working with electricity



The SmartNode device contains no user serviceable parts, and is not to be opened by the user. The equipment shall be returned to Patton Electronics for repairs or repaired by qualified service personnel.



Mains Voltage: In systems without a power switch, line voltages are present in the power supply when the power cord is connected. The mains outlet used to power the SmartNode device shall be within 10 feet (3 meters) of the device, be easily accessible, and protected by a circuit breaker.



For AC powered units, ensure that the power cable used meets all applicable standards for the country in which it is to be installed, and that it is connected to a wall outlet which has earth ground.

**WARNING**

For units with an external power adapter, the adapter shall be a listed Limited Power Source.

**WARNING**

Hazardous network voltages are present in WAN ports regardless of whether power to the SmartNode is ON or OFF. To avoid electric shock, use caution when near WAN ports. When detaching the cables, detach the end away from the SmartNode first.

**WARNING**

Before handling the device, disconnect the telephone network cables to avoid contact with telephone line voltages. When detaching the cables, detach the end away from the SmartNode device first.

**WARNING**

Do not work on the system or connect or disconnect cables during periods of lightning activity.

Deutsch

Warnhinweise:

**WARNUNG**

Dieses Gerät ist NICHT für den Anschluss an das Telefonnetz (PSTN) bestimmt und auch NICHT dafür zugelassen. Es ist nur für den Anschluss an Endgeräte beim Kunden vorgesehen.



- Das Gerät enthält keine austauschbaren Komponenten und ist vom Benutzer nicht zu öffnen. Bei Systemen ohne Netzschalter und ohne externes Netzteil liegt Netzspannung im Gerät an, wenn das Netzkabel angeschlossen ist.
- Bei Geräten mit externem Netzteil muss das Netzteil die Anforderungen an eine zugelassene Stromquelle mit begrenzter Leistung erfüllen. Die Steckdose, die für die Stromversorgung des Gerätes verwendet wird, sollte höchstens 3 Meter vom Gerät entfernt und leicht zugänglich sein sowie durch einen den örtlichen regulatorischen Anforderungen entsprechenden Schutzschalter abgesichert sein.
- Für mit Wechselstrom betriebene Geräte muss sichergestellt sein, dass das verwendete Netzkabel alle gültigen Normen des Landes erfüllt, in dem es eingesetzt werden soll.
- Für mit Wechselstrom betriebene Geräte, die 3-polige Netzstecker haben (L1, L2 u. GND oder Phase, Neutraleiter u. Schutzleiter), muss die Steckdose geerdet sein.
- Für mit Gleichstrom betriebene Geräte muss sichergestellt sein, dass die Verbindungskabel für Spannung, Strom, erwartete Temperatur, Entflammbarkeit und mechanische Wartbarkeit geeignet sind.
- WAN-, LAN- u. PSTN-Ports (Anschlüsse) können unter gefährlicher Spannung stehen, unabhängig davon, ob das Gerät ein- oder ausgeschaltet ist. PSTN bezieht sich auf Schnittstellen wie Telefon, FXS, FXO, DSL, xDSL, T1, E1, ISDN, Voice, usw. Diese sind als „gefährliche Netzwerkspannungen“ bekannt. Um einen elektrischen Schlag zu vermeiden, muss in der Nähe dieser Anschlüsse mit Vorsicht gearbeitet werden. Werden Kabel von diesen Anschlüssen getrennt, zuerst das Kabel am anderen Ende herausziehen.
- Während eines Gewitters darf nicht am Gerät gearbeitet werden und es dürfen keine Kabel angeschlossen oder vom Netz getrennt werden.



In Übereinstimmung mit den Anforderungen der Richtlinie 2002/96/EG über Elektro- und Elektronik-Altgeräte (WEEE) muss sichergestellt sein, dass Altgeräte von anderem Abfall und Schrott getrennt werden und dem Sammel- und Verwertungssystem für Elektro- und Elektronik-Altgeräte in Ihrem Land zum Recycling zugeführt werden.

General observations



Do not stack multiple SmartNode devices directly on top of one another, and do not place items on top of the device. If you will be installing equipment above the SmartNode device, leave at least 2 inches (5 cm) of clearance between the devices.

Furthermore, leave at least 2 inches (5 cm) to the left, right, front, and rear of the SmartNode device for proper ventilation.

Chapter 1 **General information**

Chapter contents

- Overview 16
- Features 16
- Front Panel LED Indicators & Rear Panels 16
 - Front panel LEDs 16
 - Rear panel connectors 19

Overview

Congratulations on becoming the owner of the SmartNode ATA, a device that connects a normal PSTN telephone to the Internet so that you can make telephone calls. The ATA provides an analog interface for PSTN, PBX, fax machines, telephones, and other devices that require an analog port.

This user manual describes how to install the ATA, and how to customize its configuration to get the most out of your new device.

This device has been thoroughly inspected and tested and is warranted for one year for parts and labor. If questions or problems arise during installation or use of this product, contact Patton Electronics Technical Support at +(301) 975-1007.

Features

The SmartNode 100 ATA series are feature-rich analog telephone adapters that enable you to connect standard telephones and make VoIP calls using your broadband connection. There is no need to replace your existing analog telephones just because you want to enhance your phone system.

Easy to install and simple to use, the SN100 series connects standard telephones or fax machines to any Voice over IP (VoIP) service provider.

Well equipped with at least one FXS RJ-11 phone interface, you can speak or fax as with the old fix net telephone. Due to the small design you can easily place the adapter anywhere.

Features include:

- Codecs:
 - / G.711-ulaw, G711-alaw, G729, G723
 - / G.726: 16k/24k/32k/40k bit per second (ADPCM)
- Call Features:
 - / Call Waiting, Call Transfer,
 - / Call Forward as Busy forward; Non-Answer forward; unconditional forward,
 - / Do-not-disturb (DND) support
 - / 3-way conferencing
- Fax Modes:
 - / T.38 relay support
 - / G.711 pass-through

Front Panel LED Indicators & Rear Panels

Front panel LEDs

Front panel indicator lights are described for the following SmartNode SN100 Series ATA models:

- SN101/1JS/E (see [figure 1](#)). [Table 1](#) lists the function of each front panel indicator.
- SN102/2JS/E (see [figure 2](#) on page 17). [Table 2](#) on page 18 lists the function of each front panel indicator.

- SN102/1JS1JO/E (see [figure 3](#) on page 18). [Table 3](#) on page 18 lists the function of each front panel indicator.

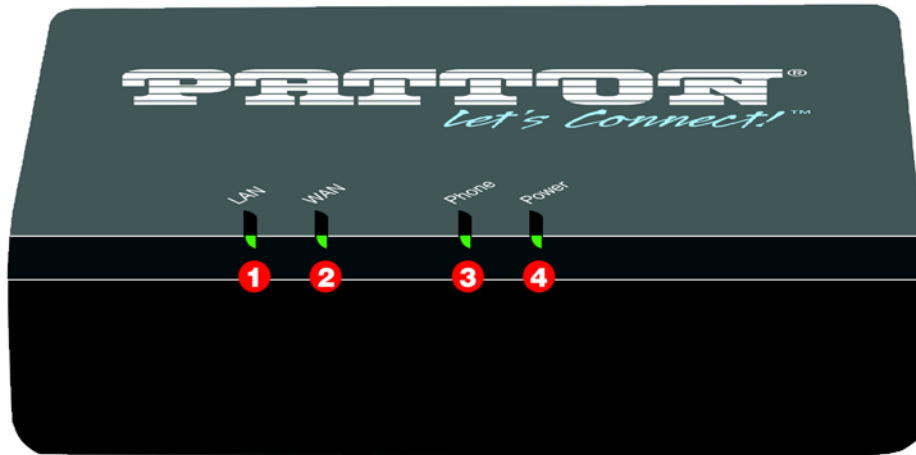


Figure 1. SN101/1JS/E ATA front panel

Table 1. SN101/1JS/E ATA front panel LED functions

Callout	LED label	Color	Status		
			On	Flashing	Off
1	LAN	Green	LAN is connected successfully	Data is transmitting	Ethernet not connected to PC
2	WAN	Green	ATA network connection established	Data traffic on cable network	Waiting for network connection
3	Phone	Green	Telephone or fax machine is on-hook	Ring Indication	Telephone or fax machine is on-hook
4	Power	Green	ATA is powered on	N/A	ATA is powered off

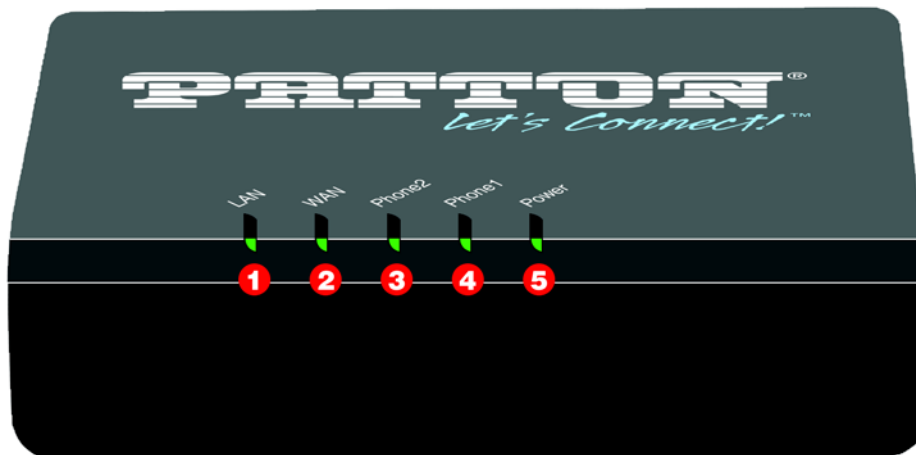


Figure 2. SN102/2JS/E ATA front panel

Table 2. SN102/2JS/E ATA front panel LED functions

Callout	LED label	Color	Status		
			On	Flashing	Off
1	LAN	Green	LAN is connected successfully	Data is transmitting	Ethernet not connected to PC
2	WAN	Green	ATA network connection established	Data traffic on cable network	Waiting for network connection
3	Phone2	Green	Telephone or fax machine is on-hook	Ring Indication	Telephone or fax machine is on-hook
4	Phone1	Green	Telephone or fax machine is on-hook	Ring Indication	Telephone or fax machine is on-hook
5	Power	Green	ATA is powered on	N/A	ATA is powered off

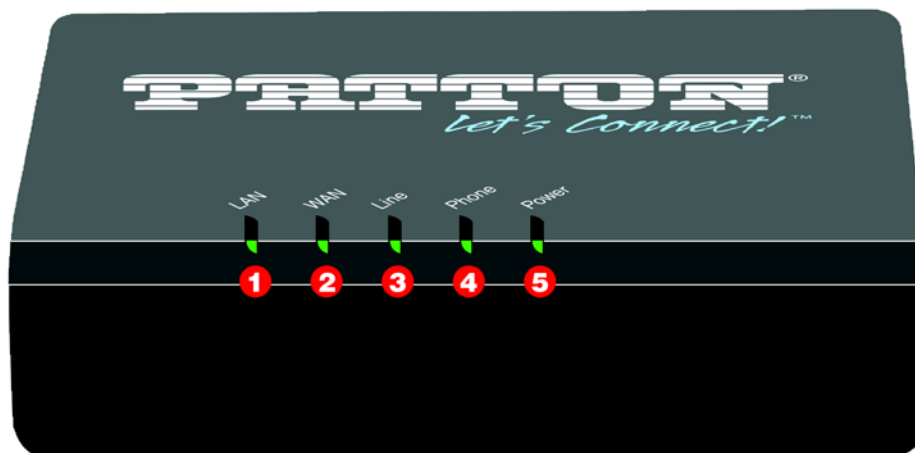


Figure 3. SN102/1JS1JO/E ATA front panel

Table 3. SN102/1JS1JO/E ATA front panel LED functions

Callout	LED label	Color	Status		
			On	Flashing	Off
1	LAN	Green	LAN is connected successfully	Data is transmitting	Ethernet not connected to PC
2	WAN	Green	ATA network connection established	Data traffic on cable network	Waiting for network connection
3	Line	Green	PBX or CO line is off-hook	Ring Indication	PBX or CO line is off-hook
4	Phone	Green	Telephone or fax machine is on-hook	Ring Indication	Telephone or fax machine is on-hook
5	Power	Green	ATA is powered on	N/A	ATA is powered off

Rear panel connectors

Rear panel connectors and switches are described for the following SmartNode SN100 Series ATA models:

- SN101/1JS/E (see [figure 4](#) on page 19). [Table 4](#) on page 19 lists the function of each connector and switch on the rear panel.
- SN102/2JS/E (see [figure 5](#) on page 20). [Table 5](#) on page 20 lists the function of each connector and switch on the rear panel.
- SN102/1JS1JO/E (see [figure 6](#) on page 20). [Table 6](#) on page 20 lists the function of each connector and switch on the rear panel.

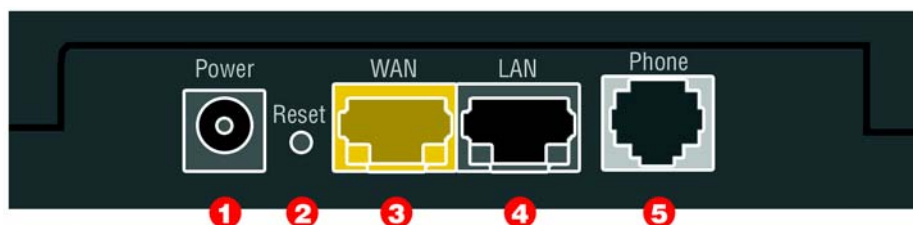


Figure 4. SN101/1JS/E ATA rear panel

Table 4. Function/description of SN101/1JS/E ATA rear panel connectors/button

Callout	Label	Color	Description
1	Power	N/A	Connects to the power adapter
2	Reset	N/A	Using a paper clip or similar object, press this button briefly to restart the unit. Press and hold for 10 seconds to restore the factory default settings.
3	WAN	Gold	Connected to PC by an Ethernet cable. This port enables your PC or switch/hub to be connected to the ATA through a networking cable with RJ-45 connectors used on 10Base-T and 100Base-TX networks.
4	LAN	Black	Connected to the network by an Ethernet cable. This port enables your ATA to be connected to an Internet Access device, e.g. router, cable modem, ADSL modem, through a networking cable with RJ-45 connectors used on 10Base-T and 100Base-TX networks.
5	Phone	Gray	FXS port can be connected to analog telephone or fax machine by an RJ-11 (Gray) analog line.



Figure 5. SN102/2JS/E ATA rear panel

Table 5. Function/description of SN102/2JS/E ATA rear panel connectors/button

Callout	Label	Color	Description
1	Power	N/A	Connects to the power adapter
2	Reset	N/A	Using a paper clip or similar object, press this button briefly to restart the unit. Press and hold for 10 seconds to restore the factory default settings.
3	WAN	Gold	Connects to a PC by an Ethernet cable. This port enables your PC or switch/hub to be connected to the ATA through a networking cable with RJ-45 connectors used on 10Base-T and 100Base-TX networks.
4	LAN	Black	Connects to the network by an Ethernet cable. This port enables your ATA to be connected to an Internet Access device, e.g. router, cable modem, ADSL modem, through a networking cable with RJ-45 connectors used on 10Base-T and 100Base-TX networks.
5	Phone1	Gray	FXS port can be connected to analog telephone or fax machine by an RJ-11 (Gray) analog line.
6	Phone2	Gray	FXS port can be connected to analog telephone or fax machine by an RJ-11 (Gray) analog line.

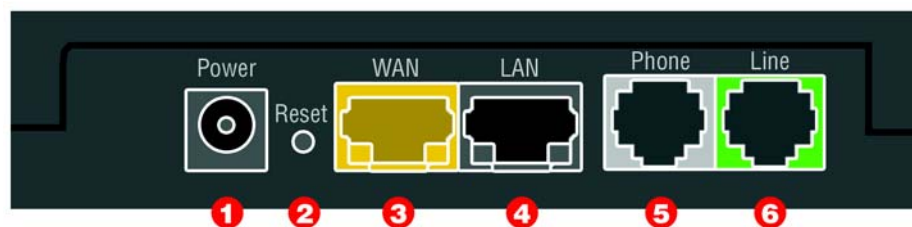


Figure 6. SN102/1JS1JO/E ATA rear panel

Table 6. Function/description of SN102/1JS1JO/E ATA rear panel connectors/button

Callout	Label	Color	Description
1	Power	N/A	Connects to the power adapter
2	Reset	N/A	Using a paper clip or similar object, press this button briefly to restart the unit. Press and hold for 10 seconds to restore the factory default settings.
3	WAN	Gold	Connects to a PC by an Ethernet cable. This port enables your PC or switch/hub to be connected to the ATA through a networking cable with RJ-45 connectors used on 10Base-T and 100Base-TX networks.

Table 6. Function/description of SN102/1JS1JO/E ATA rear panel connectors/button (Continued)

Callout	Label	Color	Description
4	LAN	Black	Connects to the network by an Ethernet cable. This port enables your ATA to be connected to an Internet Access device, e.g. router, cable modem, ADSL modem, through a networking cable with RJ-45 connectors used on 10Base-T and 100Base-TX networks.
5	Phone	Gray	FXS port can be connected to analog telephone or fax machine by an RJ-11 (Gray) analog line.
6	Line	Green	Connected to PBX or CO line by an RJ-11 (Gray) analog line. The PSTN (FXO) port can be connected to the extension port of a PBX or directly connected to a carrier's PSTN line.

Chapter 2 Installation

Chapter contents

- Introduction23
- Installing the SN101/1JS/E (1 FXS port) ATA.....23
 - Package contents24
 - Connecting the ATA to a computer24
 - Connecting the ATA to a cable/DSL modem or router25
 - Connecting the ATA to a telephone or fax machine25
 - Connecting power to the ATA25
- Installing the SN102/2JS/E (2 FXS ports) ATA25
 - Package contents25
 - Connecting the ATA to a computer26
 - Connecting the ATA to a cable/DSL modem or router26
 - Connecting the ATA to telephones or fax machines26
 - Connecting power to the ATA26
- Installing the SN102/1JS1JO/E (1 FXS port and 1 FXO ports) ATA.....26
 - Package contents27
 - Connecting the ATA to a computer27
 - Connecting the ATA to a cable/DSL modem or router27
 - Connecting the ATA to a telephone or fax machine27
 - Connecting the ATA to the PSTN or a PBX27
 - Connecting power to the ATA27

Introduction

This chapter describes installing the following SmartNode 100 Series devices:

- “Installing the SN101/1JS/E (1 FXS port) ATA” on page 23
- “Installing the SN102/2JS/E (2 FXS ports) ATA” on page 25
- “Installing the SN102/1JS1JO/E (1 FXS port and 1 FXO ports) ATA” on page 26

Refer to the appropriate section to install the ATA as shown in figure 7.

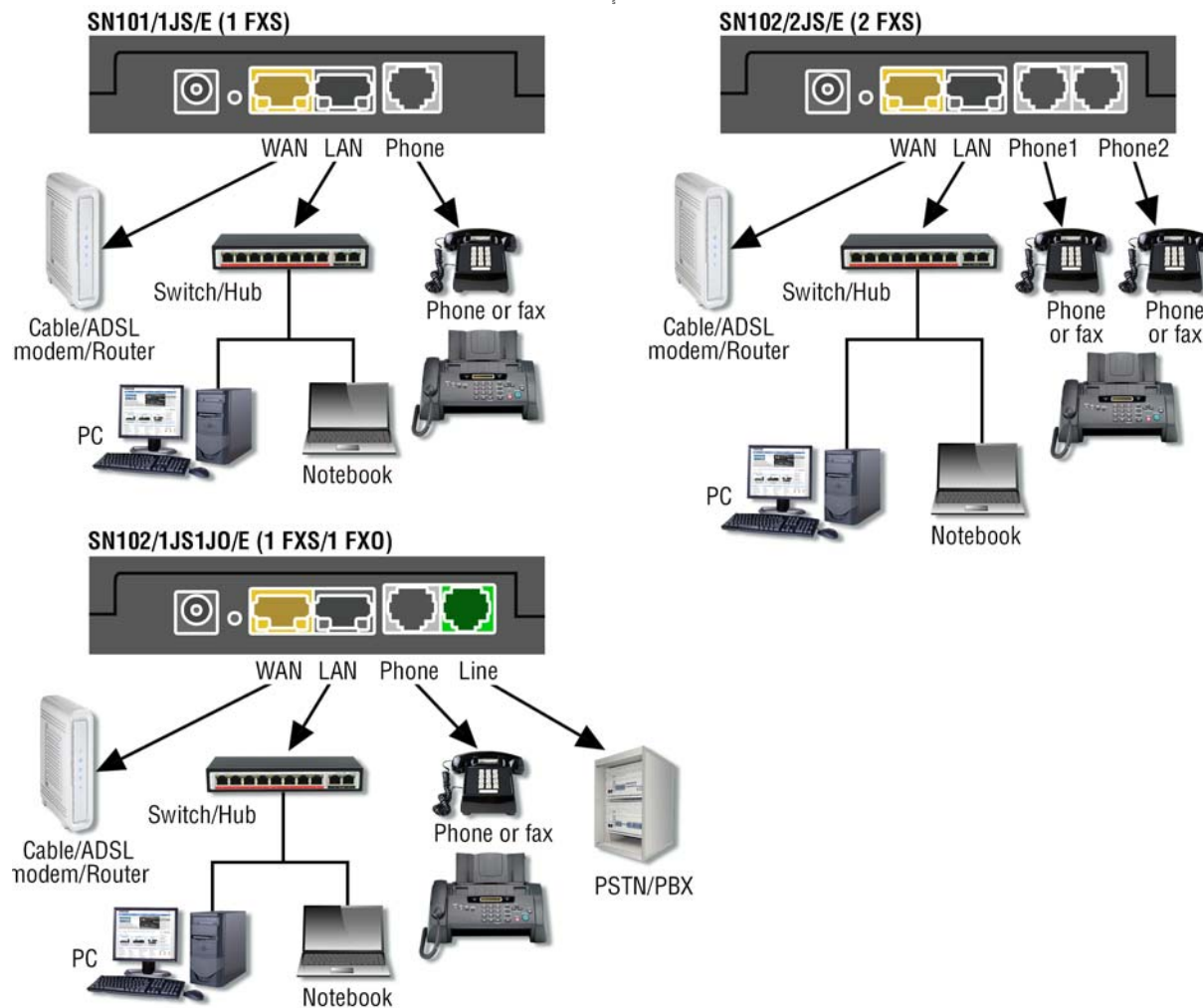


Figure 7. Typical SN100 Series applications

Installing the SN101/1JS/E (1 FXS port) ATA

Installation consists of the following:

- Verifying the package contents (see section “Package contents” on page 24)
- Connecting the ATA LAN port directly to a computer or to a computer via a switch/hub (see section “” on page 24)

- Connecting the ATA *WAN* port to a cable/DSL modem or router (see section “[Connecting the ATA to a cable/DSL modem or router](#)” on page 25)
- Connecting the ATA *Phone* port to an analog telephone or fax machine (see section “[Connecting the ATA to a telephone or fax machine](#)” on page 25)
- Connecting power to the ATA (see section “[Connecting power to the ATA](#)” on page 25)

Package contents

- SmartNode 100 Series ATA
- Ethernet cable (Cat. 5, UTP, unshielded twisted pair, Color: yellow, RJ-45 connectors, Length 5 feet/1.5 m) (see [figure 8](#))
- Phone line cable (Color: gray, RJ-11 connectors, Length 5 feet/1.5 m)
- Power adapter (12VDC/1A)

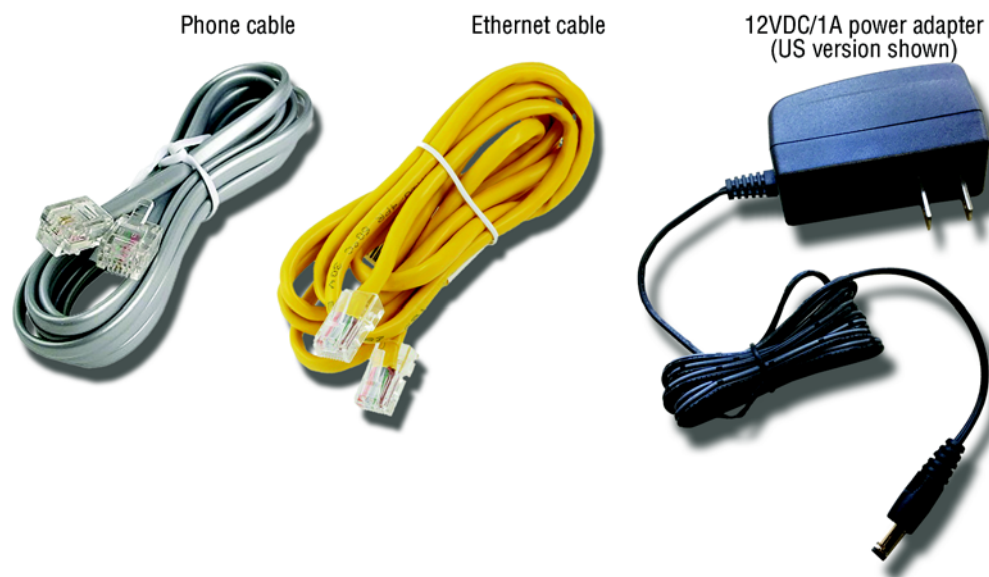


Figure 8. SN100 ATA cables and 12VDC/1A power adapter

Connecting the ATA to a computer

1. Connect one end of the Ethernet cable included in the SN100 package to the *LAN* port on the ATA. If you are connecting the ATA directly to a computer, go to step 2. Otherwise, go to step 4 to connect multiple computers to the ATA via a hub, switch, or router.
2. Disconnect power from your computer.
3. Connect the other end of the Ethernet cable to your computer's network interface card (NIC). Go to section “[Connecting the ATA to a cable/DSL modem or router](#)”.
4. Disconnect power from your hub, switch, or router.
5. Connect the other end of the Ethernet cable to your hub, switch, or router's WAN/Internet port.

