

SL2100

Networking Manual

Copyright

NEC Platforms, Ltd. reserves the right to change the specifications, functions, or features at any time, without notice.

NEC Platforms, Ltd. has prepared this document for use by its employees and customers. The information contained herein is the property of NEC Platforms, Ltd. and shall not be reproduced without prior written approval of NEC Platforms, Ltd.

Windows is a registered trademark of Microsoft Corporation. AT&T is a registered trademark of AT&T Wireless Services, Inc. All other brand names and product names referenced in this document are trademarks or registered trademarks of their respective companies.

Copyright 2017 - 2020

NEC Platforms, Ltd.

TABLE OF CONTENTS

TABLE OF CONTENTS	1
INTRODUCTION.....	5
Section 1 GENERAL OVERVIEW.....	5
Section 2 COMMON TERMS	5
GENERAL INFORMATION	7
Section 1 VOICE OVER IP	7
IP NETWORKING	9
Section 1 INTRODUCTION.....	9
Section 2 IP TRUNKS.....	9
GENERAL IP CONFIGURATION.....	11
Section 1 INTRODUCTION.....	11
Section 2 NETWORK ADDRESSING OVERVIEW	11
Section 3 CONFIGURATION EXAMPLES	12
Section 4 TESTING THE NEC SL2100 NETWORK CONNECTION.....	14
PROGRAMMING	17
Section 1 BEFORE YOU START PROGRAMMING	17
Section 2 HOW TO USE THIS MANUAL	17
Section 3 HOW TO ENTER PROGRAMMING MODE.....	18
Section 4 HOW TO EXIT PROGRAMMING MODE	18
Section 5 USING KEYS TO MOVE AROUND IN THE PROGRAMS.....	19
Section 6 PROGRAMMING NAMES AND TEXT MESSAGES	20
Section 7 USING SOFTKEYS FOR PROGRAMMING	21
Section 8 WHAT THE SOFTKEY DISPLAY PROMPTS MEAN.....	21
Section 9 PROGRAMMING YOUR SYSTEM	21
Program 10 : System Configuration Setup.....	22

Program 15 : Extension, Basic Setup	42
Program 84 : Hardware Setup for VoIPDB.....	46
Program 90 : Maintenance Program	50
NETWORK DESIGN CONSIDERATIONS.....	53
Section 1 INTRODUCTION.....	53
Section 2 QoS	53
Section 3 INTERNET BASED CONNECTIONS (XDSL, CABLE, ETC.)	56
Section 4 FIREWALLS AND NAT.....	57
Section 5 CODEC AND BANDWIDTH.....	59
Section 6 QUALITY OF SERVICE (QoS) IMPLEMENTATION.....	61
Section 7 PORT DESIGNATIONS	73
SIP TRUNKING.....	77
Section 1 VoIP	77
Section 2 IP NETWORKING	77
Section 3 SIP TRUNKING.....	77
Section 4 SIP TRUNK OVERVIEW.....	79
Section 5 SUPPORTED SIP TRUNKING FUNCTIONS	81
Section 6 SIP TRUNK PROGRAMMING	83
Section 7 SIP TRUNK E.164 SUPPORT	93
Section 8 SIP TRUNK E.164 CLIP ENHANCEMENT.....	95
Section 9 SIP TRUNK KEEP ALIVE USING OPTION MESSAGE.....	99
DHCP CLIENT.....	101
Section 1 DHCP CLIENT.....	101
Section 2 DHCP SERVER CONFIGURATION EXAMPLE.....	102
IP MULTILINE STATION (SIP).....	107
Section 1 INTRODUCTION.....	107
Section 2 IP TO TDM CONVERSION	107
Section 3 PROVIDING POWER	109
Section 4 PEER-TO-PEER	109

Section 5	PROGRAMMING	110
Section 6	CONFIGURATION EXAMPLES	110
Section 7	IP PHONE PROGRAMMING INTERFACE.....	115
Section 8	DHCP SERVER CONFIGURATION	115
Section 9	CONFIGURING QUALITY OF SERVICE.....	115
Section 10	IP TELEPHONE REGISTRATION AND DELETION	117
Section 11	SYSTEM IP PHONES AND ANALOG TRUNKS.....	117
Section 12	FIRMWARE UPGRADE PROCEDURE	117
Section 13	IP STATION (SIP MULTILINE TELEPHONE).....	119
IP SINGLE LINE TELEPHONE (SIP).....		153
Section 1	INTRODUCTION.....	153
Section 2	PROGRAMMING	154
Section 3	IP Single Line Telephone (SIP) - TLS Connection Support	162
NAPT.....		176
Section 1	NAPT	176
Section 2	CONDITIONS	178
Section 3	RESTRICTIONS.....	178
Section 4	MINIMUM REQUIRED PROGRAMMING	179
ALL DSP BUSY INDICATION.....		182
Section 1	INTRODUCTION.....	182
Section 2	SERVICE CONDITIONS.....	182
Section 3	RELATED FEATURES.....	183
Section 4	GUIDE TO FEATURE PROGRAMMING.....	183
SL NET		184
Section 1	INTRODUCTION.....	184
Section 2	System Capacity.....	184
Section 3	Network Requirements	185
Section 4	QUALITY OF SERVICE SETTINGS (QOS)	186

Section 5 IP PRECEDENCE 186

Section 6 DIFFSERV 187

Section 7 GUIDE TO FEATURE PROGRAMMING..... 191

Section 8 PROGRAMMING EXAMPLES 201

Section 9 LIST OF SUPPORTED FEATURES IN A NETWORKED SYSTEM 205

Introduction

Section 1 GENERAL OVERVIEW

This manual provides information for networking for the NEC SL2100 system.

Section 2 COMMON TERMS

The following terms and the associated abbreviations or alternate nomenclature may be found throughout this document.

Table 1-1 Common Terms and Associated Abbreviations

Term	Abbreviation	Description
IP7XX-CPU-C1	CPU-C1 SL2100 CPU CPU	CPU-C1 with main software
IP7WW- VOIPDB- C1	VOIPDB VOIP Daughter Board	Mount this card onto the CPU card (VoIPDB slot) at Main Chassis. Max. 128 channels by license control.
IP7WW-3COIDB-C1	3COIDB	The 3COIDB provides three analog trunks and is mounted on the 082U, 008U or 000U card.
IP7WW-082U-B1	082U card	8-digital station + 2 Analog station interface card
IP7WW- 12TXH- B1 TEL IP7WW- 24TXH- B1 TEL	2-wire Digital Multiline Telephone	12TXH-B1 TEL 12-button digital telephone 24TXH-B1 TEL 24-button digital telephone
IP7WW-8IPLD-C1 TEL	IP Multiline Telephone	8IPLD-C1 TEL 8-button IP DESI-Less telephone
ITK-8LCX-1TEL	IP Multiline Telephone	IP 8 Line Key Self Labeling Color Display Telephone

MEMO

General Information

Section 1 VOICE OVER IP

Voice over IP (VoIP) is a technology that converts speech into data packets and transmits these packets over TCP/IP networks. The technology also facilitates compression and silence suppression to reduce network bandwidth demands.