6. Connect your computer(s) to the available hub, switch, or router LAN ports using separate Ethernet cables.

Connecting the ATA to a cable/DSL modem or router

1. Connect one end of an Ethernet cable (with RJ-45 connectors) to the *WAN* port on the ATA.
2. Disconnect power from your cable/DSL modem or router.
3. Connect the other end of the Ethernet cable to a DSL/cable modem or router.

Connecting the ATA to a telephone or fax machine

Connect your analog telephone or fax machine to the *Phone* port on the ATA.

Connecting power to the ATA

1. Connect the power adapter's barrel jack to the *Power* port on the ATA.
2. Connect the other end of the power adapter to the AC power outlet.
3. Verify that the ATA's *Power* LED is lit.
4. Connect power to the computer or hub, switch, or router.
5. Connect power to the cable/DSL modem or router.

The ATA is installed. Proceed to Chapter 3, "Quick Start" on page 29.

Installing the SN102/2JS/E (2 FXS ports) ATA

Installation consists of the following:

- Verifying the package contents (see section "Package contents" on page 25)
- Connecting the ATA *LAN* port directly to a computer or to a computer via a switch/hub (see section "Connecting the ATA to a computer" on page 26)
- Connecting the ATA *WAN* port to a cable/DSL modem or router (see section "Connecting the ATA to a cable/DSL modem or router" on page 26)
- Connecting the ATA *Phone1* and *Phone2* ports to two analog telephones, two fax machines or one phone and one fax machine (see section "Connecting the ATA to telephones or fax machines" on page 26)
- Connecting power to the ATA (see section "Connecting power to the ATA" on page 26)

Package contents

- SmartNode 100 Series ATA
- Ethernet cable (Cat. 5, UTP, unshielded twisted pair, Color: yellow, RJ-45 connectors, Length 5 feet/1.5 m) (see figure 8 on page 24)
- Phone line cable (Color: gray, RJ-11 connectors, Length 5 feet/1.5 m)
- Power adapter (12VDC/1A)

Connecting the ATA to a computer

1. Connect the one end of the yellow Ethernet cable included in the SN100 package to the *LAN* port on the ATA. If you are connecting the ATA directly to a computer, go to step 2. Otherwise, go to step 4 to connect multiple computers to the ATA via a hub, switch, or router.
2. Disconnect power from your computer.
3. Connect the other end of the Ethernet cable to your computer's network interface card (NIC).
4. Disconnect power from your hub, switch, or router.
5. Connect the other end of the Ethernet cable to your hub, switch, or router's WAN/Internet port.
6. Connect your computer(s) to the available hub, switch, or router LAN ports using separate Ethernet cables.

Connecting the ATA to a cable/DSL modem or router

1. Connect one end of an Ethernet cable (with RJ-45 connectors) to the *WAN* port on the ATA.
2. Disconnect power from your cable/DSL modem or router.
3. Connect the other end of the Ethernet cable to a DSL/cable modem or router.

Connecting the ATA to telephones or fax machines

The two ATA FXS phone ports enable you to connect two analog telephones, two fax machines, or one telephone and one fax machine to the ATA.

1. Connect an analog telephone or fax machine to the *Phone1* port on the ATA.
2. Connect an analog telephone or fax machine to the *Phone2* port on the ATA.

Connecting power to the ATA

1. Connect the power adapter's barrel jack to the *Power* port on the ATA.
2. Connect the other end of the power adapter to the AC power outlet.
3. Verify that the ATA's *Power* LED is lit.
4. Connect power to the computer or hub, switch, or router.
5. Connect power to the cable/DSL modem or router.

The ATA is installed. Proceed to Chapter 3, "Quick Start" on page 29.

Installing the SN102/1JS1JO/E (1 FXS port and 1 FXO ports) ATA

Installation consists of the following:

- Verifying the package contents (see section "Package contents" on page 27)
- Connecting the ATA *LAN* port directly to a computer or to a computer via a switch/hub (see section "Connecting the ATA to a computer" on page 27)
- Connecting the ATA *WAN* port to a cable/DSL modem or router (see section "Connecting the ATA to a cable/DSL modem or router" on page 27)

- Connecting the ATA *Phone* FXS port to an analog telephone or fax machine (see section “Connecting the ATA to a telephone or fax machine” on page 27)
- Connecting the ATA *Line* FXO port to the PSTN or a PBX (see section “Connecting the ATA to the PSTN or a PBX” on page 27)
- Connecting power to the ATA (see section “Connecting power to the ATA” on page 27)

Package contents

- SmartNode 100 Series ATA
- Ethernet cable (Cat. 5, UTP, unshielded twisted pair, Color: yellow, RJ-45 connectors, Length 5 feet/1.5 m) (see figure 8 on page 24)
- Phone line cable (Color: gray, RJ-11 connectors, Length 5 feet./1.5 m)
- Power adapter (12VDC/1A)

Connecting the ATA to a computer

1. Connect the one end of yellow Ethernet cable included in the SN100 package to the *LAN* port on the ATA. If you are connecting the ATA directly to a computer, go to step 2. Otherwise, go to step 4 to connect multiple computers to the ATA via a hub, switch, or router.
2. Disconnect power from your computer.
3. Connect the other end of the Ethernet cable to your computer’s network interface card (NIC).
4. Disconnect power from your hub, switch, or router.
5. Connect the other end of the Ethernet cable to your hub, switch, or router’s WAN/Internet port.
6. Connect your computer(s) to the available hub, switch, or router LAN ports using separate Ethernet cables.

Connecting the ATA to a cable/DSL modem or router

1. Connect one end of an Ethernet cable (with RJ-45 connectors) to the *WAN* port on the ATA.
2. Disconnect power from your cable/DSL modem or router.
3. Connect the other end of the Ethernet cable to a DSL/cable modem or router.

Connecting the ATA to a telephone or fax machine

Using the included gray phone cable, connect your analog telephone or fax machine to the *Phone* port on the ATA.

Connecting the ATA to the PSTN or a PBX

Connect the PSTN or a PBX to the *Line* port on the ATA.

Connecting power to the ATA

1. Connect the power adapter’s barrel jack to the *Power* port on the ATA.
2. Connect the other end of the power adapter to the AC power outlet.
3. Verify that the ATA’s *Power* LED is lit.

4. Connect power to the computer or hub, switch, or router.
5. Connect power to the cable/DSL modem or router.

The ATA is installed. Proceed to Chapter 3, "[Quick Start](#)" on page 29.

Chapter 3 Quick Start

Chapter contents

- Introduction30
- Configuring the SN100 to communicate with your computer.....30
- Wizard Setup window31
- WAN Port Type set up.....34
- VoIP set up35
 - Configuring SN101/1JS/E (1 FXS) ATA VoIP settings36
 - Configuring SN102/2JS/E (2 FXS) ATA VoIP settings39
 - Configuring SN102/1JS1JO/E (1 FXS/1 FXO) ATA VoIP settings42

Introduction

This chapter describes using the Connection Setup and VoIP Setup wizards to quickly configure the ATA for operation.

Configuring the SN100 to communicate with your computer

By default, the SN100 is configured for the following network environment:

- WAN type: **DHCP client**
- LAN IP: **192.168.1.1**
- LAN subnet mask: **255.255.255.0**

Do the following:

1. Configure the network interface of your computer to be the DHCP client. It will obtain an IP address from the SmartNode ATA automatically.
2. Using a Web browser (Microsoft Edge, Google Chrome, etc.) link to URL **http://192.168.1.1**. A login window displays (see [figure 9](#)).

Note Most examples of SN100 screens in this manual are from an SN102/2JS/E (ATA with 2 FXS ports). Where differences are relevant, screens from other SN100 models will be shown.

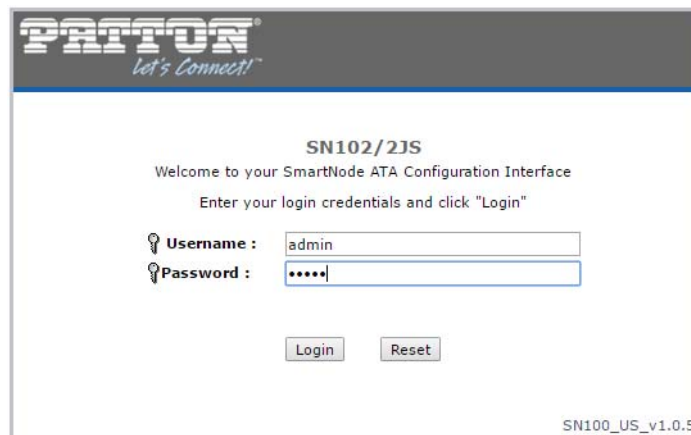


Figure 9. Login window

3. Type the default user name in the *Username* box: **admin**
4. Type the default password in the *Password* box: **admin**
5. Click the *Login* button. The *Please select Wizard or Advanced mode* window displays (see [figure 10](#) on page 31).

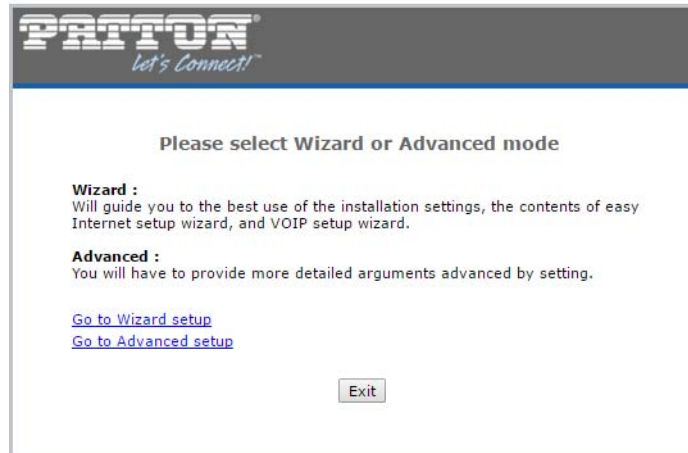


Figure 10. Please select Wizard or Advanced mode window

Wizard Setup window

1. After finishing the authentication, the *Wizard Setup* window displays (see figure 11). Click *CONNECTION WIZARD* to begin. The *Welcome to the Connection Wizard* window displays (see figure 12 on page 32).

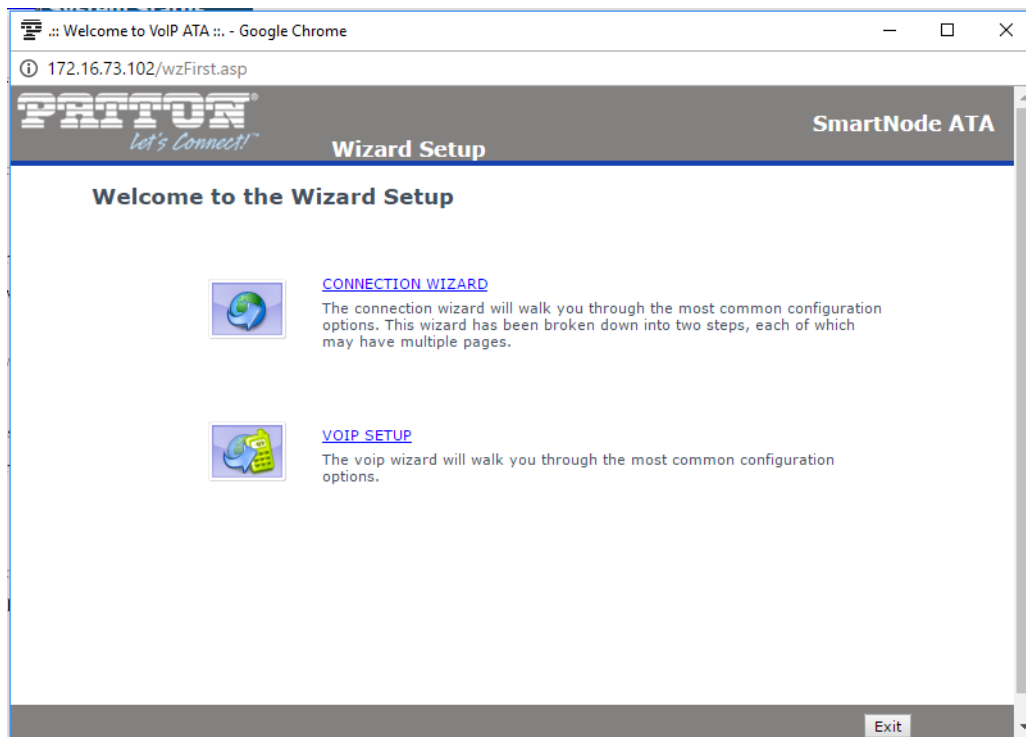


Figure 11. Wizard Setup window

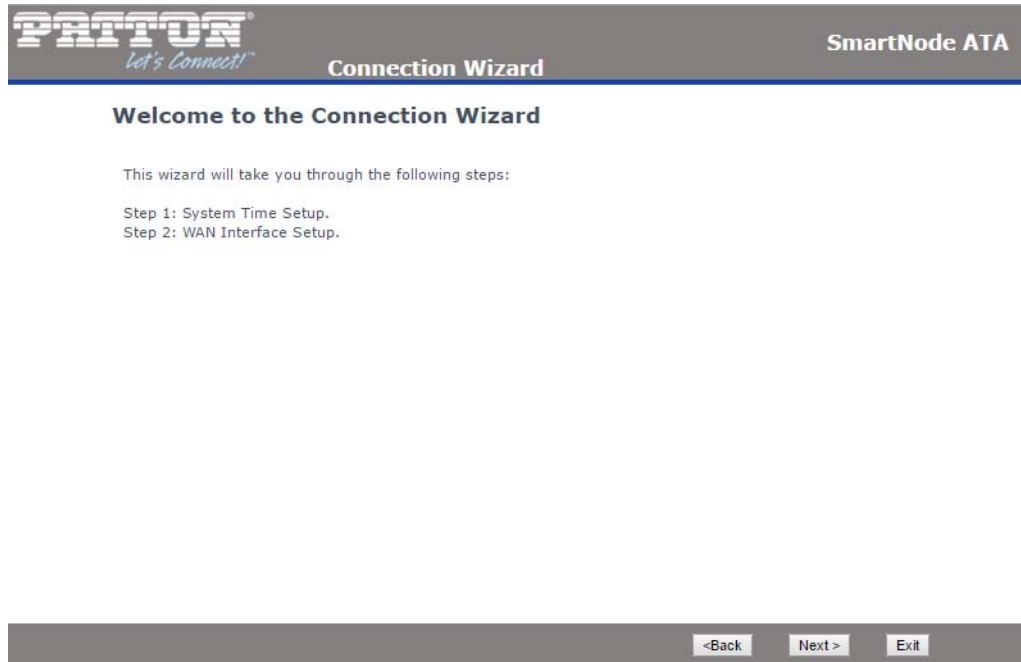


Figure 12. Welcome to the Connection Wizard window

Note To return to a previous window in the wizard, click the *< Back* button. To go to the next window in the wizard, click the *Next >* button. To cancel the setup process, click the *Exit* button.



Changes are only saved when you click the *Finish* button that is displayed at the end of each wizard, so if you click *Exit*, **all changes will be lost.**

- Click the *Next>* button to begin system time setup. The *Time Zone Setting* window displays (see [figure 13](#)).

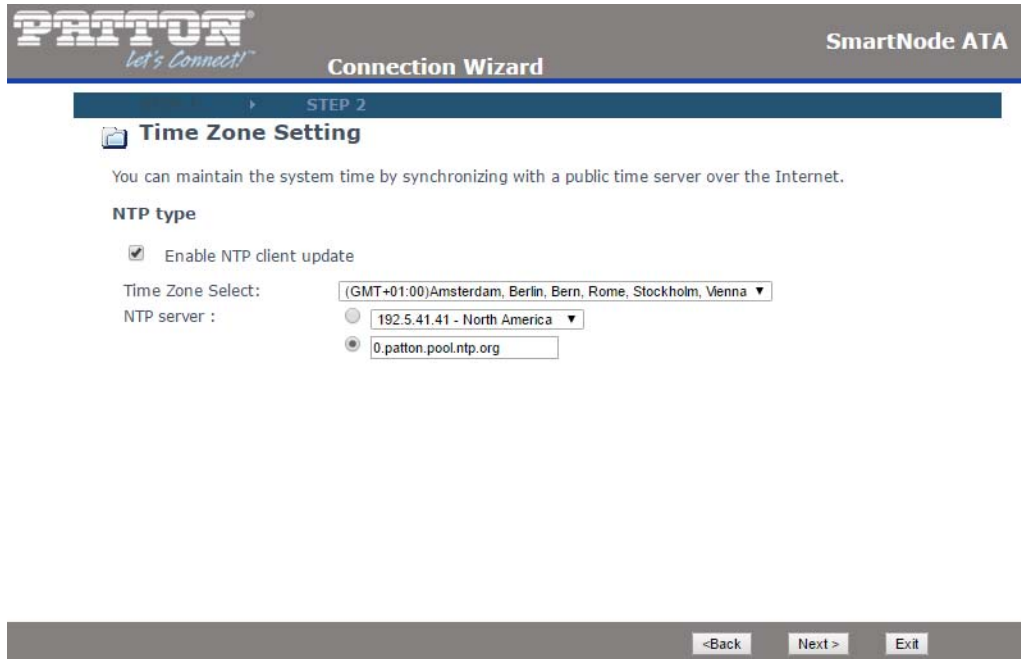


Figure 13. Time Zone Setting window

- Click to enable *Enable NTP client update*.

Enable NTP client update

- Click the *Time Zone Select* drop-down menu, then select the appropriate time zone.

Time Zone Select: (GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna ▼

- Click the *NTP server* drop-down menu, then select the appropriate NTP server.

NTP server : 192.5.41.41 - North America ▼

- Click the *Next>* button. The *WAN Interface Setting* window displays (see [figure 14](#) on page 34).

PATTON
Let's Connect!

Connection Wizard SmartNode ATA

STEP 1

WAN Interface Setting

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point.
Here you may change the access method to static IP, DHCP, PPPoE, by click the item value of WAN Access type.

WAN IP

WAN Access Type:

IP Address:

Subnet Mask:

Default Gateway:

DNS:

<Back Finished Exit

Figure 14. WAN Interface Setting window

Go to section “WAN Port Type set up” to set up the WAN interface.

WAN Port Type set up

For most users, Internet access is the primary application. The SN100 supports the WAN interface for Internet access and remote access.

The following sections explain details of WAN Port Internet access and broadband access setup:

1. Click the *WAN Access Type* drop-down menu, then select from the following options:

WAN Access Type:	<input type="text" value="Static IP"/>
IP Address:	<input type="text" value="172.16.73.102"/>
Subnet Mask:	<input type="text" value="255.255.224.0"/>
Default Gateway:	<input type="text" value="172.16.64.1"/>

- **Static IP (Fixed IP User):** If you are a leased line user with a fixed IP address, fill out the following items with the information provided by your ISP:
 - *IP Address:* check with your ISP provider
 - *Subnet Mask:* check with your ISP provider
 - *Default Gateway:* check with your ISP provider
- **Dynamic IP (DHCP Client):** Obtain WAN IP address automatically
- **PPPoE (ADSL Dial-Up User):** Some ISPs provide DSL-based service and use PPPoE to establish communication links with end-users. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you need to select this option.

- *User Name*: Enter User Name provided by your ISP
 - *Password*: Enter Password provided by your ISP.
2. Click the *Finished*> button. The *Setting Internet interface* message window displays (see [figure 15](#)).



Figure 15. Setting Internet interface message window

When the Internet interface has been set up, the *Wizard Setup* window displays (see [figure 11](#) on page 31).

VoIP set up

This section describes configuring SN100 Series ATA VoIP settings. Chose the appropriate section from the following:

- “Configuring SN101/1JS/E (1 FXS) ATA VoIP settings” on page 36
- “Configuring SN102/2JS/E (2 FXS) ATA VoIP settings” on page 39
- “Configuring SN102/1JS1JO/E (1 FXS/1 FXO) ATA VoIP settings” on page 42

Configuring SN101/1JS/E (1 FXS) ATA VoIP settings

1. Click *VOIP SETUP*. The *VoIP Configuration* window displays (see figure 16 on page 36). Do the following to configure Phone 1 SIP settings:

The screenshot shows the 'VoIP Configuration' window for a Patton SmartNode ATA. The window is titled 'VoIP Setup' and 'SmartNode ATA'. It indicates 'STEP 2' and 'VoIP Configuration'. The configuration is for 'Phone 1 SIP Settings'. The fields are as follows:

Field	Value
SIP Number	2602
SIP Server Address	10.10.50.10
SIP Service Domain	
Authentication	
User Name	2602
Password

Navigation buttons at the bottom: <Back, Next >, Exit.

Figure 16. VoIP Configuration window

2. Type the SIP number that was provided by your ISP in the *SIP Number* box.

SIP Number

3. Type the proxy address that was provided by your ISP in the *SIP Server Address* box.

SIP Server Address

4. Type the SIP domain that was provided by your ISP in the *SIP Service Domain* box.

SIP Service Domain

5. Type the user name that was provided by your ISP in the *Username* box.

User Name

6. Type the password that was provided by your ISP in the *Password* box.

Password

7. Click the *Finish* button. The *Congratulations!* window displays (see [figure 17](#)). After a short delay, the *REG Status* table (see [figure 18](#)) should display *Reg Success* (registration successful).

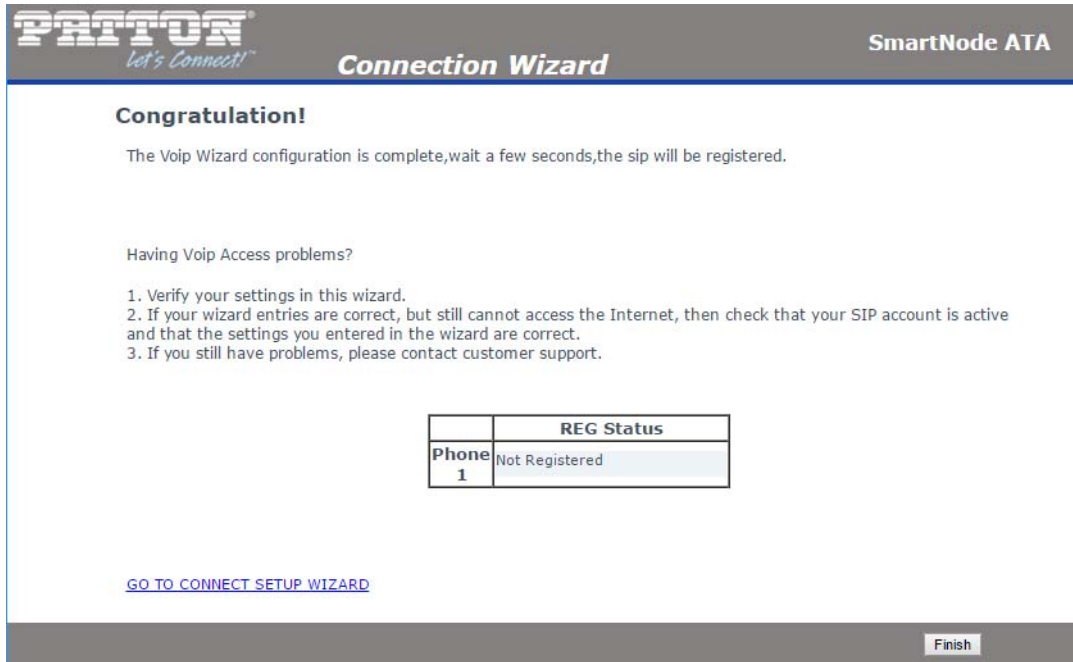


Figure 17. Congratulations! window

REG Status	
Phone 1	Reg Processing

Figure 18. REG Status table

- Note** If the ATA is having a problem registering a phone or fax machine, do the following:
- Verify that the VoIP settings were entered correctly.
 - If the VoIP entries are correct, but the ATA still cannot access the Internet, verify that your SIP account is active.
 - If ATA is still having problems, please contact technical support (see Chapter 9, "Contacting Patton for assistance" on page 133 for details).

8. Click the *Finish* button. The SmartNode ATA home window (see [figure 19](#) on page 38) displays.

The screenshot displays the 'Status' page of the SmartNode ATA web interface. On the left is a navigation menu with 'System Status' selected. The main content area is divided into several sections:

- Device Information:** Shows Model Type (SN101/1JS) and Firmware Version (SN100_EU_v1.0.5). It includes WAN and LAN information with IP addresses, subnet masks, default gateways, and MAC addresses.
- System Status:** Displays System Uptime (0day:0h:5m:22s), Current Date/Time (Thu Mar 30 19:48:39 2017), System Resource, CPU Usage (0%), and Memory Usage (39%).
- Interface Status:** A table showing the status of WAN (Down) and LAN (Up) interfaces.
- Summary Status:** Provides links for DHCP Table, VoIP Status, and Packet Statistics.
- VoIP Status:** A table showing SIP Account (SIP 1), Registration (Register button), and REG Status (Not Registered).

Figure 19. SN101/1JS/E ATA home window

Congratulations! The ATA is ready for use.

Configuring SN102/2JS/E (2 FXS) ATA VoIP settings

1. Click *VOIP SETUP*. The *VoIP Configuration* window displays (see figure 20). Do the following to configure Phone 1 SIP settings:

The screenshot shows the 'VoIP Setup' window for a Patton SmartNode ATA. The window title is 'VoIP Setup' and it is labeled 'SmartNode ATA'. It is 'STEP 2' of the configuration process. The main heading is 'VoIP Configuration'. Under 'Phone 1 SIP Settings', there are three input fields: 'SIP Number' with the value '2602', 'SIP Server Address' with the value '10.10.50.10', and 'SIP Service Domain' which is empty. Under 'Authentication', there are two input fields: 'User Name' with the value '2602' and 'Password' which is masked with dots. At the bottom right, there are three buttons: '<Back', 'Next >', and 'Exit'.

Figure 20. VoIP Configuration - Phone 1 window

2. Type the SIP number that was provided by your ISP in the *SIP Number* box.

SIP Number

3. Type the proxy address that was provided by your ISP in the *SIP Server Address* box.

SIP Server Address

4. Type the SIP domain that was provided by your ISP in the *SIP Service Domain* box.

SIP Service Domain

5. Type the user name that was provided by your ISP in the *Username* box.

User Name

6. Type the password that was provided by your ISP in the *Password* box.

Password

Click the *Next >* button. The *VoIP Configuration* window displays (see [figure 21](#)). Do the following to configure Phone 2 SIP settings:

Figure 21. VoIP Configuration - Phone 2 window

7. Type the SIP number that was provided by your ISP in the *SIP Number* box.

SIP Number

8. Type the proxy address that was provided by your ISP in the *SIP Server Address* box.

SIP Server Address

9. Type the SIP domain that was provided by your ISP in the *SIP Service Domain* box.

SIP Service Domain

10. Type the user name that was provided by your ISP in the *Username* box.

User Name

11. Type the password that was provided by your ISP in the *Password* box.

Password

12. Click the *Finish* button. The *Congratulations!* window displays (see [figure 22](#)). After a short delay, the *REG Status* table (see [figure 23](#)) should display *Reg Success* (registration successful) for each phone you set up.

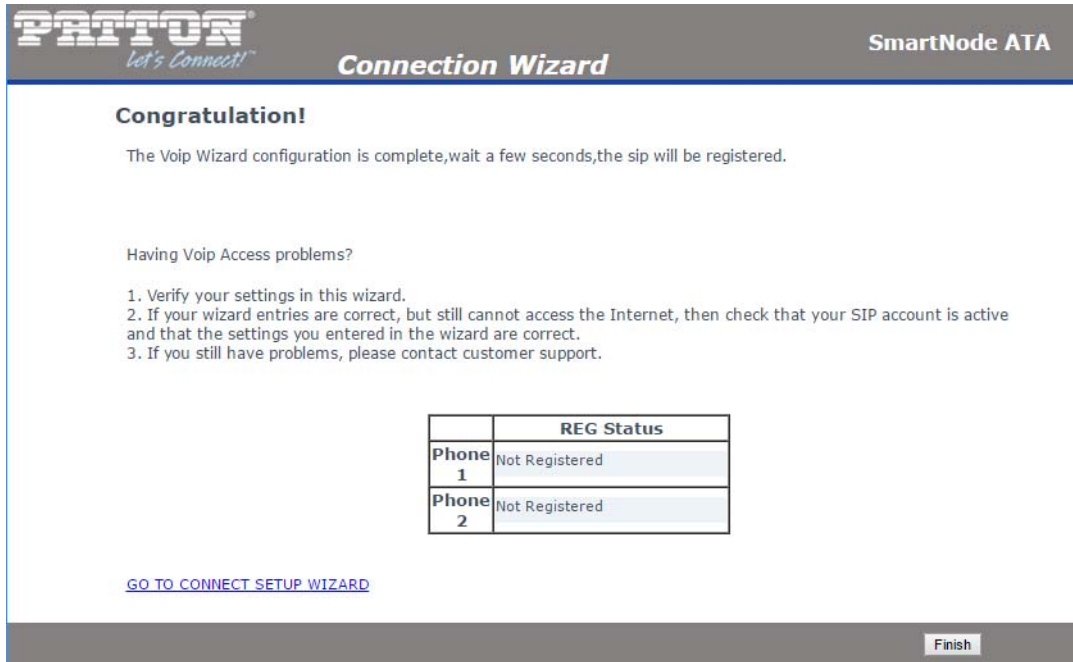


Figure 22. Congratulations! window

	REG Status
Phone 1	Reg Processing
Phone 2	Reg Processing

Figure 23. REG Status table

Note If the ATA is having a problem registering phones/fax machines, do the following:

- Verify that the VoIP settings were entered correctly.
- If the VoIP entries are correct, but the ATA still cannot access the Internet, verify that your SIP account is active.
- If ATA is still having problems, please contact technical support (see Chapter 9, "Contacting Patton for assistance" on page 133 for details).

13. Click the *Finish* button. The SmartNode ATA home window (see [figure 24](#) on page 42) displays.

The screenshot shows the SmartNode ATA home window with the following sections:

- System Status:**
 - System Uptime: 2day:21h:2m:57s
 - Current Date/Time: Mon May 15 18:59:56 2017
 - System Resource:
 - CPU Usage: 1%
 - Memory Usage: 40%
- Device Information:**
 - Model Type: SN102/2JS
 - Firmware Version: SN100_US_v1.0.5
 - WAN Information:**
 - WAN Access Type: Static IP
 - IP Address: [10.10.50.70](#)
 - IP Subnet Mask: 255.255.255.0
 - Default Gateway: 10.10.50.1
 - MAC Address: 78:8c:54:27:ab:42
 - LAN Information:**
 - IP Address: [192.168.1.1](#)
 - IP Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.1.1
 - MAC Address: 78:8c:54:27:ad:77
 - DHCP Server: Enabled
- Interface Status:**

Interface	Status	Rate
WAN	Up	100M
LAN	Down	N/A
- Summary Status:**
 - DHCP Table ([Details....](#))
 - Packet Statistics ([Details....](#))
 - VoIP Status([Details....](#))
- VoIP Status:**

SIP Account	Registration	REG Status	URI
SIP 1	<input type="button" value="UnRegister"/>	Reg Success	2602@10.10.50.10
SIP 2	<input type="button" value="Register"/>	Not Registered	

Figure 24. SN102/2JS/E ATA home window

Congratulations! The ATA is ready for use.

Configuring SN102/1JS1JO/E (1 FXS/1 FXO) ATA VoIP settings

1. Click *VOIP SETUP*. The *VoIP Configuration* window displays (see figure 25 on page 43). Do the following to configure Phone 1 SIP settings:

PRITON
Let's Connect!

VoIP Setup

SmartNode ATA

STEP 2

VoIP Configuration

Phone 1 SIP Settings

SIP Number

SIP Server Address

SIP Service Domain

Authentication

User Name

Password

<Back Next > Exit

Figure 25. VoIP Configuration - Phone 1 window

2. Type the SIP number that was provided by your ISP in the *SIP Number* box.

SIP Number

3. Type the proxy address that was provided by your ISP in the *SIP Server Address* box.

SIP Server Address

4. Type the SIP domain that was provided by your ISP in the *SIP Service Domain* box.

SIP Service Domain

5. Type the user name that was provided by your ISP in the *Username* box.

User Name

6. Type the password that was provided by your ISP in the *Password* box.

Password

7. Click the *Finish* button. The *Congratulations!* window displays (see [figure 26](#)). After a short delay, the *REG Status* table (see [figure 27](#)) should display *Reg Success* (registration successful).

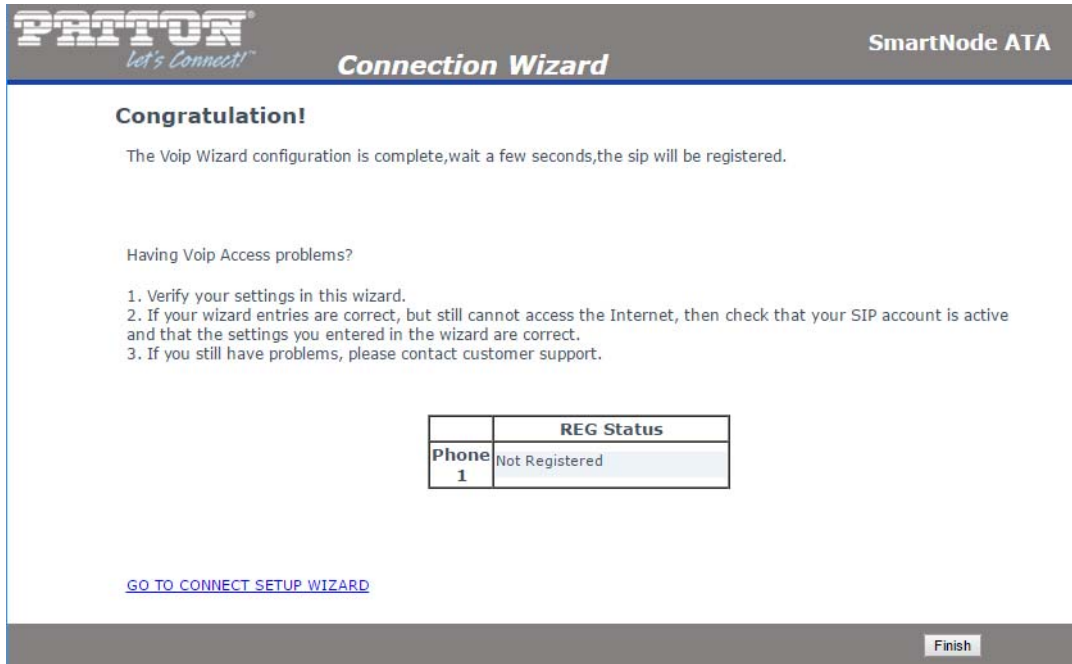


Figure 26. Congratulations! window

	REG Status
Phone 1	Reg Processing

Figure 27. REG Status table

- Note** If the ATA is having a problem registering a phone or fax machine, do the following:
- Verify that the VoIP settings were entered correctly.
 - If the VoIP entries are correct, but the ATA still cannot access the Internet, verify that your SIP account is active.
 - If ATA is still having problems, please contact technical support (see Chapter 9, "[Contacting Patton for assistance](#)" on page 133 for details).

8. Click the *Finish* button. The SmartNode ATA home window (see [figure 28](#) on page 45) displays.

The screenshot shows the SmartNode ATA home window with the following sections:

- System Status:**
 - SN102/2JS
 - Network
 - VoIP
 - Security
 - Maintenance
- Status:**
 - Device Information:**
 - Model Type: SN102/2JS
 - Firmware Version: SN100_US_v1.0.5
 - WAN Information:**
 - WAN Access Type: Static IP
 - IP Address: [10.10.50.70](#)
 - IP Subnet Mask: 255.255.255.0
 - Default Gateway: 10.10.50.1
 - MAC Address: 78:8c:54:27:ab:42
 - LAN Information:**
 - IP Address: [192.168.1.1](#)
 - IP Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.1.1
 - MAC Address: 78:8c:54:27:ad:77
 - DHCP Server: Enabled
 - System Status:**
 - System Uptime: 2day:21h:2m:57s
 - Current Date/Time: Mon May 15 18:59:56 2017
 - System Resource:
 - CPU Usage: 1%
 - Memory Usage: 40%
 - Interface Status:**

Interface	Status	Rate
WAN	Up	100M
LAN	Down	N/A
 - Summary Status:**
 - DHCP Table ([Details...](#))
 - Packet Statistics ([Details...](#))
 - VoIP Status([Details...](#))
 - VoIP Status:**

SIP Account	Registration	REG Status	URI
SIP 1	<input type="button" value="UnRegister"/>	Reg Success	2602@10.10.50.10
SIP 2	<input type="button" value="Register"/>	Not Registered	

Figure 28. SN102/1JS1JO/E ATA home window

Congratulations! The ATA is ready for use.



For proper security we recommend that you change from the default credentials to a new administrator’s user name and password as soon as possible (see Chapter 8, “[Configuring Administrator Account’s user name and password](#)” on page 121).

Chapter 4 **SmartNode ATA Home**

Chapter contents

- Introduction47
- Accessing the home window47
- System Status pane49
 - Device information50
 - System status50
 - Interface status51
 - Summary status51
 - VoIP status51
- Network, VoIP, Security, and Maintenance Menu52

Introduction

This chapter describes using the SmartNode ATA home window (see [figure 29](#)) to monitor ATA status or to use the advanced settings to configure the ATA.

The screenshot displays the SmartNode ATA home window. The top header features the Patton logo and the text "let's Connect!" on the left, and "SmartNode ATA" on the right. A left sidebar contains navigation options: "System Status" (selected), "SN102/2JS", "Network", "VoIP", "Security", and "Maintenance". The main content area is titled "Status" and is divided into several sections:

- Device Information:**
 - Model Type: SN102/2JS
 - Firmware Version: SN100_US_v1.0.5
 - WAN Information:**
 - WAN Access Type: Static IP
 - IP Address: [10.10.50.70](#)
 - IP Subnet Mask: 255.255.255.0
 - Default Gateway: 10.10.50.1
 - MAC Address: 78:8c:54:27:ab:42
 - LAN Information:**
 - IP Address: [192.168.1.1](#)
 - IP Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.1.1
 - MAC Address: 78:8c:54:27:ad:77
 - DHCP Server: Enabled
- System Status:**
 - System Uptime: 2day:21h:2m:57s
 - Current Date/Time: Mon May 15 18:59:56 2017
 - System Resource:
 - CPU Usage: 1% (represented by a progress bar)
 - Memory Usage: 40% (represented by a progress bar)
- Interface Status:**

Interface	Status	Rate
WAN	Up	100M
LAN	Down	N/A
- Summary Status:**
 - DHCP Table ([Details...](#))
 - Packet Statistics ([Details...](#))
 - VoIP Status([Details...](#))
- VoIP Status:**

SIP Account	Registration	REG Status	URI
SIP 1	<input type="button" value="UnRegister"/>	Reg Success	2602@10.10.50.10
SIP 2	<input type="button" value="Register"/>	Not Registered	

Figure 29. SmartNode ATA home window

Accessing the home window

1. Using a Web browser (Microsoft Edge, Google Chrome, etc.) link to URL <http://192.168.1.1>. The login window displays (see [figure 30](#) on page 48).

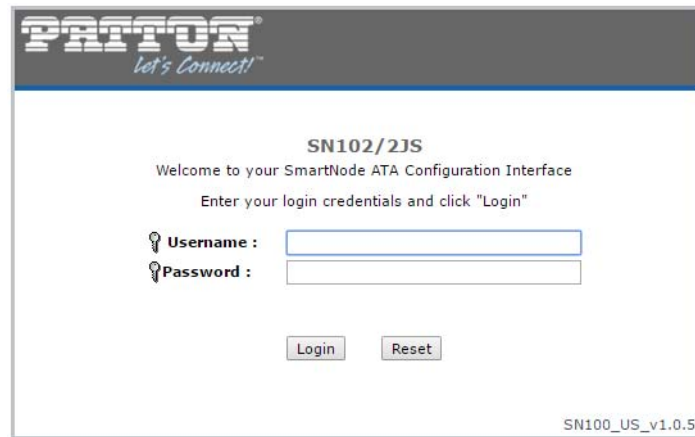


Figure 30. Login window

2. Type the default user name in the *Username* box: **admin**
3. Type the default password in the *Password* box: **admin**
4. Click the *Login* button. The *Please select Wizard or Advanced mode* window displays (see [figure 31](#) on page 48).

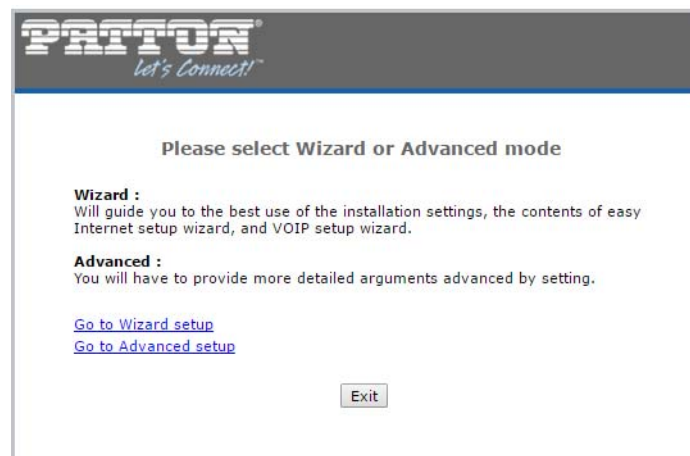


Figure 31. Please select Wizard or Advanced mode window

5. Click *Go to Advanced Setup*. The SmartNode ATA home window (see [figure 29](#) on page 47) displays.

The home window consists of the following sections:

- “System Status pane” on page 49
- “Network, VoIP, Security, and Maintenance Menu” on page 52

System Status pane

The *System Status* pane (see [figure 32](#)) consists of the following sections where you can view the current status and change basic settings of the ATA:

- “Device information” on page 50
- “System status” on page 50
- “Interface status” on page 51
- “Summary status” on page 51
- “VoIP status” on page 51

Note The *Status* pane is replaced when you click on items in the Network, VoIP, Security, and Maintenance menu. To return to the *Status* pane, click *System Status* as shown in [figure 32](#).

System Status

Click here to return to the Status pane

Device Information

Model Type: SN102/2JS
Firmware Version: SN100_US_v1.0.5

WAN Information

- WAN Access Type: Static IP
- IP Address: [10.10.50.70](#)
- IP Subnet Mask: 255.255.255.0
- Default Gateway: 10.10.50.1
- MAC Address: 78:8c:54:27:ab:42

LAN Information

- IP Address: [192.168.1.1](#)
- IP Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1
- MAC Address: 78:8c:54:27:ad:77
- DHCP Server: Enabled

System Status

System Uptime: 2day:22h:23m:13s
Current Date/Time: Mon May 15 19:20:02 2017
System Resource:

CPU Usage: 1%
Memory Usage: 39%

Interface Status

Interface	Status	Rate
WAN	Up	100M
LAN	Down	N/A

Summary Status

DHCP Table ([Details....](#)) Packet Statistics ([Details....](#))
VoIP Status([Details....](#))

VoIP Status

SIP Account	Registration	REG Status	URI
SIP 1	<input type="button" value="UnRegister"/>	Reg Success	2602@10.10.50.10
SIP 2	<input type="button" value="Register"/>	Not Registered	

Figure 32. System Status pane

Device information

The *Device Information* section of the *Status* pane displays model type, firmware version, and information about the WAN (WAN access type, IP address, IP subnet mask, default gateway address, and the MAC address) and information about the LAN (IP address, IP subnet mask, default gateway address, MAC address, and whether the DHCP server is enabled).

Device Information	
Model Type:	SN102/2JS
Firmware Version:	SN100_US_v1.0.5
WAN Information	
- WAN Access Type:	Static IP
- IP Address:	10.10.50.70
- IP Subnet Mask:	255.255.255.0
- Default Gateway:	10.10.50.1
- MAC Address:	78:8c:54:27:ab:42
LAN Information	
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- Default Gateway:	192.168.1.1
- MAC Address:	78:8c:54:27:ad:77
- DHCP Server:	Enabled

Figure 33. Device Information window

Note If you want to change WAN Internet connection settings, a shortcut is to click on the IP Address link under *WAN Information* to display the *Internet Connection* section of the *Network > WAN > Internet Connection* pane.

Note If you want to change LAN settings, a shortcut is to click on the IP Address link under *LAN Information* to display the *LAN Setup* section of the *Network > LAN > LAN Setup* pane.

System status

The *System Status* section of the *Status* pane displays how long the system has been running since the last reset (uptime), the current date and time, the percent of CPU capacity in use, and the percent of memory capacity in use.

System Status	
System Uptime:	2day:22h:23m:13s
Current Date/Time:	Mon May 15 19:20:02 2017
System Resource:	
CPU Usage:	<div style="width: 1%; background-color: #ccc; border: 1px solid #000;"></div> 1%
Memory Usage:	<div style="width: 39%; background-color: #007bff; border: 1px solid #000;"></div> 39%

Figure 34. System Status window

Interface status

The *Interface Status* section of the *Status* pane displays the status (up or down) of the WAN and LAN interfaces, and the rate that data is being transferred across each interface.

Interface Status		
Interface	Status	Rate
WAN	Up	100M
LAN	Down	N/A

Figure 35. Interface Status window

Summary status

The *Summary Status* section of the *Status* pane contains links to windows that display the DHCP table, VoIP SIP status and call statistics, and port packet statistics.

Summary Status	
DHCP Table (Details....)	Packet Statistics (Details....)
VoIP Status(Details....)	

Figure 36. Summary Status window

VoIP status

The *VoIP Status* section of the *Status* pane displays the SIP account registration status and URI value for each SIP account. It also includes (depending on the REG status of the SIP account) a *Register* button you can click to register a SIP account or an *UnRegister* button that will unregister a SIP account.

VoIP Status			
SIP Account	Registration	REG Status	URI
SIP 1	<input type="button" value="UnRegister"/>	Reg Success	2602@10.10.50.10
SIP 2	<input type="button" value="Register"/>	Not Registered	

Figure 37. VoIP Status window

Network, VoIP, Security, and Maintenance Menu

This menu (see [figure 38](#)) has the advanced settings for configuring the ATA. It is where you go to change the following:

- Network settings—WAN, LAN, and NAT (see Chapter 5, "Network Settings" on page 53)
- VoIP settings—SIP, phone, and phone book (see Chapter 6, "VoIP Settings" on page 61)
- Security settings—Firewall, content filter, and ACL (see Chapter 7, "Security Settings" on page 112)
- Maintenance settings—System, tools, and logs (see Chapter 8, "Maintenance Settings" on page 119)

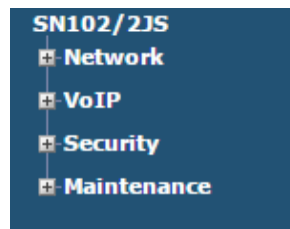


Figure 38. Network, VoIP, Security, and Maintenance Menu

Note As shown in [figure 38](#), the ATA model type is displayed at the top of the menu (*SN102/2JS* in this example).

Note Click on the plus button next to each category to display sub-categories (see [figure 39](#)). The plus button will change to a minus while the sub-categories are displayed.