As most organizations already have existing data networks in place, considerable cost savings can be achieved by utilizing spare bandwidth on these networks for voice traffic.

NEC SL2100 supports the use of IP Phones. These telephones provide the same functionality as a multiline telephone but use the data network rather than the traditional telecoms infrastructure. This can reduce costs and allow the use of NEC SL2100 telephones in locations that would not normally be supported by multiline telephones.

[Table 2-1 Table 2-1 VoIP Specifications](#) lists the specifications for various aspects of NEC SL2100 VoIP system.

Table 2-1 VoIP Specifications

Category	Feature	Notes
IP Address	DHCP Server ^{*1}	CPU-C1/VoIPDB
	DHCP Client ^{*1}	VoIPDB/IP Phone
QoS	802.1p/1q	CPU-C1
	L3 QoS (ToS)	Diffserv/IP Precedence
Maintenance	HTTP Server	CPU-C1/VoIPDB
VLAN	Tag and port-based VLAN	
VoCoder	G.711 μ -law/A-law	
	G.729a	
	G.722	
	G.726	
Jitter Buffer Size	Set by system programming	
RTP Length	Set by system programming	
Echo Canceller Tail Size	Set by system programming	
Level Adjustment	Set by system programming	
IP Phone	SIP Phone	SIP Phone
SIP Trunk	SIP Trunk	Maximum 128 Trunks

^{*1}. *DHCP Server and DHCP Client cannot be used at the same time. When the DHCP Server is enabled the DHCP Client function cannot be activated.*



When the VoIPDB is installed, the CPU-C1 is no longer active, all IP connections go through the VoIPDB.

MEMO

IP Networking

Section 1 INTRODUCTION

IP Networking uses VoIP technology to connect two or more telephone systems together. This allows calls to be made between sites without using the public telephone network. This saves considerable money, and makes communication between sites much easier.



The voice quality of VoIP is dependent on variables such as available bandwidth, network latency and Quality of Service (QoS) initiatives, all of which are controlled by the network and Internet Service Providers. Because these variables are not in NEC control, it cannot guarantee the performance of the user's IP-based remote voice solution. Therefore, NEC recommends connecting VoIP equipment through a local area network using a Private IP address.

Section 2 IP TRUNKS

The SIP Trunks method of networking allows connection to SIP devices. This could be a PBX system or a third-party product. When using SIP, the feature set is limited and the advanced networking features cannot be used.

Refer to [SIP Trunking](#) for a detailed description of SIP trunking and for set up instructions.

To set up IP trunks:

1. Connect the system to the Data Network. (Refer to [General IP Configuration](#) for detailed instructions.)
2. Configure the IP trunks.
3. Configure the SIP information.
4. Configure the F-Route.

2.1 Configure IP Trunks

When installing a VoIP daughter board in the NEC SL2100 system, external line ports are allotted in accordance with the number of Licensed ports for the particular IP Application.

The NEC SL2100 system now has the required information about the remote destinations and the SIP configuration is complete. The only remaining task is to configure F-Route to route calls to remote destinations via the IP trunks. F-Route configuration is discussed in detail in the Automatic Route Selection (ARS) feature in the NEC SL2100 Programming Manual.

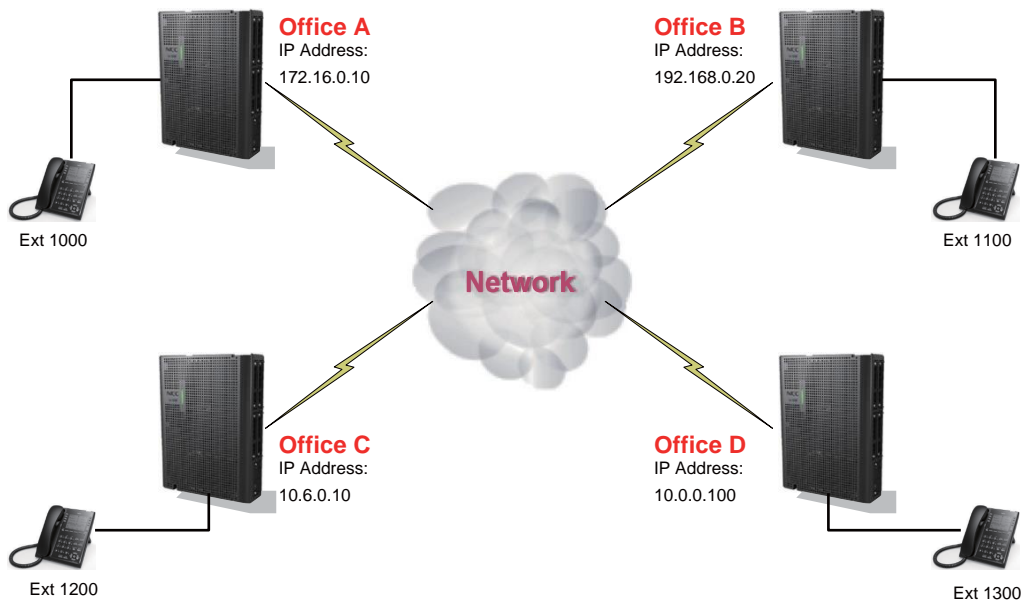


Figure 3-1 Example of SL2100 IP Network Configuration

General IP Configuration

Section 1 INTRODUCTION

The NEC SL2100 system uses IP for various applications, including:

- System Programming
- Voice Over IP

This section describes the procedure for connecting the NEC SL2100 system to an existing data network and configuring TCP/IP. This is the first step in implementing VoIP and other IP applications.

Section 2 NETWORK ADDRESSING OVERVIEW

Before connecting the system to a data network, it is necessary to obtain the relevant IP Addressing information. This information is supplied by the IT Manager or Network Administrator at the customer site.