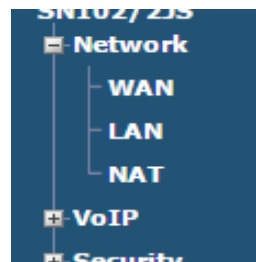


Figure 39. Displaying sub-categories

Chapter 5 **Network Settings**

Chapter contents

Introduction.....	54
WAN Interface.....	54
Static IP	55
DHCP client	56
PPPoE	56
L2TP with WAN	57
LAN Interface	57
NAT Port Forwarding.....	59

Introduction

This chapter describes the following:

- Configuring the WAN interface (see section “WAN Interface”)
- Configuring the LAN interface (see section “LAN Interface” on page 57)
- Configuring NAT (see section “NAT Port Forwarding” on page 59)

WAN Interface

Do the following to display WAN settings:

1. Click on the plus button next to *Network* to display the sub-categories (see figure 40).

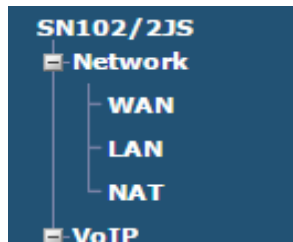


Figure 40. Network sub-categories

2. Click *WAN*. The *Internet Connection* window displays (see figure 41).

A screenshot of the 'Internet Connection' configuration window. The window has a title bar 'Internet Connection' and a subtitle 'ISP Parameters for Internet Access'. It contains several sections: 'WAN Access Type' with a dropdown menu set to 'Static IP'; 'WAN Type Setting' with fields for IP Address (10.10.50.70), Subnet Mask (255.255.255.0), Default Gateway (10.10.50.1), and MTU Size (1500, with a note '(1400-1500 bytes)'); 'VPN Type Setting' with checkboxes for 'Enable PPTP' and 'Enable L2TP', and a 'Remote LAN setting' section with a checkbox for 'SIP Call by LAN IP Address'; 'DNS Servers' with fields for 'First DNS Server' (8.8.8.8) and 'Second DNS Server' (8.8.8.8); 'Clone MAC Address' with radio buttons for 'Clone the computer's MAC address-IP Address' (selected) and 'Use specified MAC Address', with a field for the IP address (0.0.0.0) and a field for the MAC address (000000000000); and 'Other Setting' with a checkbox for 'Enable uPNP'. At the bottom, there are 'Apply' and 'Reset' buttons.

Figure 41. Internet Connection window

A wide area network (WAN) is a network connection connecting one or more local area networks (LANs) together over some distance. For example, two networked office buildings separated by several miles would be referred to as a WAN connection. The size of a WAN and the number of distinct LANs connected to a WAN is not limited by any definition. Therefore, the Internet can be called a WAN.

For most users, Internet access is the primary application. The ATA supports the WAN interface for Internet access and remote access. The WAN settings on the *Internet Connection* window are used to connect to your Internet service provider (ISP). The WAN settings are provided by your ISP and are often referred to as “public settings”.

The following sections will explain details of WAN port Internet access and broadband access set up.

- Static IP WAN access type. Click the *WAN Access Type* drop-down menu, then select *Static IP* (see section “Static IP” on page 55).

The screenshot shows the 'Internet Connection' window. Under the 'ISP Parameters for Internet Access' section, the 'WAN Access Type' is set to 'Static IP' via a drop-down menu.

- DHCP client WAN access type. Click the *WAN Access Type* drop-down menu, then select *Dynamic IP* (see section “DHCP client” on page 56).

The screenshot shows the 'Internet Connection' window. Under the 'ISP Parameters for Internet Access' section, the 'WAN Access Type' is set to 'Dynamic IP' via a drop-down menu.

- PPPoE WAN access type. Click the *WAN Access Type* drop-down menu, then select *PPPoE* (see section “PPPoE” on page 56).

The screenshot shows the 'Internet Connection' window. Under the 'ISP Parameters for Internet Access' section, the 'WAN Access Type' is set to 'PPPoE' via a drop-down menu.

Static IP

If you are a leased-line user with a fixed IP address, type the IP address, subnet mask, gateway address, and DNS (domain name server) address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by three dots (x.x.x.x). The ATA will not accept the IP address if it is not in this format.

Example: 168.95.1.1

Do the following:

1. Type the IP address that was provided by your ISP.
2. Type the subnet mask that was provided by your ISP.
3. Type the default gateway address that was provided by your ISP.

WAN Type Setting	
IP Address:	10.10.50.70
Subnet Mask:	255.255.255.0
Default Gateway:	10.10.50.1

4. Click the *Apply* button.

<input type="button" value="Apply"/> <input type="button" value="Reset"/>

Note If your ISP uses Layer 2 Tunneling Protocol (L2TP) to support virtual private networks (VPNs) or other services, go to section “[L2TP with WAN](#)” on page 57.

DHCP client

When Dynamic Host Configuration Protocol (DHCP) Internet Protocol (Dynamic IP) is selected, the WAN IP address, subnet mask, and default gateway IP address will be obtained automatically. If you are connected to the Internet through a cable modem line, dynamic IP will be assigned.

Note If your ISP uses Layer 2 Tunneling Protocol (L2TP) to support virtual private networks (VPNs) or other services, go to section “[L2TP with WAN](#)” on page 57.

PPPoE

Some ISPs provide DSL-based services and use Point-to-Point Protocol over Ethernet (PPPoE) to establish communication links with end-users. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you need to configure the following:

1. User name: Type the username provided by your ISP.
2. Password: Type the password provided by your ISP.

WAN Type Setting	
User Name:	<input type="text"/>
Password:	<input type="password"/>
Service Name:	<input type="text"/>

3. Click the *Apply* button.

<input type="button" value="Apply"/> <input type="button" value="Reset"/>

Note If your ISP uses Layer 2 Tunneling Protocol (L2TP) to support virtual private networks (VPNs) or other services, go to section “L2TP with WAN” on page 57.

L2TP with WAN

Some ISPs use L2TP with static, DHCP, or PPPoE to establish communication links with end-users.

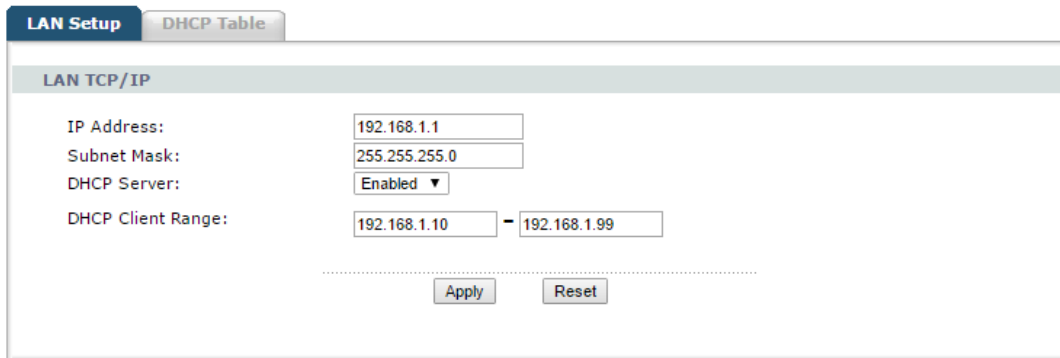
1. Type the L2TP server IP address: that was provided by your VPN /PPTP server provider
2. Type the L2TP user name (L2TP dial-in account)
3. Type the L2TP password (L2TP dial-in password)
4. Type the L2TP MTU size
5. If appropriate, click the *Remote LAN setting* check box to *enable SIP Call by LAN IP Address*

6. If appropriate, click the *Remote LAN setting* check box to *enable SIP Call by LAN IP Address*
7. Click the *Apply* button.

LAN Interface

Do the following to display LAN settings:

1. Click on the plus button next to *Network* to display the sub-categories (see [figure 40](#) on page 54).
2. Click *LAN*. The *LAN Setup* window displays (see [figure 41](#) on page 54).



The screenshot shows a web-based configuration interface for LAN settings. At the top, there are two tabs: "LAN Setup" (selected) and "DHCP Table". Below the tabs is a section titled "LAN TCP/IP". This section contains four rows of settings:

- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0
- DHCP Server: Enabled (with a dropdown arrow)
- DHCP Client Range: 192.168.1.10 - 192.168.1.99

At the bottom of the "LAN TCP/IP" section, there are two buttons: "Apply" and "Reset".

Figure 42. LAN setup window

A local area network (LAN) is a network of computers or other devices that are in relatively close range of each other. For example, devices in a home or office building would be considered part of a local area network.

The LAN Setup window contains the LAN TCP/IP interface settings for the ATA. These settings may be referred to as "private settings". As the LAN IP address is private to your internal network and cannot be seen on the Internet, you can change the LAN IP address if needed.

Do the following:

1. Type the IP address that was provided by your ISP. The default address is *192.168.1.1*.
2. Type the subnet mask that was provided by your ISP. The default is *255.255.255.0*.



This is a close-up view of the "LAN TCP/IP" section from the screenshot above. It shows the "IP Address" field containing "192.168.1.1" and the "Subnet Mask" field containing "255.255.255.0".

3. If you will be using a DHCP Server, click on the drop-down menu, then select Enabled.

DHCP stands for Dynamic Host Control Protocol. The DHCP server gives out IP addresses when a device is starting up and requests an IP address to be logged onto the network. The device must be set as a DHCP client to "Obtain the IP address automatically". By default, the DHCP Server is enabled in the unit. The DHCP address pool contains the range of the IP address that will automatically be assigned to the clients on the network.

DHCP client computers connected to the unit will have their information displayed in the DHCP Client List table (click the *DHCP Table* tab to display the table). The table displays the type, host name, IP address, MAC address, description, and expired time of the DHCP lease for each client computer.

IP Address	Host Name	MAC Address
192.168.1.100	sam-38a7a156f43	00:e0:91:01:4b:97

Figure 43. DHCP Table window

DHCP Server is a useful tool that automates the assignment of IP addresses to numbers of computers in your network. The server maintains a pool of IP addresses that you use to create scopes. (A DHCP scope is a collection of IP addresses and TCP/IP configuration parameters that are available for DHCP clients to lease.) Then, the server automatically allocates these IP addresses and related TCP/IP configuration settings to DHCP-enabled clients in the network. The DHCP Server leases the IP addresses to clients for a period that you specify when you create a scope. A lease becomes inactive when it expires. Through the DHCP Server, you can reserve specific IP addresses permanently for hardware devices that must have a static IP address (e.g., a DNS Server).

An advantage of using DHCP is that the service assigns addresses dynamically. The DHCP Server returns addresses that are no longer in use to the IP addresses pool so that the server can reallocate them to other machines in the network. If you disable this DHCP, you would have to manually configure IP for new computers, keep track of IP addresses so that you could reassign addresses that clients aren't using, and reconfigure computers that you move from one subnet to another. The DHCP Static MAP table lists all MAC and IP address which are active now.

4. Set the *Assigned DHCP IP Address* by typing the starting IP address for the DHCP server's IP assignment and the ending IP address for the DHCP server's IP assignment.
5. Set the *DHCP IP Lease Time* by assigning the length of time for the IP lease. The default setting is 86400 seconds.
6. Click the *Apply* button.

Apply

Reset

NAT Port Forwarding

Port forwarding is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. In other words, port forwarding is used when someone on an outside network (public network) wants to access a service running on a private network machine. An example where port forwarding is applicable is if you plan to run a web, email, or file server on your computer.

Do the following to display port forwarding settings:

1. Click on the plus button next to *Network* to display the sub-categories (see [figure 40](#) on page 54).
2. Click *NAT*. The *Port Forwarding* window displays (see [figure 44](#)).

Port Forwarding

Default Server Setup

Default Server : 0.0.0.0

Forward Setting

Enable Port Forwarding

IP Address: Protocol: Both Port Range: - Comment:

Current Forward Table

Local IP Address	Protocol	Port Range	Comment	Select
------------------	----------	------------	---------	--------

Figure 44. Port Forwarding window

Entries in this table enable you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or email server on the private local network behind your gateway's NAT firewall.

Chapter 6 **VoIP Settings**

Chapter contents

Introduction	63
SIP	63
Configuring SN101/1JS/E (1 FXS) ATA SIP settings	63
SIP Settings	64
Edit SIP Settings window	66
Advanced Edit SIP Settings window	68
SIP Advanced	70
Forward Setting	71
Fax Option	71
P-Asserted-Identity	71
Dial Termination Key	72
Session Timer	72
MWI (Message Waiting Indication)	72
DND (Do Not Disturb)	73
Block Anonymous Call	73
Codec Setting	73
QoS	74
ToS	74
VLAN Tagging	74
Configuring SN102/2JS/E (2 FXS) ATA SIP settings	75
SIP Settings	76
Edit SIP Settings window	78
Advanced Edit SIP Settings window	80
SIP Advanced	82
Forward Setting	83
Fax Option	83
P-Asserted-Identity	83
Dial Termination Key	84
Session Timer	84
MWI (Message Waiting Indication)	84
DND (Do Not Disturb)	85
Block Anonymous Call	85
Codec Setting	85
QoS	86
ToS	86
VLAN Tagging	86
Configuring SN102/1JS1JO/E (1 FXS/1 FXO) ATA SIP settings	87
SIP Settings	88
Edit SIP Settings window	90

Advanced Edit SIP Settings window	92
SIP Advanced	94
Forward Setting.....	94
Fax Option.....	95
P-Asserted-Identity.....	95
Dial Termination Key	95
Session Timer.....	96
MWI (Message Waiting Indication).....	96
DND (Do Not Disturb)	96
Block Anonymous Call.....	97
Codec Setting.....	97
QoS	98
ToS	98
VLAN Tagging	98
Phone.....	99
Analog Phone window	100
Phone Advanced Setup window	101
Jitter Buffer Control settings	102
Voice Activity Detection settings.....	102
G.168 Echo cancellation settings.....	102
Voice Volume Control settings.....	103
Loop Current settings.....	103
Polarity Reversal settings	103
Caller ID settings	104
Hook-Flash Timing settings	104
Hot Line settings.....	105
Common window	105
Pulse Dial Detection settings	105
Dialing Parameter settings	106
Off-Hook Alarm settings	106
DTMF Detection Threshold settings	106
Region window	106
Region settings	106
Customer Ring settings	107
Phone Book.....	107
Speed Dial window	109
Dial Plan with URL window	109
PSTN Line.....	111

Introduction

This chapter describes the following:

- Configuring session initiation protocol (SIP) and quality of service (QoS) settings (see section “SIP”)
- Configuring analog phone settings (see section “Phone” on page 99)
- Configuring speed-dial settings (see section “Phone Book” on page 107)
- Configuring public switched telephone network (PSTN) line settings on the SN102/1JS1JO (FXS/FXO model) (see section “PSTN Line” on page 111)

SIP

This section describes configuring SN100 Series ATA SIP and QoS settings. Chose the appropriate section from the following:

- “Configuring SN101/1JS/E (1 FXS) ATA SIP settings” on page 63
- “Configuring SN102/2JS/E (2 FXS) ATA SIP settings” on page 75
- “Configuring SN102/1JS1JO/E (1 FXS/1 FXO) ATA SIP settings” on page 87

Configuring SN101/1JS/E (1 FXS) ATA SIP settings

Do the following to display SIP and QoS settings:

1. Click on the plus button next to *VoIP* to display the sub-categories (see [figure 45](#)).

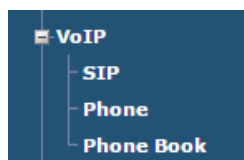


Figure 45. SN101/1JS/E VoIP sub-categories

2. Click *SIP*. The *SIP Settings* window displays (see [figure 46](#) on page 64).

Figure 46. SN101/1JS/E SIP Settings window

- Click the *QoS* tab to display the QoS window (see [figure 47](#)).

Figure 47. QoS window

Go to the appropriate section to modify SIP or QoS settings:

- “SIP Settings”
- “QoS” on page 74

SIP Settings

SIP is a request-response protocol that deals with requests from clients and responses from servers. Participants are identified by SIP URLs. Requests can be sent through any transport protocol. SIP determines the end system to be used for the session, the communication media, and media parameters, and the called party's desire

to engage in the communication. Once these are assured, SIP establishes call parameters at either end of the communication, and handles call transfer and termination.

The *SIP Settings* window displays the following:

- SIP account information (whether the account is active, the account name, user ID, and proxy server address). SIP settings can be modified by clicking on the *Modify* button for the appropriate account (see section “[Edit SIP Settings window](#)” on page 66 for more information).

SIP Setting					
SIP Account	Active	Account Name	User ID	Proxy Server	Modify
SIP 1	<input type="checkbox"/>				

Note Click the *Active* check box to activate or deactivate a SIP account. Click the *Apply* button to save and apply the change.

Note Once you are satisfied with the settings for a SIP account, if the ATA has another SIP account, you can click on the *CopyToSIP2* button to copy the settings to the other account. Click the *Apply* button to save and apply the change.

- NAT traversal information (whether STUN is enabled, the STUN server address, and the STUN server port identifier). STUN {Simple Traversal of UDP through NATs (Network Address Translation)} is a protocol for assisting devices behind a NAT firewall or router with their packet routing.

NAT Traversal	
STUN	<input type="checkbox"/> Enable
STUN Server Address	<input type="text"/>
STUN Server Port	<input type="text" value="3478"/>

Note Click the *Enable* check box to activate or deactivate STUN. Click the *Apply* button to save and apply the change.

- *Set User Header to Phone* information. Click the check box to enable *Set User Header to Phone* to have the device add a “user=phone” parameter to the SIP URI before sending a SIP INVITE request. This parameter indicates the user part of the SIP URI (<user>@<sipserver>) the device is calling is a valid telephone number.(user name and password). Click the *Apply* button to save and apply the change

Set User Header To Phone	
Set User Header To Phone	<input type="checkbox"/> Enable

- *Bind T.38 RTP Port* information. If you need to send fax messages using T.38 and want to always use the same port number for transmitted and received T.38 packets, click the radio button to select *Use Original RTP Port*. Otherwise, select *Assign Port for Reinvite* to have the device chooses a port randomly for T.38 after the re-invite process. Click the *Apply* button to save and apply the change

Figure 48. Edit SIP Settings window

Edit SIP Settings window. The Edit SIP Settings window (see [figure 48](#)) displays the following sections;

- SIP settings
- Authentication settings

SIP Settings. This section displays the following:

- Account Name: Type the name you want displayed.
- Number: Type the number provided by your ISP.

- SIP Display Name: Type the name you want displayed.
- SIP Server Address: Type the address.
- Backup SIP Proxy Server: Click to enable or disable the backup proxy server
- Backup1 Server Address: This setting appears if Backup SIP Proxy Server is enabled. Type the address.
- Backup2 Server Address: This setting appears if Backup SIP Proxy Server is enabled. Type the address.
- SIP Server Port: Type the Proxy port number provided by your ISP.
- SIP Server Domain: Type the SIP domain provided by your ISP.
- Register Expire (sec): SIP registration expired time (default is 600 and needed for calls through the satellite connection).
- Outbound Proxy Server: Click to enable or disable the outbound proxy server
- Outbound Proxy Address: Type the address provided by your ISP. If your ISP did not provide the information, you can skip this item.
- Outbound Proxy Port: Type the port number provided by your ISP.

Authentication Settings. This section displays the following:

- User Name: Type the Register Name provided by your ISP.
- Password: Type the Register Password provided by your ISP.

If you are satisfied with the settings, click the *Apply* button to save and apply the changes.

if you need to change the following:


- Advanced SIP settings
- Forwarding settings
- Fax option settings
- P-Asserted-Identity setting
- Dial termination key setting
- Session timer settings
- MWI (message waiting indication) settings
- DND (do not disturb) settings
- Block anonymous call setting
- Codec settings

Go to section “[Advanced Edit SIP Settings window](#)” on page 68. Otherwise, SIP settings are complete.

Advanced Edit SIP Settings window

To display the Advanced Edit SIP Settings window, do the following:

1. Click *SIP* under the *VoIP* submenu.
2. Click the *Modify* button in the *SIP Setting* section of the *SIP Settings* window.

SIP Setting					
SIP Account	Active	Account Name	User ID	Proxy Server	Modify
SIP 1	<input checked="" type="checkbox"/>		2602	10.10.50.10	

3. Click the *Advanced* button to display the Advanced Edit SIP Settings window.



The Advanced Edit SIP Settings window (see [figure 49](#) on page 69) displays the following:

- Advanced SIP settings (see section “[SIP Advanced](#)” on page 70)
- Forwarding settings (see section “[Forward Setting](#)” on page 71)
- Fax settings (see section “[Fax Option](#)” on page 71)
- P-Asserted-Identity setting (see section “[P-Asserted-Identity](#)” on page 71)
- Dial termination key setting (see section “[Dial Termination Key](#)” on page 72)
- Session timer settings (see section “[Session Timer](#)” on page 72)
- Message waiting indication (MWI) settings (see section “[MWI \(Message Waiting Indication\)](#)” on page 72)
- Do not disturb (DND) settings (see section “[DND \(Do Not Disturb\)](#)” on page 73)

SIP : 1

SIP Advanced

SIP Port

Media Port

Packetization

DTMF Relay

RFC2833 Payload Type

SIP INFO Duration (ms)

Call wait time 0~120 seconds

Call Waiting Enable

DNS SRV Enable

Prohibit coming calls from other SIP server Enable

Send SIP keep-alives seconds (0:Disabled)

Forward Setting

Immediate Forward to Off Enable

Immediate Number

Busy Forward to Off Enable

Busy Number

No Answer Forward to Off Enable

No Answer Number

No Answer Time (sec)

Fax Option

G.711 Fax Passthrough T.38 Fax Relay

P-Asserted-Identity

P-Asserted-Identity Enable

Dial Termination Key

Dial Termination Key Enable

Session Timer

Enable

Minimum Expiration Time (Min 90, Max 65536, Default 90) sec

Maximum Expiration Time (Min 90, Max 65536, Default 1800) sec

MWI (Message Waiting Indication)

Active

Expiration Time (1-65535) sec

DND (Do Not Disturb)

DND Mode Always Enable Disable

From : (hh:mm)

To : (hh:mm)

Block Anonymous Call

Block Anonymous Call Enable

Codec Setting

Type	Priority								Mode
	1	2	3	4	5	6	7	8	
G711-ulaw	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G711-alaw	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G729	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G723	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5.3k
G726-16k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-24k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-32k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-40k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Back Apply Reset

Figure 49. Advanced Edit SIP Settings window

- Block Anonymous Call setting (see section “Block Anonymous Call” on page 73)
- Codec settings (see section “Codec Setting” on page 73)

SIP Advanced. This section displays the following;

- SIP Port Number: Assign the SIP port number of the ATA. The default setting is 5060.
- Media Port: Port number for sending RTP packets. The default setting is 9000.
- Packetization: Select the voice codec packetization interval in milliseconds. The default is 30 ms (for terrestrial connection it is 20ms). This is used to minimize loss that happens during transmission of voice data over the network.
- DTMF Relay: Click the drop-down menu to select RFC2833, SIP INFO, or PCM as indicated by your ISP.
- RFC2833 Payload Type: Sending the DTMF tone as an RTP payload signal.
- SIP INFO Duration (ms): Modify SIP INFO duration time.

SIP Advanced	
SIP Port	5060
Media Port	9000
Packetization	20 ms
DTMF Relay	RFC2833
RFC2833 Payload Type	101
SIP INFO Duration (ms)	250
Call wait time	0 0~128 seconds
Call Waiting	<input type="checkbox"/> Enable
DNS SRV	<input checked="" type="checkbox"/> Enable
Prohibit coming calls from other SIP server	<input checked="" type="checkbox"/> Enable
Send SIP keep-alives	0 seconds (0:Disabled)

- Call wait time (seconds)
- Call Waiting: Click the check box to enable call waiting if the user wants to be informed when there is a new incoming call while he or she is on another call. Disable the feature if the user doesn't want to be informed of a new incoming call.
- DNS SRV: Click the check box to enable having the ATA query your ISP's DNS server for a list of available SIP servers that it maintains.
- Prohibit coming calls from other SIP server: Enable or disable prohibiting incoming calls from other SIP servers.
- Send SIP keep-alives (seconds)

When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Back Apply Reset

Forward Setting. You can set up the phone number you want to forward in this section. There are three forwarding modes:

- **Immediate Forward:** All incoming call will forward to the number you entered. You can input the phone number. If you select this function, then all the incoming call will direct forward to the speed dial number you entered.
- **Busy Forward:** If you are on the phone, the new incoming call will forward to the number you entered.
- **No Answer Forward:** If nobody picks up the phone, the incoming call will forward to the number you entered.

When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Fax Option. G.711 Fax Pass through: Select this if the SN100 should use G.711 to send fax messages. The peer devices must also use G.711.

T.38 Fax Relay: Select this if the SN100 should send fax messages as UDP packets through IP networks. This provides better quality, but it may have interoperability problems. The peer devices must also use T.38.

When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

P-Asserted-Identity. The SIP server authenticates the user that sent the SIP request and then uses the identity from the result of authentication to generate a P-Asserted-Identity header field.

Select enable to have the device look at the P-Asserted-Identity header field which carries the identity of the caller in SIP message, and display the caller's location if available.

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Back Apply Reset

Dial Termination Key. Select enable if you want to use the pound (#) key to tell device to make the phone call immediately.

Dial Termination Key	
Dial Termination Key	<input checked="" type="checkbox"/> Enable

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Back Apply Reset

Session Timer. Select Enable if you want to define how long the ATA waits to receive a session-alive packet for a voice session from the SIP server.

Minimum Expiration Time: Enter the minimum time the ATA waits for a session-alive packet (90-65536 seconds). If a session-alive packet is not received during this time, the voice session is terminated.

Session Timer	
<input type="checkbox"/> Enable	
Minimum Expiration Time	<input type="text" value="90"/> (Min 90, Max 65536, Default 90) sec
Maximum Expiration Time	<input type="text" value="1800"/> (Min 90, Max 65536, Default 1800) sec

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Back Apply Reset

MWI (Message Waiting Indication). Active: Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your SIP service provider must support this feature.

Expiration Time: Keep the default value, unless your SIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the ATA subscribes to the service. Before this time passes, the ATA automatically subscribes again.

MWI (Message Waiting Indication)	
<input type="checkbox"/> Active	
Expiration Time	<input type="text" value="1800"/> (1-65535) sec

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Back Apply Reset

DND (Do Not Disturb). You can set up the DND setting to keep the device silence. You can choose from the following:

- **Always:** All incoming call will be blocked until this feature is disabled by clicking on *Disable*.
- **Enable:** The ATA will be blocked during the time period. If the “From” time is large than the “To” time, the block time will from 00:00 to 23:59

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

.....

Back Apply Reset

Block Anonymous Call. If this feature is enabled, calls that have caller ID information appearing as "private" or "anonymous" will be blocked.

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

.....

Back Apply Reset

Codec Setting. A codec is an algorithm for taking voice or video and compressing the information. This type of codec combines analog-to-digital conversion and digital-to-analog conversion functions in a single chip. The codec is used to compress the voice signal into data packets. Each codec has different bandwidth requirement. There are the following types of codecs:

- G.711/Ulaw
- G.711/Alaw
- G.729 (default and standard for calls through a satellite connection)
- G.723 (5.3k/6.3k bps)
- G.726(16K bps)
- G.726(24K bps)
- G.726(32K bps)
- G.726(40K bps)

Codec Setting									
Type	Priority								Mode
	1	2	3	4	5	6	7	8	
G711-ulaw	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G711-alaw	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G729	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G723	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5.3k ▼
G726-16k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-24k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-32k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-40k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

QoS

Quality of service (QoS) refers to traffic prioritization and resource reservation control mechanisms; it is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

ToS. ToS ensures that when voice and data are being transmitted at the same time, the data will not degrade the voice signal quality. When type of service (ToS) bits are enabled, voice will have the first priority pass through ToS enabled devices.

TOS	
SIP TOS Priority Setting	<input type="text" value="184"/> (0~255)
RTP TOS Priority Setting	<input type="text" value="184"/> (0~255)

VLAN Tagging. You can set the VLAN setting in this section.

VLAN Tagging			
Use VOICE VLAN Tags	<input type="checkbox"/> Enable		
Voice VLAN ID	<input type="text" value="1"/> (0~4090)	Priority	<input type="text" value="7"/> (0~7)
Use DATA VLAN Tags	<input type="checkbox"/> Enable		
Data VLAN ID	<input type="text" value="2"/> (0~4090)	Priority	<input type="text" value="0"/> (0~7)

VLAN tags: if you enable *VOICE VLAN Tags*, and set the *Voice VLAN ID* and *Priority*, then all the incoming packets will be tagged with the IP address and the VLAN ID (VID):

- Voice VLAN ID: Use the voice VLAN ID provided by your ISP to set the *Voice VLAN ID*.
- Data VLAN ID: Use the data VLAN ID provided by your ISP to set the *Data VLAN ID*.
- Priority: Defines user priority, giving eight (2³) priority levels. IEEE 802.1P defines the operation for these 3 user priority bits. Usually this will be provided by your ISP.

Configuring SN102/2JS/E (2 FXS) ATA SIP settings

Do the following to display SIP and QoS settings:

1. Click on the plus button next to *VoIP* to display the sub-categories (see [figure 50](#)).

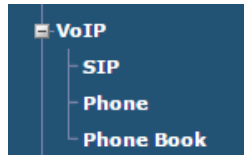


Figure 50. SN102/2JS/E VoIP sub-categories

2. Click *SIP*. The *SIP Settings* window displays (see [figure 51](#)).

 The screenshot shows a web interface with two tabs: "SIP Settings" (selected) and "QoS". Below the tabs is a "SIP Setting" section containing a table with columns: SIP Account, Active, Account Name, User ID, Proxy Server, Modify, and Copy Setting. Below the table are sections for "NAT Traversal" (with STUN settings), "Set User Header To Phone", and "Bind T.38 RTP Port". At the bottom are "Apply" and "Reset" buttons.

SIP Account	Active	Account Name	User ID	Proxy Server	Modify	Copy Setting
SIP 1	<input checked="" type="checkbox"/>		2602	10.10.50.10		CopyToSIP2
SIP 2	<input type="checkbox"/>					CopyToSIP1

NAT Traversal

STUN Enable

STUN Server Address

STUN Server Port

Set User Header To Phone

Set User Header To Phone Enable

Bind T.38 RTP Port

Assign Port for Reinvite Use Original RTP Port

.....

Figure 51. SN102/2JS/E SIP Settings window

3. Click the *QoS* tab to display the QoS window (see [figure 52](#) on page 76).

Figure 52. QoS window

Go to the appropriate section to modify SIP or QoS settings:

- “SIP Settings”
- “QoS” on page 86

SIP Settings

SIP is a request-response protocol that deals with requests from clients and responses from servers. Participants are identified by SIP URLs. Requests can be sent through any transport protocol. SIP determines the end system to be used for the session, the communication media, and media parameters, and the called party's desire to engage in the communication. Once these are assured, SIP establishes call parameters at either end of the communication, and handles call transfer and termination.

The *SIP Settings* window displays the following:

- SIP account information (whether the account is active, the account name, user ID, and proxy server address). SIP settings can be modified by clicking on the *Modify* button for the appropriate account (see section “[Edit SIP Settings window](#)” on page 66 for more information).

SIP Account	Active	Account Name	User ID	Proxy Server	Modify	Copy Setting
SIP 1	<input checked="" type="checkbox"/>		2602	10.10.50.10		CopyToSIP2
SIP 2	<input type="checkbox"/>					CopyToSIP1

Note Click the *Active* check box to activate or deactivate a SIP account. Click the *Apply* button to save and apply the change.

Note Once you are satisfied with the settings for a SIP account, if the ATA has another SIP account, you can click on the *CopyToSIP2* button to copy the

settings to the other account. Click the *Apply* button to save and apply the change.

- NAT traversal information (whether STUN is enabled, the STUN server address, and the STUN server port identifier). STUN {Simple Traversal of UDP through NATs (Network Address Translation)} is a protocol for assisting devices behind a NAT firewall or router with their packet routing.

Note Click the *Enable* check box to activate or deactivate STUN. Click the *Apply* button to save and apply the change.

- *Set User Header to Phone* information. Click the check box to enable *Set User Header to Phone* to have the device add a “user=phone” parameter to the SIP URI before sending a SIP INVITE request. This parameter indicates the user part of the SIP URI (<user>@<sipserver>) the device is calling is a valid telephone number.(user name and password). Click the *Apply* button to save and apply the change

- *Bind T.38 RTP Port* information. If you need to send fax messages using T.38 and want to always use the same port number for transmitted and received T.38 packets, click the radio button to select *Use Original RTP Port*. Otherwise, select *Assign Port for Reinvite* to have the device chooses a port randomly for T.38 after the re-invite process. Click the *Apply* button to save and apply the change

Figure 53. Edit SIP Settings window

Edit SIP Settings window. The Edit SIP Settings window (see [figure 53](#)) displays the following sections;

- SIP settings
- Authentication settings

SIP Settings. This section displays the following:

- Account Name: Type can the name you want displayed.
- Number: Type the number provided by your ISP.

- SIP Display Name: Type the name you want displayed.
- SIP Server Address: Type the address.

- Backup SIP Proxy Server: Click to enable or disable the backup proxy server
- Backup1 Server Address: This setting appears if Backup SIP Proxy Server is enabled. Type the address.
- Backup2 Server Address: This setting appears if Backup SIP Proxy Server is enabled. Type the address.
- SIP Server Port: Type the Proxy port number provided by your ISP.
- SIP Server Domain: Type the SIP domain provided by your ISP.
- Register Expire (sec): SIP registration expired time (default is 600 and needed for calls through the satellite connection).
- Outbound Proxy Server: Click to enable or disable the outbound proxy server
- Outbound Proxy Address: Type the address provided by your ISP. If your ISP did not provide the information, you can skip this item.
- Outbound Proxy Port: Type the port number provided by your ISP.

Authentication Settings. This section displays the following:

- User Name: Type the Register Name provided by your ISP.
- Password: Type the Register Password provided by your ISP.



The screenshot shows a web interface for SIP authentication settings. The title bar reads "Authentication". There are two input fields: "User Name" containing the text "2602" and "Password" containing masked characters "*****". Below the input fields, there is a horizontal line and four buttons: "Back", "Apply", "Reset", and "Advanced".

If you are satisfied with the settings, click the *Apply* button to save and apply the changes.

if you need to change the following:



- Advanced SIP settings
- Forwarding settings
- Fax option settings
- P-Asserted-Identity setting
- Dial termination key setting
- Session timer settings
- MWI (message waiting indication) settings
- DND (do not disturb) settings
- Block anonymous call setting
- Codec settings

Go to section [“Advanced Edit SIP Settings window”](#) on page 68. Otherwise, SIP settings are complete.

Advanced Edit SIP Settings window

To display the Advanced Edit SIP Settings window, do the following:

1. Click *SIP* under the *VoIP* submenu.
2. Click the *Modify* button in the *SIP Setting* section of the *SIP Settings* window.

SIP Setting					
SIP Account	Active	Account Name	User ID	Proxy Server	Modify
SIP 1	<input checked="" type="checkbox"/>		2602	10.10.50.10	
SIP 2	<input type="checkbox"/>				

3. Click the *Advanced* button to display the Advanced Edit SIP Settings window.



The Advanced Edit SIP Settings window (see [figure 54](#) on page 81) displays the following:

- Advanced SIP settings (see section “[SIP Advanced](#)” on page 82)
- Forwarding settings (see section “[Forward Setting](#)” on page 83)
- Fax settings (see section “[Fax Option](#)” on page 83)
- P-Asserted-Identity setting (see section “[P-Asserted-Identity](#)” on page 83)
- Dial termination key setting (see section “[Dial Termination Key](#)” on page 84)
- Session timer settings (see section “[Session Timer](#)” on page 84)
- Message waiting indication (MWI) settings (see section “[MWI \(Message Waiting Indication\)](#)” on page 84)
- Do not disturb (DND) settings (see section “[DND \(Do Not Disturb\)](#)” on page 85)

SIP : 1

SIP Advanced

SIP Port

Media Port

Packetization

DTMF Relay

RFC2833 Payload Type

SIP INFO Duration (ms)

Call wait time 0~128 seconds

Call Waiting Enable

DNS SRV Enable

Prohibit coming calls from other SIP server Enable

Send SIP keep-alives seconds (0:Disabled)

Forward Setting

Immediate Forward to Off Enable

Immediate Number

Busy Forward to Off Enable

Busy Number

No Answer Forward to Off Enable

No Answer Number

No Answer Time (sec)

Fax Option

G.711 Fax Passthrough T.38 Fax Relay

P-Asserted-Identity

P-Asserted-Identity Enable

Dial Termination Key

Dial Termination Key Enable

Session Timer

Enable

Minimum Expiration Time (Min 90, Max 65536, Default 90) sec

Maximum Expiration Time (Min 90, Max 65536, Default 1800) sec

MWI (Message Waiting Indication)

Active

Expiration Time (1-65535) sec

DND (Do Not Disturb)

DND Mode Always Enable Disable

From : (hh:mm)

To : (hh:mm)

Block Anonymous Call

Block Anonymous Call Enable

Codec Setting

Type	Priority								Mode
	1	2	3	4	5	6	7	8	
G711-ulaw	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G711-alaw	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G729	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G723	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5.3k
G726-16k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-24k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-32k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-40k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Back Apply Reset

Figure 54. Advanced Edit SIP Settings window

- Block Anonymous Call setting (see section “Block Anonymous Call” on page 85)
- Codec settings (see section “Codec Setting” on page 85)

SIP Advanced. This section displays the following;

- SIP Port Number: Assign the SIP port number of the ATA. The default setting is 5060.
- Media Port: Port number for sending RTP packets. The default setting is 9000.
- Packetization: Select the voice codec packetization interval in milliseconds. The default is 30 ms (for terrestrial connection it is 20ms). This is used to minimize loss that happens during transmission of voice data over the network.
- DTMF Relay: Click the drop-down menu to select RFC2833, SIP INFO, or PCM as indicated by your ISP.
- RFC2833 Payload Type: Sending the DTMF tone as an RTP payload signal.
- SIP INFO Duration (ms): Modify SIP INFO duration time.

SIP Advanced	
SIP Port	5060
Media Port	9000
Packetization	20 ms
DTMF Relay	RFC2833
RFC2833 Payload Type	101
SIP INFO Duration (ms)	250
Call wait time	0 0~128 seconds
Call Waiting	<input type="checkbox"/> Enable
DNS SRV	<input checked="" type="checkbox"/> Enable
Prohibit coming calls from other SIP server	<input checked="" type="checkbox"/> Enable
Send SIP keep-alives	0 seconds (0:Disabled)

- Call wait time (seconds)
- Call Waiting: Click the check box to enable call waiting if the user wants to be informed when there is a new incoming call while he or she is on another call. Disable the feature if the user doesn't want to be informed of a new incoming call.
- DNS SRV: Click the check box to enable having the ATA query your ISP's DNS server for a list of available SIP servers that it maintains.
- Prohibit coming calls from other SIP server: Enable or disable prohibiting incoming calls from other SIP servers.
- Send SIP keep-alives (seconds)

When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Forward Setting. You can set up the phone number you want to forward in this section. There are three forwarding modes:

- **Immediate Forward:** All incoming call will forward to the number you entered. You can input the phone number. If you select this function, then all the incoming call will direct forward to the speed dial number you entered.
- **Busy Forward:** If you are on the phone, the new incoming call will forward to the number you entered.
- **No Answer Forward:** If nobody picks up the phone, the incoming call will forward to the number you entered.

When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Fax Option. G.711 Fax Pass through: Select this if the SN100 should use G.711 to send fax messages. The peer devices must also use G.711.

T.38 Fax Relay: Select this if the SN100 should send fax messages as UDP packets through IP networks. This provides better quality, but it may have interoperability problems. The peer devices must also use T.38.

When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

P-Asserted-Identity. The SIP server authenticates the user that sent the SIP request and then uses the identity from the result of authentication to generate a P-Asserted-Identity header field.

Select enable to have the device look at the P-Asserted-Identity header field which carries the identity of the caller in SIP message, and display the caller's location if available.

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Back Apply Reset

Dial Termination Key. Select enable if you want to use the pound (#) key to tell device to make the phone call immediately.

Dial Termination Key	
Dial Termination Key	<input checked="" type="checkbox"/> Enable

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Back Apply Reset

Session Timer. Select Enable if you want to define how long the ATA waits to receive a session-alive packet for a voice session from the SIP server.

Minimum Expiration Time: Enter the minimum time the ATA waits for a session-alive packet (90-65536 seconds). If a session-alive packet is not received during this time, the voice session is terminated.

Session Timer	
<input type="checkbox"/> Enable	
Minimum Expiration Time	<input type="text" value="90"/> (Min 90, Max 65536, Default 90) sec
Maximum Expiration Time	<input type="text" value="1800"/> (Min 90, Max 65536, Default 1800) sec

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Back Apply Reset

MWI (Message Waiting Indication). Active: Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your SIP service provider must support this feature.

Expiration Time: Keep the default value, unless your SIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the ATA subscribes to the service. Before this time passes, the ATA automatically subscribes again.

MWI (Message Waiting Indication)	
<input type="checkbox"/> Active	
Expiration Time	<input type="text" value="1800"/> (1-65535) sec

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Back Apply Reset

DND (Do Not Disturb). You can set up the DND setting to keep the device silence. You can choose from the following:

- **Always:** All incoming call will be blocked until this feature is disabled by clicking on *Disable*.
- **Enable:** The ATA will be blocked during the time period. If the “From” time is large than the “To” time, the block time will from 00:00 to 23:59

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Block Anonymous Call. If this feature is enabled, calls that have caller ID information appearing as "private" or "anonymous" will be blocked.

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Codec Setting. A codec is an algorithm for taking voice or video and compressing the information. This type of codec combines analog-to-digital conversion and digital-to-analog conversion functions in a single chip. The codec is used to compress the voice signal into data packets. Each codec has different bandwidth requirement. There are the following types of codecs:

- G.711/Ulaw
- G.711/Alaw
- G.729 (default and standard for calls through a satellite connection)
- G.723 (5.3k/6.3k bps)
- G.726(16K bps)
- G.726(24K bps)
- G.726(32K bps)
- G.726(40K bps)

Codec Setting									
Type	Priority								Mode
	1	2	3	4	5	6	7	8	
G711-ulaw	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G711-alaw	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G729	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G723	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5.3k ▾
G726-16k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-24k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-32k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-40k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

QoS

Quality of service (QoS) refers to traffic prioritization and resource reservation control mechanisms; it is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

ToS. ToS ensures that when voice and data are being transmitted at the same time, the data will not degrade the voice signal quality. When type of service (ToS) bits are enabled, voice will have the first priority pass through ToS enabled devices.

TOS		
SIP TOS Priority Setting	<input type="text" value="184"/>	(0~255)
RTP TOS Priority Setting	<input type="text" value="184"/>	(0~255)

VLAN Tagging. You can set the VLAN setting in this section.

VLAN Tagging			
Use VOICE VLAN Tags	<input type="checkbox"/> Enable		
Voice VLAN ID	<input type="text" value="1"/>	(0~4090)	Priority <input type="text" value="7"/> (0~7)
Use DATA VLAN Tags	<input type="checkbox"/> Enable		
Data VLAN ID	<input type="text" value="2"/>	(0~4090)	Priority <input type="text" value="0"/> (0~7)

VLAN tags: if you enable *VOICE VLAN Tags*, and set the *Voice VLAN ID* and *Priority*, then all the incoming packets will be tagged with the IP address and the VLAN ID (VID):

- Voice VLAN ID: Use the voice VLAN ID provided by your ISP to set the *Voice VLAN ID*.
- Data VLAN ID: Use the data VLAN ID provided by your ISP to set the *Data VLAN ID*.
- Priority: Defines user priority, giving eight (2³) priority levels. IEEE 802.1P defines the operation for these 3 user priority bits. Usually this will be provided by your ISP.

Configuring SN102/1JS1JO/E (1 FXS/1 FXO) ATA SIP settings

Do the following to display SIP and QoS settings:

1. Click on the plus button next to *VoIP* to display the sub-categories (see [figure 55](#)).

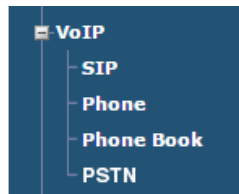


Figure 55. SN102/1JS1JO/E VoIP sub-categories

2. Click *SIP*. The *SIP Settings* window displays (see [figure 56](#)).

SIP Account	Active	Account Name	User ID	Proxy Server	Modify
SIP 1	<input type="checkbox"/>				

NAT Traversal

STUN Enable

STUN Server Address

STUN Server Port

Set User Header To Phone

Set User Header To Phone Enable

Bind T.38 RTP Port

Assign Port for Reinvite Use Original RTP Port

Apply Reset

Figure 56. SN102/1JS1JO/E SIP Settings window

3. Click the *QoS* tab to display the QoS window (see [figure 57](#) on page 88).

Figure 57. QoS window

Go to the appropriate section to modify SIP or QoS settings:

- “SIP Settings”
- “QoS” on page 98

SIP Settings

SIP is a request-response protocol that deals with requests from clients and responses from servers. Participants are identified by SIP URLs. Requests can be sent through any transport protocol. SIP determines the end system to be used for the session, the communication media, and media parameters, and the called party's desire to engage in the communication. Once these are assured, SIP establishes call parameters at either end of the communication, and handles call transfer and termination.

The *SIP Settings* window displays the following:

- SIP account information (whether the account is active, the account name, user ID, and proxy server address). SIP settings can be modified by clicking on the *Modify* button for the appropriate account (see section “[Edit SIP Settings window](#)” on page 90 for more information).

SIP Setting					
SIP Account	Active	Account Name	User ID	Proxy Server	Modify
SIP 1	<input type="checkbox"/>				

Note Click the *Active* check box to activate or deactivate a SIP account. Click the *Apply* button to save and apply the change.

Note Once you are satisfied with the settings for a SIP account, if the ATA has another SIP account, you can click on the *CopyToSIP2* button to copy the settings to the other account. Click the *Apply* button to save and apply the change.

- NAT traversal information (whether STUN is enabled, the STUN server address, and the STUN server port identifier). STUN {Simple Traversal of UDP through NATs (Network Address Translation)} is a protocol for assisting devices behind a NAT firewall or router with their packet routing.

Note Click the *Enable* check box to activate or deactivate STUN. Click the *Apply* button to save and apply the change.

- *Set User Header to Phone* information. Click the check box to enable *Set User Header to Phone* to have the device add a “user=phone” parameter to the SIP URI before sending a SIP INVITE request. This parameter indicates the user part of the SIP URI (<user>@<sipserver>) the device is calling is a valid telephone number.(user name and password). Click the *Apply* button to save and apply the change

- *Bind T.38 RTP Port* information. If you need to send fax messages using T.38 and want to always use the same port number for transmitted and received T.38 packets, click the radio button to select *Use Original RTP Port*. Otherwise, select *Assign Port for Reinvite* to have the device chooses a port randomly for T.38 after the re-invite process. Click the *Apply* button to save and apply the change

Figure 58. Edit SIP Settings window

Edit SIP Settings window. The Edit SIP Settings window (see [figure 58](#)) displays the following sections;

- SIP settings
- Authentication settings

SIP Settings. This section displays the following:

- Account Name: Type can the name you want displayed.
- Number: Type the number provided by your ISP.

- SIP Display Name: Type the name you want displayed.
- SIP Server Address: Type the address.

- Backup SIP Proxy Server: Click to enable or disable the backup proxy server
- Backup1 Server Address: This setting appears if Backup SIP Proxy Server is enabled. Type the address.
- Backup2 Server Address: This setting appears if Backup SIP Proxy Server is enabled. Type the address.
- SIP Server Port: Type the Proxy port number provided by your ISP.
- SIP Server Domain: Type the SIP domain provided by your ISP.
- Register Expire (sec): SIP registration expired time (default is 600 and needed for calls through the satellite connection).
- Outbound Proxy Server: Click to enable or disable the outbound proxy server
- Outbound Proxy Address: Type the address provided by your ISP. If your ISP did not provide the information, you can skip this item.
- Outbound Proxy Port: Type the port number provided by your ISP.

Authentication Settings. This section displays the following:

- User Name: Type the Register Name provided by your ISP.
- Password: Type the Register Password provided by your ISP.

The screenshot shows a web-based configuration window titled "Authentication". It features two text input fields. The first field, labeled "User Name", contains the text "2602". The second field, labeled "Password", contains a series of asterisks "*****". Below these fields, there is a horizontal line followed by four buttons: "Back", "Apply", "Reset", and "Advanced".

If you are satisfied with the settings, click the *Apply* button to save and apply the changes.

if you need to change the following:


- Advanced SIP settings
- Forwarding settings
- Fax option settings
- P-Asserted-Identity setting
- Dial termination key setting
- Session timer settings
- MWI (message waiting indication) settings
- DND (do not disturb) settings
- Block anonymous call setting
- Codec settings

Go to section [“Advanced Edit SIP Settings window”](#) on page 92. Otherwise, SIP settings are complete.

Advanced Edit SIP Settings window

To display the Advanced Edit SIP Settings window, do the following:

1. Click *SIP* under the *VoIP* submenu.
2. Click the *Modify* button in the *SIP Setting* section of the *SIP Settings* window.