2.1 IP Address

All equipment/devices used in the LAN setup must have an IP address assignment. An IP address assigns a unique address for each device. There are two types of IP addresses: Private and Global. A Private IP address is not accessible through the Internet; a Global IP address can be accessed through the Internet.

In most cases, a Private address is used, as LAN devices are not usually directly connected to the Internet. Private addresses are usually taken from the following ranges:

- Class A 10.0.0.0 ~ 10.255.255.255
- Class B 172.16.0.0 ~ 172.31.255.255
- Class C 192.168.0.0 ~ 192.168.255.255

A Public address is normally only used when a device is directly connected to the Internet. This is unlikely in the case of the equipment. If Public addressing is used, the numbers are normally allocated by an ISP.

2.2 Subnet Mask

As the IP address includes information to identify both the network and the final destination, the Subnet Mask sets apart the network and destination information. The default subnet masks are:

- Class A 255.0.0.0
- Class B 255.255.0.0
- Class C 255.255.255.0

The Subnet Mask is made up of four groups of numbers. When a group contains the number 255, the router ignores or masks that group of numbers in the IP address as it is defining the network location of the final destination.

For example, if the IP address is: 172.16.0.10 and the Subnet Mask used is Class B (255.255.0.0), the first two groups of numbers (172.16) are ignored once they reach the proper network location. The next two groups (0.10) are the final destination within the LAN to which the connection is to be made.



For sub-netted networks, the subnet mask may be different from the default subnet masks listed above.

2.3 DHCP

Dynamic Host Configuration Protocol (DHCP) assigns a dynamic IP address. Network control may be easier with DHCP as there is no need to assign and program individual IP addresses for the LAN equipment. To use a dynamic IP address, a DHCP server must be provided. The SL2100 can be configured to be the DHCP server for the customers network. Before the DHCP server in the SL2100 can be enabled, the DHCP client function must first be disabled.

When equipment, which is connected to the LAN (the DHCP client), is requesting an IP address, it searches the DHCP server.

When the request for an address is recognized, the DHCP server assigns an IP address, Subnet mask, and the IP address of the router, based on NEC SL2100 system programming.

Section 3 CONFIGURATION EXAMPLES

The following configuration examples illustrate a typical network configuration for an existing network that uses a static address and a typical configuration for a new network that uses a dynamic address.

3.1 Example Configuration 1 - Existing Network with Static Addressing

[Figure 4-1 Example Configuration 1 - Existing Network with Static IP Address](#) shows a typical network configuration that uses Static IP Addressing.

Each client device has a manually assigned IP address in the 192.168.1.0/24 network (i.e., 192.168.1.1 to 192.168.1.254 with a subnet mask of 255.255.255.0). They also have a default gateway address configured (192.168.1.254) this allows the device to route packets to destinations that exist outside of their own LAN.

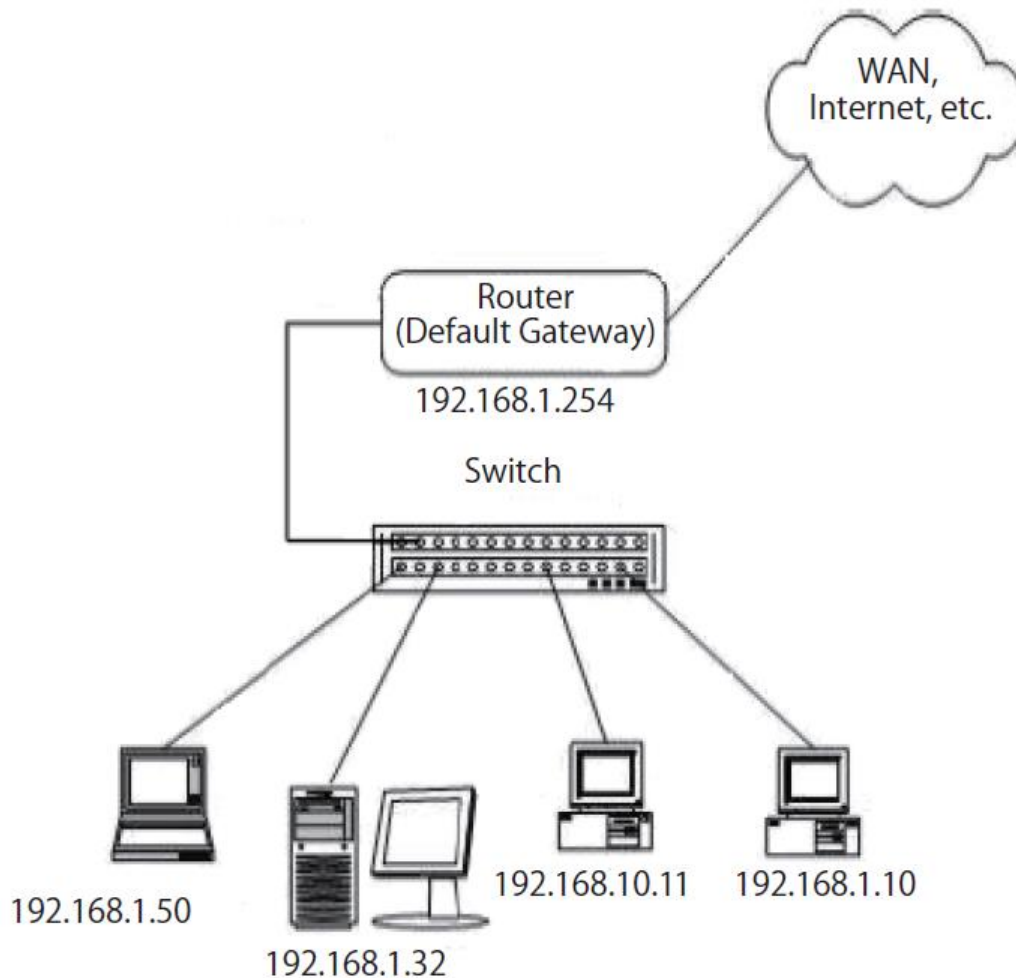



Figure 4-1 Example Configuration 1 - Existing Network with Static IP Address

Assume that a NEC SL2100 is added to the existing data network. The Network Administrator (or IT Manager) should provide the following:

- IP Address (for the CPU-C1)
- IP Addresses (for the VoIP daughter board)
- Subnet Mask
- Default Gateway
- A spare switch

First, program the NEC SL2100:

- 192.168.1.200
- 255.255.255.0
- PRG10-12-03: 192.168.1.254

 A system reset is required for the IP Address changes to take effect.