SIP Setting					
SIP Account	Active	Account Name	User ID	Proxy Server	Modify
SIP 1	<input checked="" type="checkbox"/>		2602	10.10.50.10	

3. Click the *Advanced* button to display the Advanced Edit SIP Settings window.



The Advanced Edit SIP Settings window (see [figure 49](#) on page 69) displays the following:

- Advanced SIP settings (see section “[SIP Advanced](#)” on page 94)
- Forwarding settings (see section “[Forward Setting](#)” on page 94)
- Fax settings (see section “[Fax Option](#)” on page 95)
- P-Asserted-Identity setting (see section “[P-Asserted-Identity](#)” on page 95)
- Dial termination key setting (see section “[Dial Termination Key](#)” on page 95)
- Session timer settings (see section “[Session Timer](#)” on page 96)
- Message waiting indication (MWI) settings (see section “[MWI \(Message Waiting Indication\)](#)” on page 96)
- Do not disturb (DND) settings (see section “[DND \(Do Not Disturb\)](#)” on page 96)
- Block Anonymous Call setting (see section “[Block Anonymous Call](#)” on page 97)
- Codec settings (see section “[Codec Setting](#)” on page 97)

SIP : 1

SIP Advanced

SIP Port

Media Port

Packetization

DTMF Relay

RFC2833 Payload Type

SIP INFO Duration (ms)

Call wait time 0~128 seconds

Call Waiting Enable

DNS SRV Enable

Prohibit coming calls from other SIP server Enable

Send SIP keep-alives seconds (0:Disabled)

Forward Setting

Immediate Forward to Off Enable

Immediate Number

Busy Forward to Off Enable

Busy Number

No Answer Forward to Off Enable

No Answer Number

No Answer Time (sec)

Fax Option

G.711 Fax Passthrough T.38 Fax Relay

P-Asserted-Identity

P-Asserted-Identity Enable

Dial Termination Key

Dial Termination Key Enable

Session Timer

Enable

Minimum Expiration Time (Min 90, Max 65536, Default 90) sec

Maximum Expiration Time (Min 90, Max 65536, Default 1800) sec

MWI (Message Waiting Indication)

Active

Expiration Time (1-65535) sec

DND (Do Not Disturb)

DND Mode Always Enable Disable

From : (hh:mm)

To : (hh:mm)

Block Anonymous Call

Block Anonymous Call Enable

Codec Setting

Type	Priority								Mode
	1	2	3	4	5	6	7	8	
G711-ulaw	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G711-alaw	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G729	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G723	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5.3k
G726-16k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-24k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-32k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-40k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Back Apply Reset

Figure 59. Advanced Edit SIP Settings window

SIP Advanced. This section displays the following;

- **SIP Port Number:** Assign the SIP port number of the ATA. The default setting is 5060.
- **Media Port:** Port number for sending RTP packets. The default setting is 9000.
- **Packetization:** Select the voice codec packetization interval in milliseconds. The default is 30 ms (for terrestrial connection it is 20ms). This is used to minimize loss that happens during transmission of voice data over the network.
- **DTMF Relay:** Click the drop-down menu to select RFC2833, SIP INFO, or PCM as indicated by your ISP.
- **RFC2833 Payload Type:** Sending the DTMF tone as an RTP payload signal.
- **SIP INFO Duration (ms):** Modify SIP INFO duration time.

SIP Advanced	
SIP Port	5060
Media Port	9000
Packetization	20 ms ▼
DTMF Relay	RFC2833 ▼
RFC2833 Payload Type	101
SIP INFO Duration (ms)	250
Call wait time	0 0~128 seconds
Call Waiting	<input type="checkbox"/> Enable
DNS SRV	<input checked="" type="checkbox"/> Enable
Prohibit coming calls from other SIP server	<input checked="" type="checkbox"/> Enable
Send SIP keep-alives	0 seconds (0:Disabled)

- **Call wait time (seconds)**
- **Call Waiting:** Click the check box to enable call waiting if the user wants to be informed when there is a new incoming call while he or she is on another call. Disable the feature if the user doesn't want to be informed of a new incoming call.
- **DNS SRV:** Click the check box to enable having the ATA query your ISP's DNS server for a list of available SIP servers that it maintains.
- **Prohibit coming calls from other SIP server:** Enable or disable prohibiting incoming calls from other SIP servers.
- **Send SIP keep-alives (seconds)**

When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Forward Setting. You can set up the phone number you want to forward in this section. There are three forwarding modes:

- **Immediate Forward:** All incoming call will forward to the number you entered. You can input the phone number. If you select this function, then all the incoming call will direct forward to the speed dial number you entered.

- **Busy Forward:** If you are on the phone, the new incoming call will forward to the number you entered.
- **No Answer Forward:** If nobody picks up the phone, the incoming call will forward to the number you entered.

When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Fax Option. G.711 Fax Pass through: Select this if the SN100 should use G.711 to send fax messages. The peer devices must also use G.711.

T.38 Fax Relay: Select this if the SN100 should send fax messages as UDP packets through IP networks. This provides better quality, but it may have interoperability problems. The peer devices must also use T.38.

When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

P-Asserted-Identity. The SIP server authenticates the user that sent the SIP request and then uses the identity from the result of authentication to generate a P-Asserted-Identity header field.

Select enable to have the device look at the P-Asserted-Identity header field which carries the identity of the caller in SIP message, and display the caller's location if available.

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Dial Termination Key. Select enable if you want to use the pound (#) key to tell device to make the phone call immediately.

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Session Timer. Select *Enable* if you want to define how long the ATA waits to receive a session-alive packet for a voice session from the SIP server.

Minimum Expiration Time: Enter the minimum time the ATA waits for a session-alive packet (90-65536 seconds). If a session-alive packet is not received during this time, the voice session is terminated.

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

MWI (Message Waiting Indication). *Active:* Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your SIP service provider must support this feature.

Expiration Time: Keep the default value, unless your SIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the ATA subscribes to the service. Before this time passes, the ATA automatically subscribes again.

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

DND (Do Not Disturb). You can set up the DND setting to keep the device silence. You can choose from the following:

- *Always:* All incoming call will be blocked until this feature is disabled by clicking on *Disable*.
- *Enable:* The ATA will be blocked during the time period. If the “From” time is large than the “To” time, the block time will from 00:00 to 23:59

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Block Anonymous Call. If this feature is enabled, calls that have caller ID information appearing as "private" or "anonymous" will be blocked.

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Codec Setting. A codec is an algorithm for taking voice or video and compressing the information. This type of codec combines analog-to-digital conversion and digital-to-analog conversion functions in a single chip. The codec is used to compress the voice signal into data packets. Each codec has different bandwidth requirement. There are the following types of codecs:

- G.711/Ulaw
- G.711/Alaw
- G.729 (default and standard for calls through a satellite connection)
- G.723 (5.3k/6.3k bps)
- G.726(16K bps)
- G.726(24K bps)
- G.726(32K bps)
- G.726(40K bps)

Codec Setting									
Type	Priority								Mode
	1	2	3	4	5	6	7	8	
G711-ulaw	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G711-alaw	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G729	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G723	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5.3k ▾
G726-16k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-24k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-32k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
G726-40k	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

QoS

Quality of service (QoS) refers to traffic prioritization and resource reservation control mechanisms; it is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

ToS. ToS ensures that when voice and data are being transmitted at the same time, the data will not degrade the voice signal quality. When type of service (ToS) bits are enabled, voice will have the first priority pass through ToS enabled devices.

TOS		
SIP TOS Priority Setting	<input type="text" value="184"/>	(0~255)
RTP TOS Priority Setting	<input type="text" value="184"/>	(0~255)

VLAN Tagging. You can set the VLAN setting in this section.

VLAN Tagging			
Use VOICE VLAN Tags	<input type="checkbox"/> Enable		
Voice VLAN ID	<input type="text" value="1"/> (0~4090)	Priority	<input type="text" value="7"/> (0~7)
Use DATA VLAN Tags	<input type="checkbox"/> Enable		
Data VLAN ID	<input type="text" value="2"/> (0~4090)	Priority	<input type="text" value="0"/> (0~7)

VLAN tags: if you enable *VOICE VLAN Tags*, and set the *Voice VLAN ID* and *Priority*, then all the incoming packets will be tagged with the IP address and the VLAN ID (VID):

- Voice VLAN ID: Use the voice VLAN ID provided by your ISP to set the *Voice VLAN ID*.
- Data VLAN ID: Use the data VLAN ID provided by your ISP to set the *Data VLAN ID*.
- Priority: Defines user priority, giving eight (2³) priority levels. IEEE 802.1P defines the operation for these 3 user priority bits. Usually this will be provided by your ISP.

Phone

Do the following to display the *Analog Phone* window:

1. Click on the plus button next to *VoIP* to display the *Phone* sub-category (see [figure 60](#)).

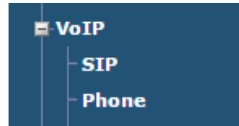


Figure 60. Phone sub-category

2. Click *Phone*. The *Analog Phone* window displays (see [figure 61](#)).

 A web interface window titled 'Analog Phone' with three tabs: 'Analog Phone' (selected), 'Common', and 'Region'. Below the tabs is a 'Port Setting' dropdown menu set to 'Phone 1'. There are two main sections: 'Outgoing Call Use' with radio buttons for 'SIP1' (selected) and 'SIP2'; and 'Incoming Call apply to' with checkboxes for 'SIP1' (checked) and 'SIP2'. At the bottom are 'Apply', 'Reset', and 'Advanced Setup' buttons.

Figure 61. Analog Phone window

3. Click the *Common* tab to display the *Common* window (see [figure 62](#)).

 A web interface window titled 'Analog Phone' with three tabs: 'Analog Phone', 'Common' (selected), and 'Region'. The window contains several settings sections: 'Pulse Dial Detection' with radio buttons for 'Disable' (selected) and 'Enable', and a text input for 'Interdigit Pause Duration' set to '450' (msec); 'Dailing Parameter' with a text input for 'Auto Dial Time' set to '3' (3~9 sec, 0 is disable); 'Off-Hook Alarm' with a text input for 'Off-Hook Alarm Time' set to '15' (10~60 sec, 0 is disable); and 'DTMF Detection Threshold' with a text input for 'DTMF Detection Threshold Level' set to '10' (0 ~ 40, it means 0 ~ -40 dBm). At the bottom are 'Apply' and 'Reset' buttons.

Figure 62. Common window

4. Click the *Region* tab to display the *Region* window (see [figure 63](#) on page 100).

The screenshot shows a web-based configuration interface for a SmartNode 100 Series ATA. At the top, there are three tabs: 'Analog Phone', 'Common', and 'Region'. The 'Region' tab is active. Below the tabs, there are two main sections: 'Region Settings' and 'Customer Ring Setting'. In the 'Region Settings' section, 'Country' is set to 'SWITZERLAND' and 'Call Service Mode' is set to 'Europe Type'. In the 'Customer Ring Setting' section, 'Ring Setting Enable' is unchecked, 'Cadence ON (msec)' is set to 1000, and 'Cadence OFF (msec)' is set to 4000. An 'Apply' button is located at the bottom of the form.

Figure 63. Region window

Go to the appropriate section to modify analog phone, common, or region settings:

- ““Region window” on page 106”
- “Common window” on page 105
- “Region window” on page 106

Analog Phone window

1. If your SN100 ATA has only one FXS port, go to step 2. Otherwise, select *Phone 1* or *Phone 2* from the Port Setting drop-down menu.

Port Setting : Phone 1 ▼

2. Click the *Advance Setup* button. The Advanced Setup window appears (see [figure 64](#) on page 101).

Apply Reset Advanced Setup

Phone Advanced Setup window

Phone Port : 2	
Jitter Buffer Size	
Min delay (ms):	60 ▼
Max delay (ms):	200 ▼
Voice Activity Detection	
VAD	<input type="checkbox"/> Enable
G.168 Echo cancelation	
LEC Tail Length (ms)	2 ▼
Voice Volume Control	
Listening Volume	-3 (-32~31 ,Mute:-32)
Speaking Volume	-3 (-32~31 ,Mute:-32)
Loop Current	
Loop Current	22 mA ▼
Polarity Reversal	
Polarity Reversal	<input type="checkbox"/> Enable
Caller ID setting	
Caller ID Mode	FSK_ETSI ▼
FSK Date & Time Sync	<input checked="" type="checkbox"/> Enable
Short Ring before Caller ID	<input type="checkbox"/> Enable
Dual Tone before Caller ID	<input type="checkbox"/> Enable
Caller ID Prior First Ring	<input type="checkbox"/> Enable
Caller ID DTMF Start Digit	DTMF_A ▼
Caller ID DTMF End Digit	DTMF_C ▼
Private Caller ID	<input type="checkbox"/> Enable
Replace + with 00 for Caller ID	<input type="checkbox"/> Enable
Hook-Flash Timing	
Minimum on-hook time	30 (Minimum:30 ms)
Maximum on-hook time	500 (Maximum:2000 ms)
Hot Line	
Use Hot Line	<input type="checkbox"/> Enable
Hot Line Timer	3 (0~30 seconds)
Hot Line Number	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Figure 64. Phone Advanced Setup window

The Phone Advanced Setup window displays the following;

- Jitter Buffer Size settings (see section “[Jitter Buffer Control settings](#)” on page 102)
- Voice Activity Detection settings (see section “[Voice Activity Detection settings](#)” on page 102)
- G.168 Echo cancellation settings (see section “[G.168 Echo cancellation settings](#)” on page 102)
- Voice Volume Control settings (see section “[Voice Volume Control settings](#)” on page 103)
- Loop Current settings (see section “[Loop Current settings](#)” on page 103)

- Polarity Reversal settings (see section “Polarity Reversal settings” on page 103)
- Caller ID settings (see section “Caller ID settings” on page 104)
- Hook-Flash Timing settings (see section “Hook-Flash Timing settings” on page 104)
- Hot Line settings (see section “Hot Line settings” on page 105)

Jitter Buffer Control settings. Changes in packets arrival time, called jitter, can occur because of network congestion, timing drift, or route changes. The jitter buffer control is a shared data area where voice packets can be stored, collected, and sent to the voice shared buffer in evenly spaced intervals.

- Min delay (ms): Select minimum delay buffer time from the drop-down menu
- Max delay (ms): Select maximum delay buffer time from the drop-down menu

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Back Apply Reset

Voice Activity Detection settings. If this function is enabled, if silence occurs for a period of time, no data will be sent across the network during that period in order to save bandwidth.

Click the check box to enable voice activity detection (VAD).

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Back Apply Reset

G.168 Echo cancellation settings. Select the LEC tail length (ms) from the drop-down menu.

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Back Apply Reset

Voice Volume Control settings. Voice volume control sets the intensity in dB for receiving sound (listening), and for transmitting sound (speaking):

- **Listening Volume:** Sets a specific sound intensity for receiving sound. Type a value from -32 to 31 dB
- **Speaking Volume:** Sets a specific sound intensity for transmitting sound. Type a value from -32 to 31 dB

Note A value of -32 will mute the volume.

Voice Volume Control		
Listening Volume	<input type="text" value="-3"/>	(-32~31 ,Mute:-32)
Speaking Volume	<input type="text" value="-3"/>	(-32~31 ,Mute:-32)

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Loop Current settings. Select the loop current from the drop-down menu.

Loop Current	
Loop Current	<input type="text" value="22 mA"/>

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Polarity Reversal settings. A function that changes the polarity on the current on a FXS phone line to notify billing software or other applications of events like such as a call being answered.

Click the check box to enable polarity reversal.

Polarity Reversal	
Polarity Reversal	<input type="checkbox"/> Enable

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.

Caller ID setting	
Caller ID Mode	FSK_ETSI ▼
FSK Date & Time Sync	<input checked="" type="checkbox"/> Enable
Short Ring before Caller ID	<input type="checkbox"/> Enable
Dual Tone before Caller ID	<input type="checkbox"/> Enable
Caller ID Prior First Ring	<input type="checkbox"/> Enable
Caller ID DTMF Start Digit	DTMF_A ▼
Caller ID DTMF End Digit	DTMF_C ▼
Private Caller ID	<input type="checkbox"/> Enable
Replace + with 00 for Caller ID	<input type="checkbox"/> Enable

Caller ID settings. The following settings are available:

- Caller ID Mode: Click the drop-down menu to select the caller ID mode.
- FSK Date & Time Sync: Click the check box to enable sending FSK date and time to the display device.
- Reverse Polarity before Caller ID: Click the check box to enable sending reverse polarity before caller ID
- Short Ring before Caller ID: Click the check box to enable sending a short ring before caller ID.
- Dual Tone before Caller ID: Click the check box to enable sending dual tone before caller ID.
- Caller ID Prior First Ring: Click the check box to enable sending caller ID before first ring.
- Caller ID DTMF Start Digit: Click the drop-down menu to set the caller ID DTMF start digit.
- Caller ID DTMF END Digit: Click the drop-down menu to set the caller ID DTMF end digit.
- Private Caller ID: A private caller has hidden or otherwise obfuscated their phone number. Often their number displays as “Private Caller”, “Restricted”, “Unknown Caller ID” or “No Caller ID”. Click the check box to enable private caller ID.

When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

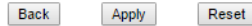
Hook-Flash Timing settings. Hook-flash is a button on a telephone that simulates quickly hanging up then picking up again (a quick off-hook/on-hook/off-hook cycle). This action can signal the telephone exchange to do something. A common use of hook flash is to switch to another incoming call with the call waiting service. Another use is to indicate a request for voice conferencing, for example, a user may use a procedure like the following to initiate three-way calling.

The following settings are available:

- Minimum on-hook time: Type the value (default is 30 ms)
- Maximum on-hook time: Type the value (default is 2000 ms)

Hook-Flash Timing	
Minimum on-hook time	30 (Minimum:30 ms)
Maximum on-hook time	500 (Maximum:2000 ms)

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.



Hot Line settings. This service enables you to call a pre-programmed number simply by lifting the handset.

The following settings are available:

- Use Hot Line: Click the check box to enable the hot line service.
- Hot Line Timer: This feature is typically used for setting up a hot line or warm line, with a 0-second timer delay for the hot line and a non-zero delay for a warm line. Type the value in seconds.
- Hot Line Number: Input the number for the hot line service—This number will be called immediately when the telephone goes off-hook.

The screenshot shows a form titled "Hot Line" with the following fields:

- Use Hot Line: Enable
- Hot Line Timer: (0~30 seconds)
- Hot Line Number:

When you are satisfied with the setting, click the *Apply* button to save and apply the changes.



Common window

The Common window displays the following;

- Pulse Dial Detection settings (see section “[Pulse Dial Detection settings](#)” on page 105)
- Off-Hook Alarm settings (see section “[Off-Hook Alarm settings](#)” on page 106)
- DTMF Detection Threshold settings (see section “[DTMF Detection Threshold settings](#)” on page 106)

Pulse Dial Detection settings

1. Click to enable pulse dial detection if you are connecting a pulse (rotary) dialing telephone to the SN100.

The screenshot shows a form titled "Pulse Dial Detection" with the following fields:

- Disable Enable
- Interdigit Pause Duration: (msec)

2. Type the Interdigit Pause Duration value.
3. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.



Dialing Parameter settings

If no other number is being dialed within this interval, the SN100 will terminate the call. Assign the time interval from 1 to 9 seconds.

Dialing Parameter	
Auto Dial Time	<input type="text" value="3"/> (3~9 sec, 0 is disable)

When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

<input type="button" value="Apply"/>	<input type="button" value="Reset"/>
--------------------------------------	--------------------------------------

Off-Hook Alarm settings

The amount of time the phone can be off-hook before an alarm sounds.

Off-Hook Alarm	
Off-Hook Alarm Time	<input type="text" value="15"/> (10~60 sec, 0 is disable)

When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

<input type="button" value="Apply"/>	<input type="button" value="Reset"/>
--------------------------------------	--------------------------------------

DTMF Detection Threshold settings

Type the DTMF Detection Threshold Level value.

DTMF Detection Threshold	
DTMF Detection Threshold Level	<input type="text" value="10"/> (0 ~ 40, it means 0 ~ -40 dBm)

When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

<input type="button" value="Apply"/>	<input type="button" value="Reset"/>
--------------------------------------	--------------------------------------

Region window

The Region window displays the following;

- Region settings (see section “Region settings” on page 106)
- Customer Ring settings (see section “Customer Ring settings” on page 107)

Region settings

Adjust the tone frequency according to each country

1. Select the country from the drop-down menu

Region Settings	
Country	<input type="text" value="SWITZERLAND"/>
Call Service Mode	<input type="text" value="Europe Type"/>

2. Select the call service mode from the drop-down menu
3. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.



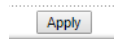
Customer Ring settings

Create custom ring cadences.

1. Click to enable ring setting.

 A screenshot of a web form titled "Customer Ring Setting". It contains three fields: "Ring Setting Enable" with a checkbox, "Cadence ON (msec)" with a text input field containing "1000", and "Cadence OFF (msec)" with a text input field containing "4000".

2. Type the Cadence ON (length of time the tone will sound) value.
3. Type the Cadence OFF (length of time the tone is silent) value.
4. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.



Phone Book

Do the following to display the *Speed Dial* window:

1. Click on the plus button next to *VoIP* to display the *Phone* sub-category (see [figure 65](#)).

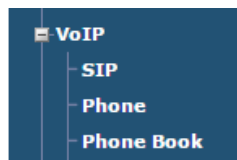


Figure 65. Phone Book sub-category

2. Click *Phone Book*. The *Speed Dial* window displays (see [figure 66](#) on page 108).

Position	Name	Phone Number	Select
#01			<input type="checkbox"/>
#02			<input type="checkbox"/>
#03			<input type="checkbox"/>
#04			<input type="checkbox"/>
#05			<input type="checkbox"/>
#06			<input type="checkbox"/>
#07			<input type="checkbox"/>
#08			<input type="checkbox"/>
#09			<input type="checkbox"/>
#10			<input type="checkbox"/>

Figure 66. Speed Dial window

3. Click the *Dial Plan with URL* tab to display the *Dial Plan with URL* window (see [figure 67](#)).

Port Setting : Phone 1 ▼

Dial Plan with URL

Priority	Applied Target rule			Applied Operation				Select(Enable)
	Lead Number	Min-Max Digits	Strip Digits Length	Prefix Number	Destination IP / URI	Destination SIP Port		
1		~ 0					<input type="checkbox"/>	
2		~ 0					<input type="checkbox"/>	
3		~ 0					<input type="checkbox"/>	
4		~ 0					<input type="checkbox"/>	
5		~ 0					<input type="checkbox"/>	
6		~ 0					<input type="checkbox"/>	
7		~ 0					<input type="checkbox"/>	
8		~ 0					<input type="checkbox"/>	
9		~ 0					<input type="checkbox"/>	
10		~ 0					<input type="checkbox"/>	
11		~ 0					<input type="checkbox"/>	
12		~ 0					<input type="checkbox"/>	
13		~ 0					<input type="checkbox"/>	
14		~ 0					<input type="checkbox"/>	
15		~ 0					<input type="checkbox"/>	
16		~ 0					<input type="checkbox"/>	
17		~ 0					<input type="checkbox"/>	
18		~ 0					<input type="checkbox"/>	
19		~ 0					<input type="checkbox"/>	
20		~ 0					<input type="checkbox"/>	

(* means any)

Figure 67. Dial Plan with URL window

Go to the appropriate section to modify analog phone, common, or region settings:

- “Speed Dial window”
- “Dial Plan with URL window” on page 109

Speed Dial window

Speed Dial lets you define a button or a set of buttons to link to numbers defined in the Speed Dial list.

1. If your SN100 ATA has only one FXS port, go to step 2. Otherwise, select *Phone 1* or *Phone 2* from the Port Setting drop-down menu.

Port Setting : Phone 1 ▼

2. Position: Decide which speed dial shortcut to use from 01 to 10.

Position	Name	Phone Number	Select
#01			<input type="checkbox"/>
#02			<input type="checkbox"/>
#03			<input type="checkbox"/>
#04			<input type="checkbox"/>
#05			<input type="checkbox"/>
#06			<input type="checkbox"/>
#07			<input type="checkbox"/>
#08			<input type="checkbox"/>
#09			<input type="checkbox"/>
#10			<input type="checkbox"/>

3. Name: Type a short name for the phone number shortcut.
4. Phone Number: Enter the desired phone number in the corresponding format that is required, using the ISP of your preference.
5. Repeat steps 2 through 4 to create additional speed dialing shortcuts.
6. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Dial Plan with URL window

Use this window to create dial plan with URL entries that enable users to make peer-to-peer calls. In peer-to-peer calls, a user calls another VoIP device directly without going through a VoIP service provider’s SIP server. Enter the callee’s IP address or domain name. The SN100 sends SIP INVITE requests to the specified peer VoIP device when you dial the SIP number configured in this screen.