Now connect the CPU-C1/VoIPDB Ethernet Port to the switch port, using a standard Cat-5 patch cable. The NEC SL2100 is now configured on the network and should be accessible by other devices on the network. Refer to [Figure 4-2 Example Configuration 1 - Adding the NEC SL2100 Chassis to the Network](#).

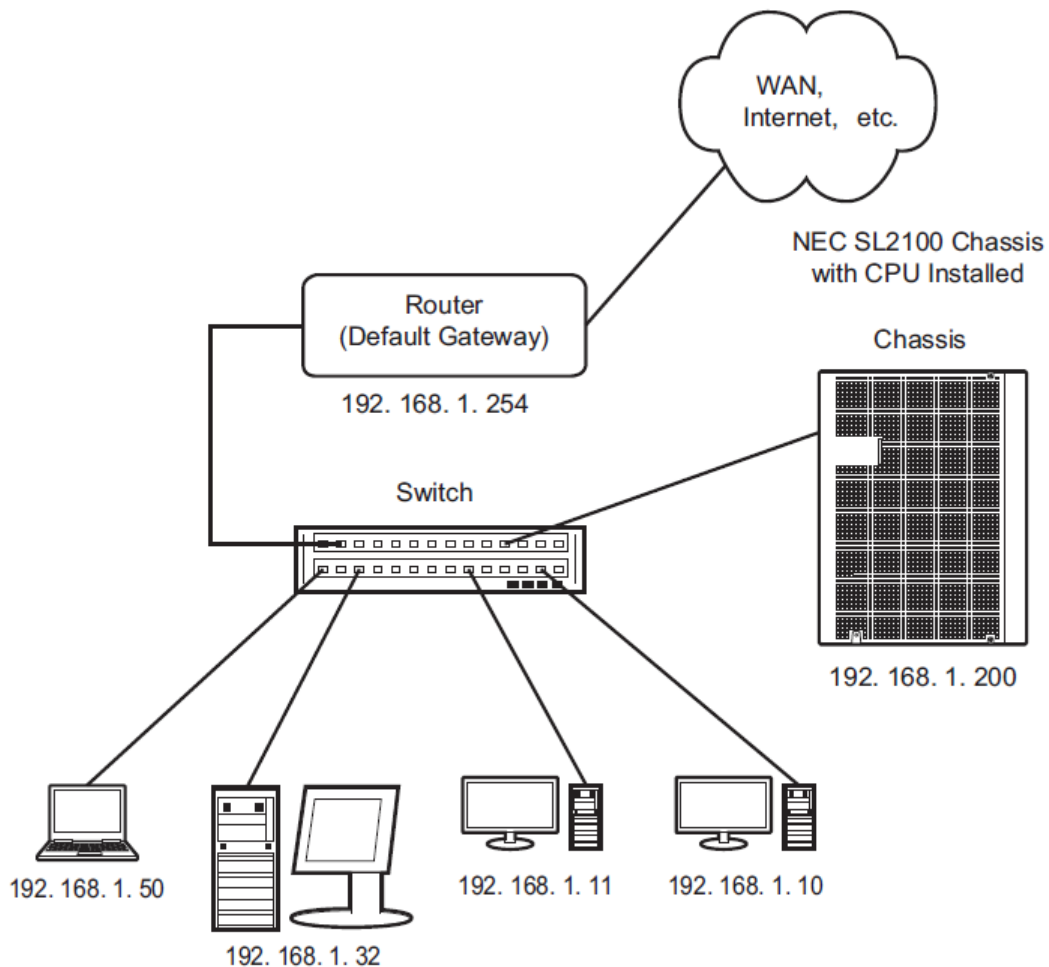


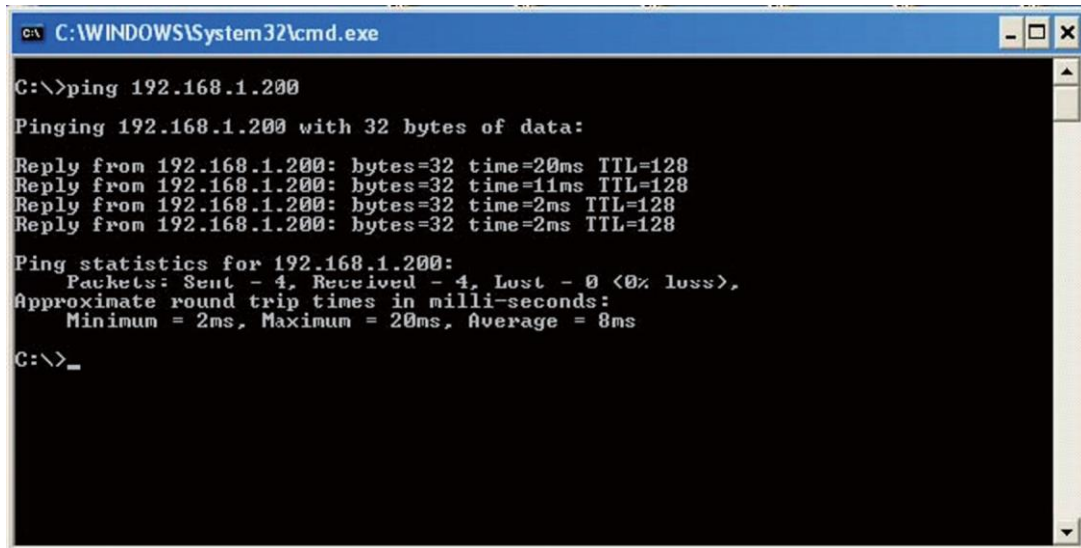
Figure 4-2 Example Configuration 1 - Adding the NEC SL2100 Chassis to the Network

Section 4 TESTING THE NEC SL2100 NETWORK CONNECTION

To test the NEC SL2100 network connection, it is possible to use the ICMP (Internet Control Message Protocol) Ping command. This basically sends a small amount of data from one device to another and then waits for a reply. This test confirms that the IP addressing and physical connection are good. To perform this test, from a Windows PC:

1. Click **Start**.
2. Click **Run...**
3. In the Open dialogue box, enter **command**.
4. Click **OK**. A Command prompt window opens.
5. Type **ping 192.168.1.200**.

[Figure 4-3 Testing the Network Connection](#) shows that the NEC SL2100 system has replied to the Ping request – this indicates that the NEC SL2100 system is correctly connected to the network.



```
C:\WINDOWS\System32\cmd.exe
C:\>ping 192.168.1.200
Pinging 192.168.1.200 with 32 bytes of data:
Reply from 192.168.1.200: bytes=32 time=20ms TTL=128
Reply from 192.168.1.200: bytes=32 time=11ms TTL=128
Reply from 192.168.1.200: bytes=32 time=2ms TTL=128
Reply from 192.168.1.200: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 20ms, Average = 8ms
C:\>_
```

Figure 4-3 Testing the Network Connection

MEMO

PROGRAMMING

The remainder of this chapter provides instructions for programming individual program blocks.

Section 1 BEFORE YOU START PROGRAMMING

This chapter provides you with detailed information about the NEC SL2100 program blocks that may be required to connect the NEC SL2100 to a data network and to configure the VoIP function. The configuration and programming examples, found in the earlier chapters, can be a useful reference when programming the data.

Section 2 HOW TO USE THIS MANUAL

This section lists each program in numerical order. For example, Program 10-01 is at the beginning of the section and Program 92-01 is at the end. The information on each program is subdivided into the following headings :

Description describes what the program options control. The Default Settings for each program are also included. When you first install the system, it uses the Default Setting for all programs. Along with the Description are the **Conditions** which describe any limits or special considerations that may apply to the program.

The program access level is just above the Description heading. You can only use the program if your access level meets or exceeds the level the program requires. Refer to [How to Enter Programming Mode](#) for a list of the system access levels and passwords.

Feature Cross Reference provides you with a table of all the features affected by the program. You will want to keep the referenced features in mind when you change a program. Customizing a feature may have an effect on another feature that you did not intend.

Telephone Programming Instructions shows how to enter the program data into system memory. For example :

1. Enter the programming mode.
2. 15-07-01

```

15-07-01      TEL
KY01 = *01
  <          -          +          ->
  
```

Digital (2W) Multiline Terminal

```


15-07-01      TEL
KY01 = *01
  <          -          +          ->
  
```

IP Multiline Terminal

tells you to enter the programming mode, dial 150701 from the telephone dial pad. After you do, you will see the message "15-07-01 TEL" on the first line of the telephone display. This indicates the program number (15-07), item number (01), and that the options are being set for the extension. The second row of the display "KY01 = *01" indicates that Key 01 is being programmed with the entry of *01. The third row allows you to move the cursor to the left or right, depending on which arrow is pressed. To learn how to enter the programming mode, refer to [How to Enter Programming Mode](#).

Section 3 HOW TO ENTER PROGRAMMING MODE

To enter programming mode :

1. Go to any working display telephone.
 -  *In a newly installed system, use extension (port 1).*
2. Do not lift the handset.
3. Press **Speaker**.
4. **##****.

Password

5. Dial the system password + **Hold**.
Refer to the following table for the default system passwords. To change the passwords, use **90-02 : Programming Password Setup**.

```

Program Mode
Base Service OP1  OP2

```

Digital (2W) Multiline Terminal, IP Multiline Terminal

Password	User Name	Level	Programs at this Level
12345678	tech	2 (IN)	Installation (IN) : IN, SA and SB levels defined by 90-26 are available.
0000	ADMIN1	3 (SA)	System Administrator - Level 1 (SA) : 10-01, 10-02, 10-12, 10-13, 10-14, 10-15, 10-16, 10-23, 10-28, 10-29, 10-45, 10-67, 12-02, 12-03, 12-04, 12-08, 15-01, 15-07, 15-09, 15-10, 15-11, 20-16, 20-34, 20-57, 20-63, 20-64, 20-66, 20-70, 21-07, 21-14, 22-04, 22-11, 22-17, 25-08, 30-03, 30-04, 32-02, 41-02, 41-03, 41-04, 41-05, 41-06, 41-07, 41-08, 41-09, 41-11, 41-12, 41-13, 41-14, 41-16, 41-17, 41-18, 41-19, 41-20, 45-02, 84-16, 84-22, 90-03, 90-04, 90-06, 90-07, 90-16, 90-19, 90-65, 93-01, 93-02, 93-03, 93-04, 93-05, 93-06
9999	ADMIN2	4 (SB)	System Administrator - Level 2 (SB) : 13-04, 13-05, 13-06, 13-11, 15-14, 21-20

Section 4 HOW TO EXIT PROGRAMMING MODE

To exit the programming mode :

When you are done programming, you must be out of a program option to exit (pressing the **Mute** key will exit the program option).


1. Press **Mute** key to exit the program options, if needed.

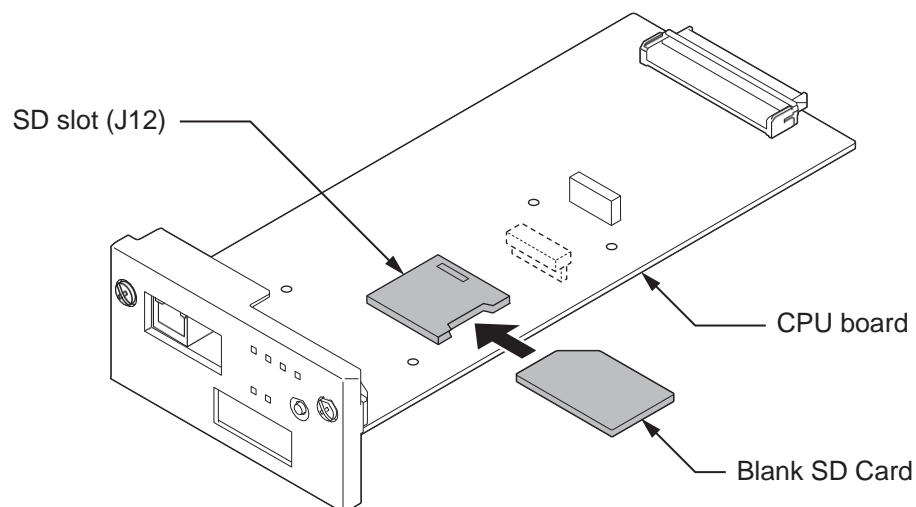
```

Program Mode
Base Service OP1  OP2
  
```

Digital (2W) Multiline Terminal, IP Multiline Terminal

2. Press **Speaker**. If changes were to the system programming, "Saving System Data" is displayed.
3. The display shows "Complete Data Save" when completed and exits the telephone to an idle mode.

 *To save a customer's database, a blank SD Card is required. Insert the SD Card into the CPU and, using Program 90-03, save the software to the SD Card. (Program 90-04 is used to reload the customer data if necessary.) Note that a SD Card can only hold one customer database. Each database to be saved requires a separate drive.*



Section 5 USING KEYS TO MOVE AROUND IN THE PROGRAMS

Once you enter the programming mode, use the keys in the following chart to enter data, edit data and move around in the menus.