1. If your SN100 ATA has only one FXS port, go to step 2. Otherwise, select *Phone 1* or *Phone 2* from the Port Setting drop-down menu.

Dial Plan with URL							
Priority	Applied Target rule		Applied Operation				
	Lead Number	Min-Max Digits	Strip Digits Length	Prefix Number	Destination IP / URI	Destination SIP Port	Select(Enable)
1	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
13	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
14	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
15	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
16	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
17	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
18	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
19	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
20	<input type="text"/>	<input type="text"/> ~ <input type="text"/> 0	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

(* means any)

2. Make the following settings:

Note When a user dials a number *xxxxxxx*, the ATA will check it against this dial plan, first by *Priority* order, and then execute.

- *Lead Number* is the first digit of the call-out dialing number.
- *Min-Max Digits* has two text fields that must be completed: *Min Length* and *Max Length* are the min/max allowed length of the number you can dial.
- *Strip Digits Length* is the number of digits that will be stripped from beginning of the dialed number.
- *Prefix Number* is the digits that will be added to the beginning of the dialed number.
- *Destination IP/ URI* is the IP address/domain name of the destination SN100 that owns this phone number. This for peer-to-peer IP calls.
- *Destination SIP Port* is used to overwrite the UDP port for the destination configured of this rule. Default port is 5060 as per the SIP server settings in Chapter 6.

3. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

PSTN Line

Do the following to display the PSTN Line *General* window:

1. Click on the plus button next to *VoIP* to display the *PSTN LINE* sub-category (see [figure 68](#) on page 111).

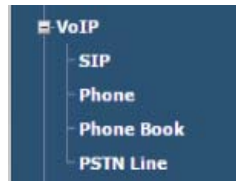


Figure 68. PSTN sub-category

2. Click *PSTN Line*. The *General* window displays (see [figure 69](#)).

 A screenshot of the 'General' configuration window for the PSTN Line. The window has a dark blue header with the word 'General' in white. Below the header, there are two main sections:

- Call through PSTN Line:** This section contains a label 'PSTN Line Prefix Number' followed by a text input field containing the characters '**'.
- Relay to PSTN Line:** This section contains a list of ten numbered input fields, labeled '1.' through '10.', for configuring pass-through numbers.

Figure 69. PSTN Line General window

3. Make the following settings:
 - *Call through PSTN line:* Set up the prefix digit function key. For example, if the PSTN Line Prefix Number is **, it means that the analog phone connected to the FXS port can press **, then get a dial tone of PSTN port to dial destination number via PSTN port.
 - *Relay to PSTN Line:* Up to 10 pass through numbers can be configured. The phone connected to the FXS port, dialing one of these numbers, will cause the call to directly go out on the PSTN line, without routing it to the SIP account. This function may be used for emergency calls such as 911 for USA or 112 for Europe.
4. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.



Chapter 7 **Security Settings**

Chapter contents

Introduction.....	113
Firewall.....	113
Configuring IP Filtering settings	113
Configuring MAC Filtering settings	114
Configuring Port Filtering settings	115
Content Filter.....	116
ACL Setting	117

Introduction

This chapter describes the following:

- Configuring the Firewall settings (see section “[Firewall](#)”)
- Configuring the Content Filter settings (see section “[Content Filter](#)” on page 116)
- Configuring ACL settings (see section “[ACL Setting](#)” on page 117)

Firewall

This section describes configuring SN100 Series ATA IP filtering, MAC filtering, and port filtering settings. Choose the appropriate section from the following:

- “[Configuring IP Filtering settings](#)”
- “[Configuring MAC Filtering settings](#)” on page 114
- “[Configuring Port Filtering settings](#)” on page 115

Configuring IP Filtering settings

Entries in the table (see [figure 71](#) on page 114) are used to restrict IP addresses from the LAN accessing the Internet. Use of such filters can be helpful in securing or restricting your local network.

Do the following to display IP Filtering settings:

1. Click on the plus button next to *Security* to display the sub-categories (see [figure 70](#)).

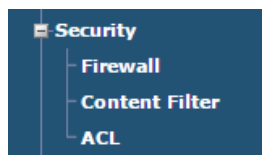


Figure 70. Security sub-categories

2. Click *Firewall*. The *IP Filtering* window displays (see [figure 71](#) on page 114).

The screenshot shows the IP Filtering configuration window. At the top, there are three tabs: 'IP Filtering', 'MAC Filtering', and 'Port Filtering'. The 'IP Filtering' tab is active. Below the tabs is a 'Filter Setting' section with a checkbox for 'Enable IP Filtering'. To the right of the checkbox are three input fields: 'Local IP Address', 'Protocol' (a dropdown menu currently showing 'Both'), and 'Comment'. Below these fields are two buttons: 'Apply' and 'Reset'. Below the 'Filter Setting' section is a 'Current Filter Table' section. It contains a table with four columns: 'Local IP Address', 'Protocol', 'Comment', and 'Select'. Below the table are three buttons: 'Delete Selected', 'Delete All', and 'Reset'.

Figure 71. IP Filtering window

3. *Enable/Disable IP Filtering:* The IP address filter function may be enabled to restrict certain IPs from the LAN accessing the Internet for a specific protocol.
4. The comment field may be used for reference purposes such as “Storage Room PC”
5. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

.....

Configuring MAC Filtering settings

Entries in the table (see [figure 72](#) on page 115) are used to restrict MAC addresses from the LAN accessing the Internet.

Do the following to display MAC Filtering settings:

1. Click on the plus button next to *Security* to display the sub-categories (see [figure 70](#) on page 113).
2. Click *Firewall*. The *IP Filtering* window displays (see [figure 71](#) on page 114).
3. Click the *MAC Filtering* tab to bring it to the front (see [figure 72](#) on page 115).

The screenshot shows the MAC Filtering configuration window. At the top, there are three tabs: 'IP Filtering', 'MAC Filtering' (which is active), and 'Port Filtering'. Below the tabs is a 'Filter Setting' section containing a checkbox labeled 'Enable MAC Filtering'. To the right of the checkbox are two input fields: 'MAC Address' and 'Comment'. Below these fields are two buttons: 'Apply' and 'Reset'. Underneath is a 'Current Filter Table' section, which is currently empty. Below the table are three buttons: 'Delete Selected', 'Delete All', and 'Reset'.

Figure 72. MAC filtering window

4. Enable/Disable MAC Filtering: Enable/Disable MAC filtering: Specify which MAC addresses are not allowed to access the Internet. The comment field may be used for reference purposes such as “Storage Room PC”.
5. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

.....

Configuring Port Filtering settings

Entries in the table (see [figure 73](#) on page 116) are used to restrict traffic based on certain ports, originating from hosts in the LAN destined to the Internet.

Do the following to display Port Filtering settings:

1. Click on the plus button next to *Security* to display the sub-categories (see [figure 70](#) on page 113).
2. Click *Firewall*. The *IP Filtering* window displays (see [figure 71](#) on page 114).
3. Click the *Port Filtering* tab to bring it to the front (see [figure 73](#) on page 116).

The screenshot shows the 'Port Filtering' configuration window. At the top, there are three tabs: 'IP Filtering', 'MAC Filtering', and 'Port Filtering'. The 'Port Filtering' tab is active. Below the tabs is a 'Filter Setting' section containing a checkbox for 'Enable Port Filtering', a 'Port Range' field with two input boxes, a 'Protocol' dropdown menu set to 'Both', and a 'Comment' text field. Below these fields are 'Apply' and 'Reset' buttons. The 'Current Filter Table' section shows a table with columns: 'Port Range', 'Protocol', 'Comment', and 'Select'. Below the table are 'Delete Selected', 'Delete All', and 'Reset' buttons.

Figure 73. Port filtering window

4. Enable/Disable Port Filtering: Restrict hosts from LAN accessing the Internet, by specific ports.
5. The comment field may be used for reference purposes such as “Storage Room PC”.
6. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

.....

Content Filter

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

Do the following to display Content Filter settings:

1. Click on the plus button next to *Security* to display the sub-categories (see [figure 70](#) on page 113).
2. Click *Content Filter*. The *Content Filter* window displays (see [figure 74](#) on page 117).

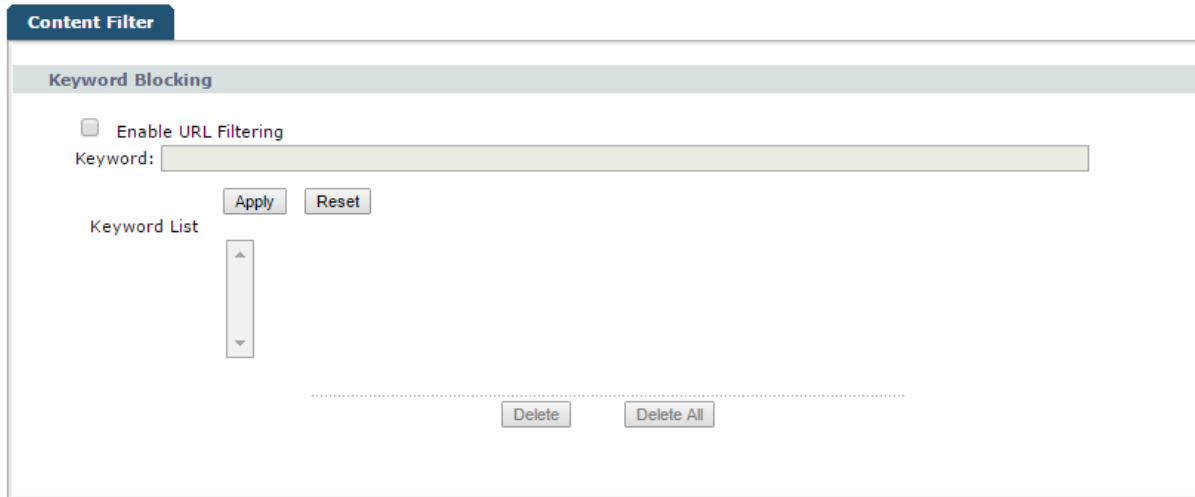


Figure 74. Content Filter Window

3. Make the following settings:
 - Enable/Disable the URL filter function (default setting is disable).
 - Enter the keywords you would like to be blocked
4. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

.....

Apply Reset

ACL Setting

The ACL is being used to control which services of the SmartNode 100 ATA can be accessed from WAN or LAN. Do the following to display the ACL Setting window:

1. Click on the plus button next to *Security* to display the sub-categories (see [figure 70](#) on page 113).
2. Click *ACL Setting*. The *ACL Setting* window displays (see [figure 75](#) on page 118).

ACL Setting

ACL Setup

Services	LAN	WAN	Port
HTTP	<input checked="" type="checkbox"/> enable	<input checked="" type="checkbox"/> enable	80
TELNET	<input checked="" type="checkbox"/> enable	<input checked="" type="checkbox"/> enable	23

Response ICMP Setup

From	Enable
WAN	<input checked="" type="checkbox"/>

Apply
Reset

Figure 75. ACL Setting window

3. Make the following settings in the *ACL Setup* section:
 - Enable/Disable the LAN and WAN HTTP service as needed (default setting is enable).
 - Enable/Disable the LAN and WAN TELNET service as needed (default setting is enable).
4. Enable/Disable the From LAN setting (default setting is enable).
5. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Apply
Reset

Chapter 8 Maintenance Settings

Chapter contents

Introduction	120
System	120
Configuring General System settings	120
Configuring Administrator Account's user name and password	121
Configuring User Account's user name and password	122
Configuring Time settings	122
Setting the time manually	123
Configuring Auto Provision settings	123
Configuring Dynamic DNS settings	124
Configuring TR069 settings	125
Tools	127
Configuration settings	127
Backup Configuration	128
Restore Configuration	128
Reset the SN100 to factory default settings	129
Upgrading SN100 firmware	129
Running a Ping Test	130
Performing an SN100 software restart	130
Logs.....	131

Introduction

This chapter describes the following:

- Configuring the System settings (see section “System”)
- Configuring the Tools settings (see section “Tools” on page 127)
- Configuring Logs settings (see section “Logs” on page 131)

System

This section describes the following:

- Configuring general system settings (see “Configuring General System settings”)
- Configuring Administrators Account’s user name and password (see “Configuring Administrator Account’s user name and password” on page 121)
- Configuring User Account’s user name and password (see “Configuring User Account’s user name and password” on page 122)
- Configuring time settings (see “Configuring Time settings” on page 122)
- Configuring auto-provisioning settings (see “Configuring Auto Provision settings” on page 123)
- Configuring dynamic DNS settings (see “Configuring Dynamic DNS settings” on page 124)
- Configuring TR069 settings (see “Configuring TR069 settings” on page 125).

Configuring General System settings

This window is where you set router or bridge mode. In bridge mode, firewall and NAT functions are disabled, which also means that there is no longer LAN IP addresses being assigned to devices connected to it. Accessing the SN100 when in bridge mode, requires a static IP to be set on the device which is to be specified under Manager IP Address as shown in [figure 77](#) on page 121.

Do the following to display General settings:

1. Click on the plus button next to *Maintenance* to display the sub-categories (see [figure 76](#)).

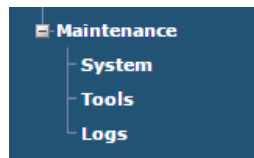


Figure 76. Maintenance sub-categories

2. Click *Maintenance*. The *General* window displays (see [figure 77](#) on page 121).

General Time Setting Auto Provision Dynamic DNS TR069 setting

System Setup

Mode Router Bridge

Administrator Inactivity Timer : (minutes, 0 means no timeout)

Manager IP Address:

Note:
 1.If change to Bridge mode, the system will automatic to disable firewall and NAT .
 2.If change to Bridge mode, Please set Management IP Address

Administrator Account

User Name:

User Password:

User Account

User Name:

User Password:

Apply Reset

Figure 77. General System settings window

- When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Apply Reset

Configuring Administrator Account's user name and password

This section describes setting the administrator's user name and password.



For proper security we recommend that you change from the default credentials to a new administrator's user name and password as soon as possible.

Do the following to display General settings:

- Click on the plus button next to *Maintenance* to display the sub-categories (see [figure 76](#)).
- Click *Maintenance*. The *General* window displays (see [figure 77](#)).
- In the *Administrator Account* section, click the *User Name* box, then type a new user name.

Administrator Account

User Name:

User Password:

- Click the *User Password* box, then type a new password.
- When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Configuring User Account's user name and password

This section describes setting the user account's user name and password. This account has limited capabilities in that it only allows changing network settings.

Do the following to display General settings:

1. Click on the plus button next to *Maintenance* to display the sub-categories (see [figure 76](#)).
2. Click *Maintenance*. The *General* window displays (see [figure 77](#)).
3. In the *User Account* section, click the *User Name* box, then type a new user name.

4. Click the *User Password* box, then type a new password.
5. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Configuring Time settings

You can maintain the system time by synchronizing with a public time server over the Internet.

Do the following to display Time settings:

1. Click on the plus button next to *Maintenance* to display the sub-categories (see [figure 76](#) on page 120).
2. Click *System*. The *General* window displays (see [figure 77](#) on page 121).
3. Click the *Time Setting* tab to bring it to the front (see [figure 78](#) on page 122).

Figure 78. Time Setting window

4. Choose the desired time zone from the *Time Zone Select* drop down-menu
5. Enabling NTP client update let's the SN100 synchronize its clock automatically to the network time server.
6. Click the check box to enable the *Automatically Adjust Daylight Saving* setting.

- If you did not enable NTP client update, go to section “[Setting the time manually](#)”. Otherwise click the button next to the NTP server drop-down menu, then choose the desired NTP server from the menu. If you want to manually enter the NTP server address, click the button next to the *Manual IP Setting* box, then type the address (for example: *0.patton.pool.ntp.org*).
- When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Apply Reset

Setting the time manually

If you wish to set the local time of the SN100 manually, in case there is no NTP server accessible from the network where the device is being installed, do the following.

- Uncheck the box for *Enable NTP client update* (see [figure 78](#) on page 122).
- Enter the date and time.
- When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Apply Reset

Configuring Auto Provision settings

The provisioning function may be used for an automated, mass configuration of SN100 CPEs in the field. The provisioned configuration file, is loaded in to the system startup config once it has been downloaded. After the download has been done, the device will reboot to apply the changes as per the new config file.

Do the following to set up auto-provisioning:

- Click on the plus button next to *Maintenance* to display the sub-categories (see [figure 76](#) on page 120).
- Click *System*. The *General* window displays (see [figure 77](#) on page 121).
- Click the *Auto Provision* tab to bring it to the front (see [figure 79](#) on page 123).

The screenshot shows the 'Auto Provision' configuration window. At the top, there are five tabs: 'General', 'Time Setting', 'Auto Provision' (which is active and highlighted in blue), 'Dynamic DNS', and 'TR069 setting'. Below the tabs, the window is divided into two main sections. The first section is titled 'Backup Auto-provision File' and contains a text prompt: 'Click **Backup** to save the auto-provision file of your system to your computer.' Below this prompt is a 'Backup' button. The second section is titled 'Auto Provision' and contains three rows of settings: 'Protocol' with a dropdown menu set to 'Disable', 'File Path' with an empty text input field and 'Exp. auto' to its right, and 'Expiration Time' with a text input field containing '10800' and 'seconds' to its right. At the bottom of the window, there are two buttons: 'Apply' and 'Reset'.

Figure 79. Auto Provision window

4. Select the provisioning protocol to match your environment. Choose between FTP, HTTP or TFTP
5. Enter the address path to access the config file which is to be provisioned
6. Optionally an expiration time may be set for the SN100 to periodically check if there is a new file available to be provisioned.
7. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

The image shows two buttons, 'Apply' and 'Reset', positioned side-by-side. They are small, rectangular buttons with a light gray background and a thin border. The text 'Apply' is on the left button and 'Reset' is on the right button.

Configuring Dynamic DNS settings

End users of Internet access receive an allocation of IP addresses, often only a single address, by their Internet service provider. The assigned addresses may be fixed (i.e. *static*), or may change from time to time, a situation called *dynamic*. Dynamic addresses are generally given only to residential customers and small businesses, as most enterprises specifically require static addresses.

Dynamic IP addresses present a problem if the customer wants to provide a service to other users on the Internet, such as a web service. As the IP address may change frequently, corresponding domain names must be quickly re-mapped in the DNS, to maintain accessibility using a well-known URL.

Dynamic DNS service addresses this scenario. The automatic reconfiguration is generally implemented in the user's router or computer, which runs software to update the DDNS service. The communication between the user's equipment and the provider is not standardized, although a few standard web-based methods of updating have emerged over time. Dynamic DNS is a service, that provides you with an unchanging Internet domain name (URL) to go with that (possibly ever changing) IP address.

Do the following to display Dynamic DNS settings:

1. Click on the plus button next to *Maintenance* to display the sub-categories (see [figure 76](#) on page 120).
2. Click *System*. The *General* window displays (see [figure 77](#) on page 121).
3. Click the *Dynamic DNS* tab to bring it to the front (see [figure 80](#) on page 125).

Figure 80. Dynamic DNS window

4. Click the check-box to enable or disable the DDNS service (default setting is disable).
5. Click the *Service Provider* drop-down menu to select the desired DDNS service provider.
6. Type the hostname you registered at the DynDns.org or TZO.net website in the *Domain Name* box.
7. Type username you registered at the DynDns.org or TZO.net website in the *User Name/Email* box.
8. Type the password you registered at the DynDns.org or TZO.net website in the *Password/Key* box.
9. In case your service at DynDNs.org or TZO.net includes a fixed IP address, you may enter this one in to the corresponding field. When doing so, make sure you set the radio button for that field as well.
10. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.



Configuring TR069 settings

TR-069 is a DSL Forum specification for CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS).

Do the following to display TR069 settings:

1. Click on the plus button next to *Maintenance* to display the sub-categories (see [figure 76](#) on page 120).
2. Click *System*. The *General* window displays (see [figure 77](#) on page 121).
3. Click the *TR069 Setting* tab to bring it to the front (see [figure 81](#) on page 126).

TR069 Setting

TR069 SSL certificates

To modify a SSL certification, browse to the location of the SSL certification and click **Upload**.

File Path:

No file chosen

General

ACS Client Enable: Disabled Enabled

ACS URL:

User Name:

Password:

Periodic Inform Enable: Disabled Enabled

Periodic Inform Interval:

NAT Traversal

STUN Enable: Disabled Enabled

STUN Server URL:

STUN Server Port:

User Name:

Password:

Connection Request

User Name:

Password:

Figure 81. TR069 window

4. Set *ACS Client Enable* to *Enabled*.

General

ACS Client Enable: Disabled Enabled

ACS URL:

User Name:

Password:

Periodic Inform Enable: Disabled Enabled

Periodic Inform Interval:

5. Type the ACS address in the *ACS URL* field. This is the address to which the SN100 device should send connection requests.
6. Specify *User Name* and *Password* for the TR-069 secure connection.
7. When enabled, *Periodic Inform Enable* will automatically contact the ACS for new configurations according to the time interface specified. Click the *Enabled* button to activate the feature.

NAT Traversal

STUN Enable: Disabled Enabled

STUN Server URL:

STUN Server Port:

User Name:

Password:

8. Optionally STUN may be configured, if the SN100 device is installed behind NAT.
9. Enter the STUN Server address
10. Specify the port for STUN. Default setting: 3478.
11. There might be a username and password required for STUN that is different from the ACS settings. If so, type the STUN *User Name* and *Password* in the corresponding fields

Connection Request

User Name:

Password:

12. For TR-069 connection requests, User Name and Password is to be configured as per figure 81
13. When you are satisfied with the settings, click the *Apply* button to save and apply the changes.

Tools

This section describes the following:

- How to back up the SN100 configuration, restore a back up configuration, and reset the SN100 configuration to factory default settings (see “[Configuration settings](#)” on page 127).
- How to upgrade SN100 firmware (see “[Reset the SN100 to factory default settings](#)” on page 129)
- How to run a ping test to troubleshoot problems network problems (see “[Running a Ping Test](#)” on page 130)
- How to make the SN100 perform a software restart (see “[Performing an SN100 software restart](#)” on page 130)

Configuration settings

This window enables you to do the following:

- Back up current SN100 settings to a file
- Restore settings from a previous backup file.
- Reset the current configuration to factory default settings

Do the following to display tools configuration settings:

1. Click on the plus button next to *Maintenance* to display the sub-categories (see [figure 76](#) on page 120).
2. Click *Tools*. The *Configuration* window displays (see [figure 82](#)).

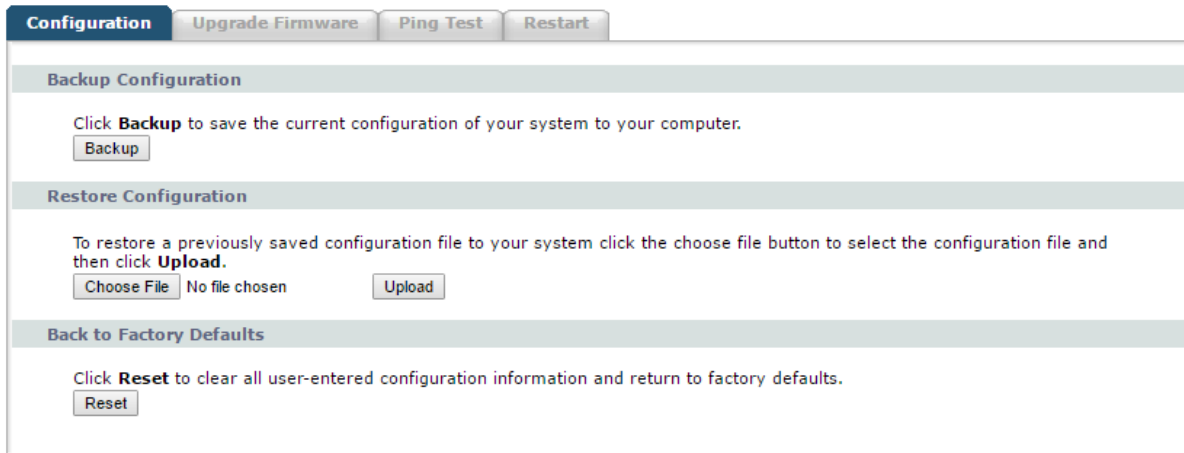


Figure 82. Tools Configuration window

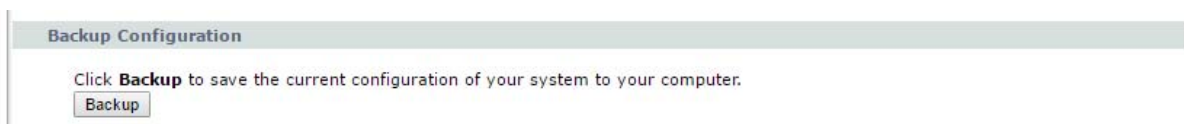
Choose from the following:

- Back up the SN100 configuration (see “[Backup Configuration](#)”)
- Restore SN100 configuration from a previous back up (see “[Restore Configuration](#)” on page 128)
- Reset the SN100 to factory default settings (see “[Reset the SN100 to factory default settings](#)” on page 129)

Backup Configuration

Do the following to back up the current SN100 configuration:

1. Click the *Backup* button to save a copy of SN100 configuration.



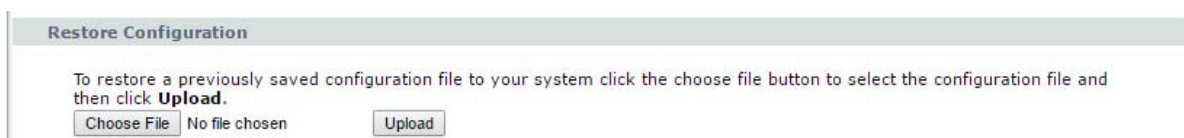
2. In the popup window select the location of where the backup configuration file should be stored.
3. Specify the filename of the backup config.
4. Click save for configuration the to be stored.