Table 5-1 Keys for Entering Data (Digital (2W) Multiline Terminal, IP Multiline Terminal)

When you want to ...	Telephone Programming
Enter Data into program	0 ~ 9, *, # Line Key (1 ~ 6)
Next Index	Cursor Key (Up)
Prior Index	Cursor Key (Down)
Select Data	Line Key (1 ~ 6)
All Clear	Flash
Apply	Hold Enter
Go Back to Prior Screen	Mute Clear / Back
Move Cursor Jump Up/Down	DND
Delete single character	Clear / Back

When you want to ...	Telephone Programming
Next Page	Help
Toggle between Number/Character	
While in a Entering Number	
Prior Page	Transfer
Quit the programming	Speaker Exit
Move Cursor to Left	Cursor Key (Left) Soft Key1
Change Program Number	Soft Key2
Change Index Number	
Change Program Number	Soft Key3
Change Index Number	
Move Cursor to Right	Cursor Key (Right) Soft Key4

Section 6 PROGRAMMING NAMES AND TEXT MESSAGES

Several programs (e.g., Program 20-16 : Selectable Display Messages) require you to enter text. Use the following chart when entering and editing text. When using the keypad digits, press the key once for the first character, twice for the second character, etc. For example, to enter a C, press the key **2** three times. Press the key six times to display the lower case letter. The name can be up to 12 digits long.

Table 5-2 Keys for Entering Names

Use this keypad digit ...	When you want to ...
1	Enter characters : 1 @ [¥] ^ _ ` { } > < - Á Â Ã Ä Å Æ Ç È É Ì Í Ö Ø
2	Enter characters : A-C, a-c, 2.
3	Enter characters : D-F, d-f, 3.
4	Enter characters : G-I, g-i, 4.
5	Enter characters : J-L, j-l, 5.
6	Enter characters : M-O, m-o, 6.
7	Enter characters : P-S, p-s, 7.
8	Enter characters : T-V, t-v, 8.
9	Enter characters : W-Z, w-z, 9.
0	Enter characters : 0 ! " # \$ % & ' () ð ó ú á ä å æ ö ü α ε θ B
*	Enter characters : * + , - . / : ; < = > ? π Σ σ Ω ∞ φ £
#	# = Accepts an entry (only required if two letters on the same key are needed - ex : TOM). Pressing # again = Space. (In system programming mode, use the right arrow Softkey instead to accept and/or add a space.)
Clear/Back or DND (2W Digital/IP Multiline Terminal)	Clear the character entry one character at a time.
Flash	Clear all the entries from the point of the flashing cursor and to the right.

Section 7 USING SOFTKEYS FOR PROGRAMMING

(This Feature is available for Digital (2W) Multiline Terminal and IP Multiline Terminal Only.)

Each Display telephone with Softkeys provides interactive Softkeys for intuitive feature access. The options for these keys will automatically change depending on where you are in the system programming. Simply press the Softkey located below the option you wish and the display will change accordingly.



Pressing the Cursor key Up or Down will scroll between the menus.



Section 8 WHAT THE SOFTKEY DISPLAY PROMPTS MEAN

(This Feature is available for Digital (2W) Multiline Terminal and IP Multiline Terminal Only.)

When using a display telephone in programming mode, various Softkey options are displayed. These keys will allow you to easily select, scan, or move through the programs.

Table 5-3 Softkey Display Prompts

Softkey Display Prompts	
If you press this Soft-key ...	The system will ...
back	Go back one step in the program display. You can press Cursor Key (UP) or Cursor Key (Down) to scroll forward or backward through a list of programs.
↑	Scroll down through the available programs.
↓	Scroll up through the available programs.
select	Select the currently displayed program.
←	Move the cursor to the left.
>	Move the cursor to the right.
- 1	Move back through the available program options.
+ 1	Move forward through the available program options.

Section 9 PROGRAMMING YOUR SYSTEM

This sections describes the programs used to connect the NEC SL2100 to a data network and to configure the VoIP functions.

Program 10 : System Configuration Setup


10-03 : ETU Setup

Level:

IN

Description

Use **Program 10-03 : ETU Setup** to setup and confirm the Basic Configuration data for each board. When changing a defined terminal type, first set the type to 0 and then plug the new device in to have the system automatically define it or you may have to reseat the board.

 *The items highlighted in gray are read only and cannot be changed.*

Input Data

Slot No.	1 ~ 12
----------	--------

For HBI PKG Setup

Physical Port Number	1 ~ 8
----------------------	-------

Item No.	Item	Input Data	Default
01	Terminal Type	0 = No Setting 1 = Multi-Line Telephone 2 = SLT 8 = Door Phone 10 = DSS Console 3 ~ 7, 9, 11, 12 = Not Used	2
02	Logical Port Number	[Terminal Type = 0] : 0 [Terminal Type = 1] : 1 ~ 128 [Terminal Type = 2] : 1 ~ 128 [Terminal Type = 8] : 1 ~ 2 [Terminal Type = 10] : 1 ~ 12	0
03	Transmit Gain level for SLT	1 ~ 57 (- 15.5 ~ + 12.5 dB)	32
04	Receive Gain level for SLT	1 ~ 57 (- 15.5 ~ + 12.5 dB)	32
05	Select port type	0 = Hybrid Port 1 = Door Phone	0
06	Multi-Line Telephone Line	0 = None 1 = 12 Line 2 = 24 Line	0

For ESI PKG Setup

Physical Port Number	1 ~ 8
----------------------	-------

Item No.	Item	Input Data	Description	Default
01	Terminal Type	0 = No Setting 1 = Multiline Telephone 10 = DSS Console		0
02	Logical Port Number	0 = No Setting 1 = Multiline Telephone (1 ~ 128) 10 = DSS Console (1 ~ 12)		0
08	Multiline Telephone Type	0 = DT3** 1 = DT4** 3 = SL1100 2W 4 = SL2100 2W		0
09	Item Side option information	0 = No Option 4 = EHS		0
10	Bottom option information	0 = None 4 = WHA 5 = BCA		0