Configuration backup is completed.

Restore Configuration

Do the following to restore a previously saved configuration file:

1. Click the *Choose File* button.

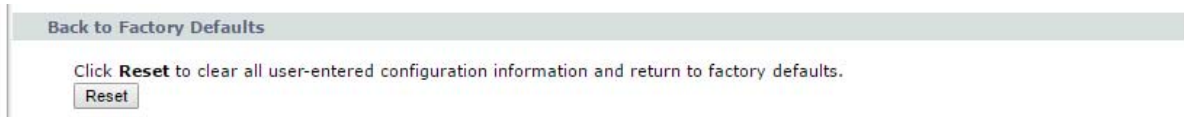


2. Select the configuration file, then click the *Upload* button.

The configuration has been restored.

Reset the SN100 to factory default settings

Click the Reset button to clear all user-entered configuration information and return the SN100 to factory defaults



The SN100 has been reset to factory defaults.

Upgrading SN100 firmware

The latest software builds are located at <https://www.patton.com/support/upgrades/>

Do the following to perform a firmware upgrade:



Do not power off the device during the upload. Doing so may crash the system.

1. Click on the plus button next to *Maintenance* to display the sub-categories (see [figure 76](#) on page 120).
2. Click *Tools*. The *Configuration* window displays (see [figure 82](#) on page 128).
3. Click the *Upgrade Firmware* tab to bring it to the front (see [figure 83](#)).

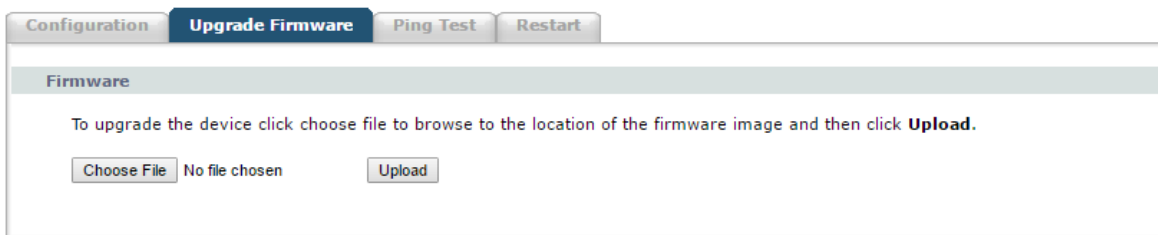
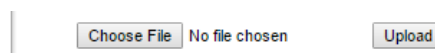


Figure 83. Upgrade Firmware window

4. Click the *Choose File* button (see [figure 83](#) on page 129), then browse to the location of the firmware image.



5. Select the firmware image, then click the *Upload* button.

The firmware has been upgraded.

Running a Ping Test

The ping test checks the reaction time of your connection—how fast you get a response after you've sent out a request. A fast ping—measured in milliseconds (ms)—means a more responsive connection.

Do the following to run the test:

1. Click on the plus button next to *Maintenance* to display the sub-categories (see [figure 76](#) on page 120).
2. Click *Tools*. The *Configuration* window displays (see [figure 82](#) on page 128).
3. Click the *Ping Test* tab to bring it to the front (see [figure 84](#)).

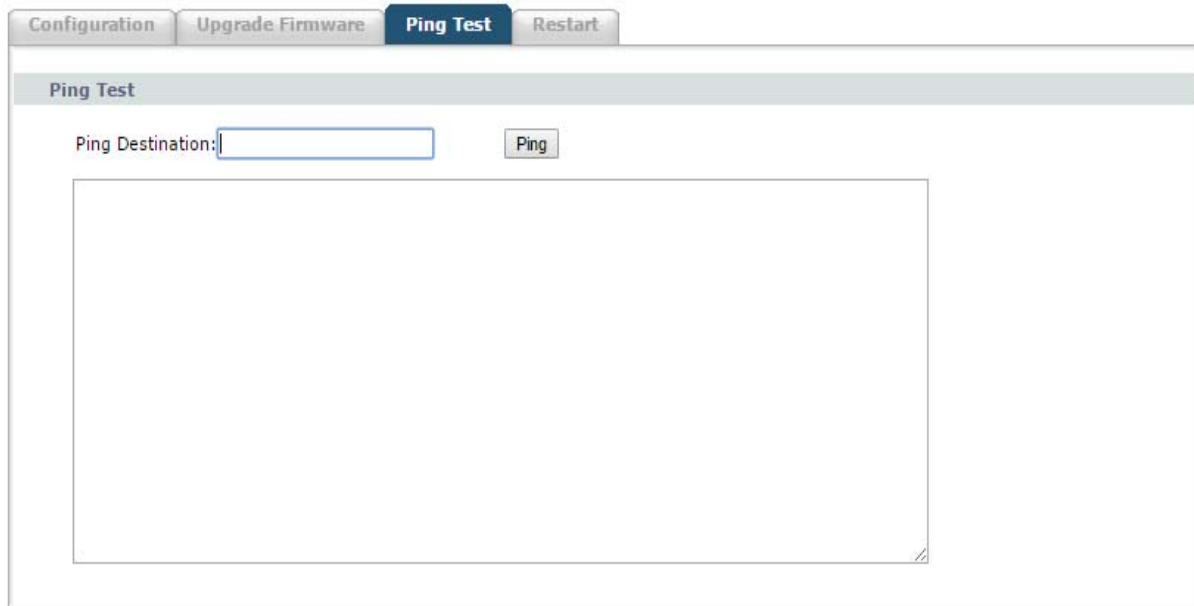


Figure 84. Ping Test window

4. Type the IP address or domain name of the destination computer in the *Ping Destination* box.
5. Click the *Ping* button to start the test. The results displayed will resemble the following example in which the IP address *169.95.1.1* is being pinged;

```
PING 168.95.1.1 (168.95.1.1): 56 data bytes
64 bytes from 168.95.1.1: icmp_seq=0 ttl=247 time=80.0 ms
64 bytes from 168.95.1.1: icmp_seq=1 ttl=247 time=100.0 ms
64 bytes from 168.95.1.1: icmp_seq=2 ttl=247 time=240.0 ms
64 bytes from 168.95.1.1: icmp_seq=3 ttl=247 time=30.0 ms
--- 168.95.1.1 ping statistics ---
5 packets transmitted, 4 packets received, 20% packet loss
round-trip min/avg/max = 30.0/112.5/240.0 ms
```

Performing an SN100 software restart

If the SN100 is not responding correctly, you may decide to restart the system software. If so, do the following:

1. Click on the plus button next to *Maintenance* to display the sub-categories (see [figure 76](#) on page 120).

2. Click *Tools*. The *Configuration* window displays (see [figure 82](#) on page 128).
3. Click the *Restart* tab to bring it to the front (see [figure 85](#)).



Figure 85. Restart window

4. Click the *Restart* button to have the device perform a software restart. Verify that the Power LED blinks as the device restarts and then stays on once the restart is completed.
5. Restart is successful.

Logs

To keep a log of SN100 activities, do the following:

1. Click on the plus button next to *Maintenance* to display the sub-categories (see [figure 76](#) on page 120).
2. Click *Tools*. The *Configuration* window displays (see [figure 82](#)).
3. Click the *Logs* tab to bring it to the front. The System Log window displays. (see [figure 86](#) on page 132).

System Log

System Log

Enable Log

system all

Enable Remote Log

Log Server IP Address: Port:

Apply Refresh Clear

Figure 86. System Log window

4. Click the check box to enable or disable the log.
5. Specify if all system logs should be part of the logging or just the major ones which are enabled by default.
6. Optionally, the logs generated by the SN100 can be sent to a centralized Syslog server. To do so, specify the Syslog server IP address and port. (Default port is 514).

Chapter 9 **Contacting Patton for assistance**

Chapter contents

- Introduction 134
- Contact information 134
- Warranty Service and Returned Merchandise Authorizations (RMAs) 134
 - Warranty Coverage 134
 - Out-of-Warranty Service 134
 - Returns for Credit 134
 - Return-for-Credit Policy 135
 - RMA Numbers 135
 - Shipping Instructions 135

Introduction

This chapter contains the following information:

- “Contact information”—describes how to contact Patton technical support for assistance.
- “Warranty Service and Returned Merchandise Authorizations (RMAs)”—contains information about obtaining a return merchandise authorization (RMA).

Contact information

Patton Electronics offers a wide array of free technical services. If you have questions about any of our other products we recommend you begin your search for answers by using our technical knowledge base. Here, we have gathered together many of the more commonly asked questions and compiled them into a searchable database to help you quickly solve your problems:

- Online support—available at <http://www.patton.com/returns/>
- E-mail support—e-mail sent to support@patton.com will be answered within 1 business day
- Telephone support—standard telephone support is available five days a week—from **8:00 am to 5:00 pm EST (1300 to 2200 UTC)**—by calling **+1 (301) 975-1007**

Warranty Service and Returned Merchandise Authorizations (RMAs)

Patton Electronics is an ISO-9001 certified manufacturer and our products are carefully tested before shipment. All of our products are backed by a comprehensive warranty program.

Note If you purchased your equipment from a Patton Electronics reseller, ask your reseller how you should proceed with warranty service. It is often more convenient for you to work with your local reseller to obtain a replacement. Patton services our products no matter how you acquired them.

Warranty Coverage

Our products are under warranty to be free from defects, and we will, at our option, repair or replace the product should it fail within one year from the first date of shipment. Our warranty is limited to defects in workmanship or materials, and does not cover customer damage, lightning or power surge damage, abuse, or unauthorized modification.

Out-of-Warranty Service

Patton services what we sell, no matter how you acquired it, including malfunctioning products that are no longer under warranty. Our products have a flat fee for repairs. Units damaged by lightning or other catastrophes may require replacement.

Returns for Credit

Customer satisfaction is important to us, therefore any product may be returned with authorization within 30 days from the shipment date for a full credit of the purchase price. If you have ordered the wrong equipment or you are dissatisfied in any way, please contact us to request an RMA number to accept your return. Patton is not responsible for equipment returned without a Return Authorization.

Return-for-Credit Policy

- Less than 30 days: No Charge. Your credit will be issued upon receipt and inspection of the equipment.
- 30 to 60 days: We will add a 20% restocking charge (crediting your account with 80% of the purchase price).
- Over 60 days: Products will be accepted for repairs only.

RMA Numbers

RMA numbers are required for all product returns. You can obtain an RMA by doing one of the following:

- Completing a request on the RMA Request page in the *Support* section at <http://www.patton.com/returns/>
- By calling +1 (301) 975-1007 and speaking to a Technical Support Engineer
- By sending an e-mail to returns@patton.com

All returned units must have the RMA number clearly visible on the outside of the shipping container. Please use the original packing material that the device came in or pack the unit securely to avoid damage during shipping.

Shipping Instructions

The RMA number should be clearly visible on the address label. Our shipping address is as follows:

Patton Electronics Company

RMA#: xxxx

7622 Rickenbacker Dr.

Gaithersburg, MD 20879-4773 USA

Patton will ship the equipment back to you in the same manner you ship it to us. Patton will pay the return shipping costs.

Appendix A **Compliance Information**

Chapter contents

- Regulatory Information 137
 - EMC Directive 137
 - Low-Voltage Directive (Safety) 137
 - PSTN 137
- Radio and TV Interference (FCC Part 15) 137
- CE Declaration of Conformity 137
- Authorized European Representative 137
- Service 138

Regulatory Information

EMC Directive

- FCC Part 15, Class B
- EN 55032 Class B
- EN55024
- EN50581

Low-Voltage Directive (Safety)

- IEC/EN60950-1, 2nd Edition

PSTN

This device is not intended nor approved for connection to the PSTN

Radio and TV Interference (FCC Part 15)

This device generates and uses radio frequency energy, and if not installed and used properly—that is, in strict accordance with the manufacturer's instructions—may cause interference to radio and television reception. The device has been tested and found to comply with the limits for a Class B computing device in accordance with specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection from such interference in a commercial installation. However, there is no guarantee that interference will not occur in a particular installation. If the device does cause interference to radio or television reception, which can be determined by disconnecting the unit, the user is encouraged to try to correct the interference by one or more of the following measures: moving the computing equipment away from the receiver, re-orienting the receiving antenna and/or plugging the receiving equipment into a different AC outlet (such that the computing equipment and receiver are on different branches).

CE Declaration of Conformity

This device is in compliance with the essential requirements and other relevant provisions of Directive 2004/108/EC relating to electromagnetic compatibility and Directive 2006/95/EC relating to electrical equipment designed for use within certain voltage limits. The Declaration of Conformity may be obtained from Patton Electronics, Inc at www.patton.com/certifications.

The safety advice in the documentation accompanying this device shall be obeyed. The conformity to the above directive is indicated by CE mark on the device.

Authorized European Representative

Martin Green
European Compliance Services Limited
Milestone house
Longcot Road
Shrivenham
SN6 8AL, UK

Service

All warranty and non-warranty repairs must be returned freight prepaid and insured to Patton Electronics. All returns must have a Return Materials Authorization number on the outside of the shipping container. This number may be obtained from Patton Electronics Technical Services at:

- Tel: +1 (301) 975-1007
- Email: support@patton.com
- URL: <http://www.patton.com>

Packages received without an RMA number will not be accepted.

Appendix B **Specifications**

Chapter contents

Telephone features.....	140
DTMF Function.....	140
Fax Modes.....	140
IP Specifications.....	140
Call Features.....	141
Network and Security.....	141
Configuration/Management.....	141
Interfaces.....	141
Operating Temperature.....	141
Power.....	142
Dimensions and Weight.....	142
Certifications.....	142

Telephone features

- G.711-ulaw
- G711-alaw
- G729
- G723
- G.726: 16k / 24k / 32k / 40k bit/s (ADPCM)
- Call Waiting
- Call Transfer
- Call Forward as Busy forward; Non-Answer forward; unconditional forward
- Do-not-disturb (DND) support
- 3-way conferencing

DTMF Function

- RFC2833
- In-Band DTMF
- SIP Info

Fax Modes

- T.38 relay support
- G.711 pass-through

IP Specifications

- SIP (RFC 3261)
- SDP (RFC 2327)
- STUN (RFC3489)
- RTP Payload for DTMF Digits (RFC2833)
- SIP Session Timers (RFC 4028)
- DNS SRV (RFC 2782)
- Outbound Proxy Support
- SIP REFER method (RFC 3515)
- Media/Ringing Tone Generation (RFC 3960)
- Message Waiting Indicator (RFC 3842)

Call Features

- Adjustable Volume
- VAD/Dynamic Jitter Buffer
- Caller ID Generation: DTMF/FSK/NTT CID
- Peer-to-Peer Call by Dial Plan
- Different Country Tone Table Configuration

Network and Security

- WAN: PPPoE client, DHCP client, Fixed IP Address, PPTP
- QoS: DSCP/VLAN Tag
- PPTP/L2TP VPN Client
- NAT
- Port/IP/MAC Filter

Configuration/Management

- Web configuration interface; password protected
- Firmware upgrades through HTTP
- SNMP v1/v2 (Customization Project)
- VR
- TR069 support with STUN
- Auto-Provision by HTTP/TFTP/FTP

Interfaces

- 1 x WAN 10/100BASE-TX
- 1 x LAN 10/100BASE-TX
- 1 x FXS (SN101)
- 2 x FXS (SN102)
- 1 x FXS/1 x FXO (SN102)
- 1 x Reset switch

Operating Temperature

- Operating Temperature: 0-40°C
- Storage Humidity: 10-90% relative humidity

Power

- AC: 100–240 VAC, 50/60 Hz
- DC: 12 VDC/1A

Dimensions and Weight

- 98mm x 86mm x 29mm
- 100g

Certifications

- CE, FCC, RoHS

Appendix C **Example Applications**

Chapter contents

ATA with SIP Server Application	144
ATA Peer to Peer Call (IP Domain Call) Application	145

ATA with SIP Server Application

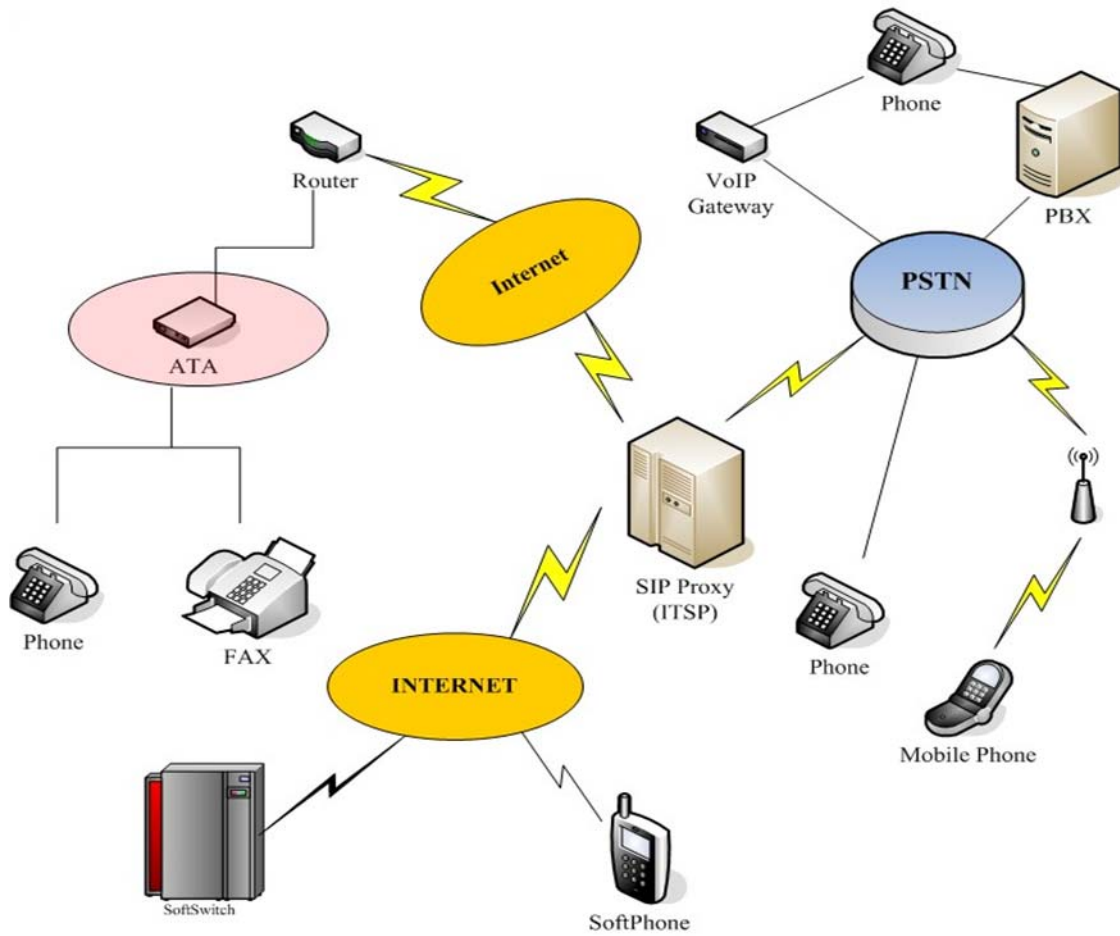


Figure 87. ATA with SIP Server Application

ATA Peer to Peer Call (IP Domain Call) Application

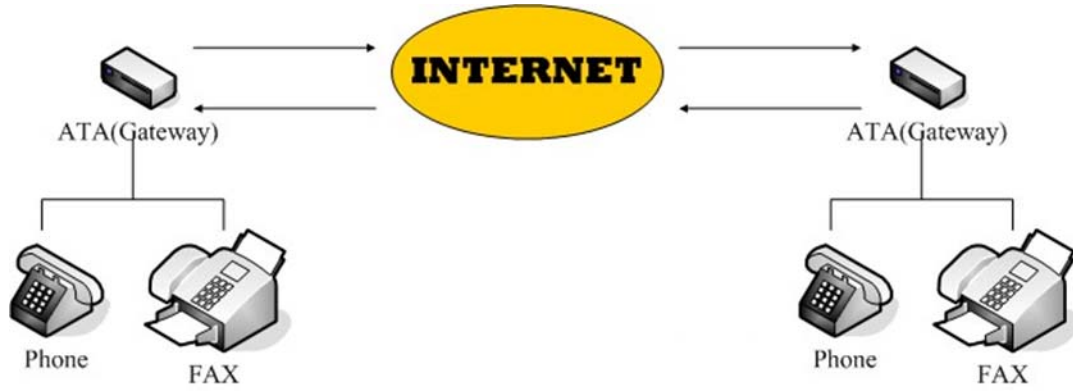


Figure 88. ATA Peer to Peer Call (IP Domain Call)

Appendix D **FAQ List**

Chapter contents

Q: What is the default administrator username and password to log in to the SN100?	147
Q: I forgot the administrator password. What should I do?	147
Q: Why is it that I can ping outside hosts, but not access Internet Web sites?.....	147
Q: What is the maximum number of IP addresses that the DHCP server of the gateway can assign to local PCs?	147
Q: Why can't I call out from the SN100?	147
Q: Why can't I use the Web Interface to configure the SN100?	147
Q: Why does one-way talk happen?	147
Q: Why can't I call out when the SN100 under the NAT?	147

Q: What is the default administrator username and password to log in to the SN100?

A: The default username is **admin**, and the default password is also **admin** to log in to the ATA. For security, you should change the password to protect your ATA against hacker attacks.

Default Wan Port Access type is **DHCP Client**

LAN Port IP Address is **192.168.1.1**.

Logging Web User Interface, open the Web browser (Microsoft Edge, Google Chrome, etc.), then input IP address.

Q: I forgot the administrator password. What should I do?

A: Press the reset button on the rear panel for at least 5 seconds to return all settings to default factory values. Then you can use the default username: **admin**, and password: **admin** to log in.

Q: Why is it that I can ping outside hosts, but not access Internet Web sites?

A: Verify the DNS server settings on your PC. You should get the DNS servers settings from your ISP. If your PC is running a DHCP client, remove any DNS IP address setting. As the router will assign the DNS settings to the DHCP-client-enabled PC.

Q: What is the maximum number of IP addresses that the DHCP server of the gateway can assign to local PCs?

A: The built-in DHCP server can support 253 IP addresses for local network usage.

Q: Why can't I call out from the SN100?

A: Verify that the SN100 is registered SIP Proxy Server (ITSP), and verify that your Internet works fine. The SN100 can't make a call without Internet or a SIP account provided by ITSP. You must have a SIP account or know the other ATA/gateway IP/domain name, before you can make a VoIP call.

Q: Why can't I use the Web Interface to configure the SN100?

A: Verify that your PC connects the SN100 LAN port, or PC and SN100 with the same subnet. If your PC isn't on the same subnet, you will not be able to log into the SN100 Web interface.

Q: Why does one-way talk happen?

A: Usually, one-way talk occurs when different codecs are used between VoIP devices making the call. Make sure both calling parties are using the same codec.

Q: Why can't I call out when the SN100 under the NAT?

A: Most VoIP products have problem in NAT Pass through. By SIP, there are many NAT Pass through Function can solve 80% NAT Problem. You can choose STUN/Outbound Proxy/ Symmetric RTP to Pass through NAT, you don't set any other setting (DMZ/Virtual Server) by router side. If you use STUN/Outbound Proxy, you must have a STUN/Outbound Proxy Server to support. If they can't pass NAT, please open the DMZ/Virtual Server by Router/NAT/Firewall.