For SLI PKG Setup

Physical Port Number	1 ~ 8
----------------------	-------

Item No.	Item	Input Data	Description	Default
01	Logical Port Number	0 ~ 128		0
03	Transmit Gain Level (S-Level)	1 ~ 57 (- 15.5 ~ + 12.5 dB)		32 (0 dB)
04	Receive Gain Level (R-Level)	1 ~ 57 (- 15.5 ~ + 12.5 dB)		32 (0 dB)
05	Select port type	0 = SLT 1 = Door Phone	HW switch can be change SLT or Door Phone.	0

For COI PKG Setup



Physical Port Number	1 ~ 3
----------------------	-------

Item No.	Item	Input Data	Default
01	Logical Port Number	0 ~ 128	0

For BRI PKG Setup



ISDN Line Number	1 ~ 2
------------------	-------

Item No.	Item	Input Data	Description	Default
01	ISDN Line Mode	0 = No Setting 1 = T-Point 2 = S-Point 3 ~ 5 = Not Used 6 = S-Point (Leased Line)		1

Item No.	Item	Input Data	Description	Default
02	Logical Port Number	[0 : No Setting] = 0 [1 : T-Point] = 1 ~ 128 [2 : S-Point] = 1 ~ 128 [3 ~ 5] = Not Used [6 : S-Point (Leased Line)] = 1 ~ 128	 <i>The starting port number of a BRI line is displayed. Two logic ports are automatically assigned to a BRI line.</i>	0
03	Connection Type	0 = Point-to-Multipoint 1 = Point-to-Point		0
04	Layer 3 Timer Type	1 ~ 5	 <i>Each timer value of Layer 3 is set up for every type using Program 81-06 (T-Bus).</i>	1
05	Calling Party Number	0 = No 1 = Yes	Based on this setting, the system includes a Presentation Allowed (1) or Presentation Restricted (0) in the Setup message to allow or deny the Calling Party Number. Program 15-01-04 must also be set to 1 if this option is enabled.	1
06	Connection Bus Mode	0 = Extended passive bus 1 = Short passive bus		0
07	S-point DDI digits	0 ~ 4		0
08	Dial Sending Mode	0 = Enblock Sending 1 = Overlap Sending	ISDN Protocol definition	1
09	Dial Information Element	0 = Keypad Facility 1 = Called Party Number	ISDN Protocol definition [Only when Dial Sending Mode (10-03-08) is set for 1 (Overlap Sending)]	1
10	Master/Slave System	0 = Slave System 1 = Master System	If set to 0, system is synchronized to network clock. If set to 1, system is not synchronized to the network clock.	0
14	Service Protocol for S-point	0 = Keypad facility 1 = Specified Protocol		0
15	Call Busy Mode for S-point	0 = Alerting 1 = Disconnect		0
17	ISDN Line Ringback Tone	0 = Disable 1 = Enable	System can provide ringback tone, if set to 1 : Enable.	0
18	Type of Number	0 = Unknown 1 = International number 2 = National number 3 = Network specific number 4 = Subscriber number 5 = Speed Dial number	ISDN Protocol definition	0
19	Numbering Plan Identification	0 = Unknown 1 = ISDN numbering plan 2 = Data numbering plan 3 = Telex numbering plan 4 = National standard numbering plan 5 = Private numbering plan	ISDN Protocol definition	0
25	Layer 1 Supervision	0 = Disable 1 = Enable		0
26	Screening Indicator (V1.5 added)	0 = user-provided (not screened) 1 = user-provided (verified and passed) 2 = user-provided (verified and failed)	Calling Party Number information element Screening indicator (octet 3a)	0

For PRI PKG Setup

SLOT Numbe	1 ~ 12
------------	--------

Item No.	Item	Input Data	Description	Default
01	ISDN Line Mode	0 = No Setting 1 = T-Point 2 = S-Point 6 = S-Point (Leased Line)		1
02	Logical Port Number	[0 : No Setting] = 0 [1 : T-Point] = 1 ~ 128 [2 : S-Point] = 1 ~ 128 [6 : S-Point (Leased Line)] = 1 ~ 128	 <i>The start port number of a PRI line is displayed.</i>	0
03	CRC Multi-frame (CRC4)	0 = off 1 = on		1
04	Layer 3 Timer Type	1 ~ 5	 <i>Each timer value of Layer 3 is set up for each type in Program 81-06 (T-Bus)</i>	1
05	CLIP Information	0 = No 1 = Yes	Based on this setting, the system includes a Presentation Allowed (1) or Presentation Restricted (0) in the Setup message to allow or deny the Calling Party Number. Program 15-01-04 must also be set to 1 if this option is enabled.	1
06	Length of Cable	0 = Level 1 1 = Level 2 2 = Level 3 3 = Level 4 4 = Level 5		2
07	S-point DDI digits	0 - 4		0
08	Dial Sending Mode	0 = Enbloc Sending 1 = Overlap Sending	ISDN Protocol definition	0
09	Dial Information Element	0 = Keypad Facility 1 = Called Party Number	ISDN Protocol definition Only when Dial Sending Mode (10-03-08) is set for 1 (Overlap Sending).	0
10	Master/Slave System	0 = Slave System 1 = Master System	If set to 0, system is synchronized to network clock. If set to 1, system is not synchronized to the network clock.	0
13	Loss-Of-Signal Detection Limit	0 = Level 0 (lowest sensitivity) 1 = Level 1 2 = Level 2 3 = Level 3 4 = Level 4 5 = Level 5 6 = Level 6 7 = Level 7 (highest sensitivity)	If the transmit/receive voltage is less than the setting in 10-03-13, the system considers this as Loss-Of-Signal and the PRI does not come up. Note that there are different values based on the setting in 10-03-12 for the PRI.	2
14	Service Protocol for S-point	0 = Keypad facility 1 = Specified Protocol for Aspire system		0
15	Call Busy Mode for S-point	0 = Alerting 1 = Disconnect		0

Item No.	Item	Input Data	Description	Default
16	Two B-Channel Transfer for PRI Service	0 = off 1 = on		0
18	Type of Number	0 = Unknown 1 = International number 2 = National number 3 = Network Specific number 4 = Subscriber number 5 = Speed Dial number	ISDN Protocol definition. Select the number type for the ISDN circuit.	2
19	Numbering Plan Identification	0 = Unknown 1 = ISDN numbering plan 2 = Data numbering plan 3 = Telex numbering plan 4 = National standard numbering plan 5 = Private numbering plan	ISDN Protocol definition. Select the Numbering Plan used for the ISDN circuit.	1
20	Network Exchanger Selection	0 = Standard 1 = reserved 2 = reserved 3 = DMS (A211) 4 = 5ESS 5 = DMS (A233) 6 = 4ESS 7 = NI-2	Select the ISDN protocol for the ISDN circuit	7
21	Number of Ports	0 = Auto 1 = 4 Ports 2 = 8 Ports 3 = 12 Ports 4 = 16 Ports 5 = 20 Ports		0
26	Screening Indicator (V1.5 added)	0 = user-provided (not screened) 1 = user-provided (verified and passed) 2 = user-provided (verified and failed)	Calling Party Number information element Screening indicator (octet 3a)	0

For PRI (T1) PKG Setup

SLOT Numbe	1 ~ 12
------------	--------

Item No.	Item	Input Data	Description	Default
01	Logical Port Number	0 ~ 128	The start port number of a T1 line is displayed, and 24 logic ports are automatically assigned to a DTI (T1) line.	0
02	T1 Signal Format Selection	0 = D4 (12 Multi Frame) 1 = ESF (24 Multi Frame)		0
03	Zero Code Suppression	0 = B8ZS 1 = AMI/ZCS		0
04	Line Length Selection	0 = 0 feet ~ 133 feet 1 = 133 feet ~ 266 feet 2 = 266 feet ~ 399 feet 3 = 399 feet ~ 533 feet 4 = 533 feet ~ 655 feet		0
05	T1 Clock Source	0 = Internal 1 = External		1

Item No.	Item	Input Data	Description	Default
06	Number of Ports	0 = Auto 1 = 4 Ports 2 = 8 Ports 3 = 12 Ports 4 = 16 Ports 5 = 20 Ports		0

For VoIP PKG Setup

SLOT Number	0
-------------	---

Item No.	Item	Input Data	Default
01	VoIP Type	4 = Built-in VoIP 5 = VoIPDB	
02	Number of Channel	8 = Built-In VoIP 16 ~ 128 = VoIPDB	
03	Number of Voice Channel	0 ~ 128	0

Conditions

- When changing a defined terminal type, first set the type to 0 and then plug the new device in to have the system automatically define it, or redefine the type manually.
- The system must have a board installed to view/change the options for that type of board.

Feature Cross Reference

None

Program 10 : System Configuration Setup

10-04 : Music On Hold Setup

Level:

IN

Description

Use **Program 10-04 : Music on Hold Setup** to set the Music on Hold (MOH) source.

Input Data

Item No.	Item	Input Data	Description	Default
01	Music on Hold Source Selection	0 = Internal MOH (Tone is fixed by one music) 1 = External MOH (Tone set by PRG 10-60-01: Audio Port No.2) 2 = Service Tone (Tone set by PRG 80-01, tone 64) 3 = VRS (Tone set by PRG 10-04-02)	<ul style="list-style-type: none"> Internal Music Tune - The tune is fixed by one music tune. External Source - ACI input via 082U (J4) audio connector (Program10-60-01). Silence - Callers on hold hear silence. 	1
02	Music on Hold Tone Selection	[In case Item 1 is 3.] 1 ~ 100 = VRS Message Number		1
03	Audio Gain Setup	1 ~ 57 (- 15.5 ~ + 12.5 dB)		32 (0 dB)

Conditions

None

Feature Cross Reference

- Background Music
- Music on Hold

Program 10 : System Configuration Setup

10-12 : CPU Network Setup

Level:

SA

Description


Use **Program 10-12 : CPU Network Setup** to setup the IP Address, Subnet-Mask, and Default Gateway addresses.

Caution!

If any IP Address or NIC settings are changed, the system must be reset for the changes to take affect.

Input Data

Item No.	Item	Input Data	Description	Default
01	IP Address	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254	Set for CPU.	192.168.0.10
02	Subnet Mask	128.0.0.0 192.0.0.0 224.0.0.0 240.0.0.0 248.0.0.0 252.0.0.0 254.0.0.0 255.0.0.0 255.128.0.0 255.192.0.0 255.224.0.0 255.240.0.0 255.248.0.0 255.252.0.0 255.254.0.0 255.255.0.0 255.255.128.0 255.255.192.0 255.255.224.0 255.255.240.0 255.255.248.0 255.255.252.0 255.255.254.0 255.255.255.0 255.255.255.128 255.255.255.192 255.255.255.224 255.255.255.240 255.255.255.248 255.255.255.252 255.255.255.254 255.255.255.255	The setting of Subnet Mask is invalid when all Host Addresses are 0. If the network section is: 0, 127, 128.0, 191.255, 192.0.0, 223.255.255 The setting of Subnet Mask is invalid.	255.255.255.0
03	Default Gateway	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254	Assign the default gateway IP address.	0.0.0.0

Item No.	Item	Input Data	Description	Default
05	NIC Interface	0 = Auto Detect 1 = 100Mbps, Full Duplex 2 = Reserved 3 = Reserved 4 = Reserved 5 = Reserved	NIC Auto Negotiate (CPU)  When this programming was changed, the LAN cable must be unplugged and then reconnected.	0
07	NAPT Router IP Address	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254	Set the IP address on the WAN side of router.	0.0.0.0
08	ICMP Redirect	0 = Enable 1 = Disable	When receiving ICMP redirect message, this determines if the IP Routing Table updates automatically or not.	0
09	VoIP IP Address	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254	Assign the IP Address for the VoIPDB.	172.16.0.10
10	VoIP Subnet Mask	128.0.0.0 192.0.0.0 224.0.0.0 240.0.0.0 248.0.0.0 252.0.0.0 254.0.0.0 255.0.0.0 255.128.0.0 255.192.0.0 255.224.0.0 255.240.0.0 255.248.0.0 255.252.0.0 255.254.0.0 255.255.0.0 255.255.128.0 255.255.192.0 255.255.224.0 255.255.240.0 255.255.248.0 255.255.252.0 255.255.254.0 255.255.255.0 255.255.255.128 255.255.255.192 255.255.255.224 255.255.255.240 255.255.255.248 255.255.255.252 255.255.255.254 255.255.255.255	Assign the subnet mask for the VoIPDB.	255.255.0.0
11	NIC Setup	0 = Auto Detect 1 = 100 Mbps, Full Duplex 2 = Not Used 3 = Not Used 4 = Not Used 5 = 1 Gbps, Full Duplex	Set for VoIPDB.	0
13	DNS Primary Address	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254	In the future, use this system data when add a function with DNS.	0.0.0.0

Item No.	Item	Input Data	Description	Default
14	DNS Secondary Address	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254	In the future, use this system data when add a function with DNS.	0.0.0.0
15	DNS Port	1 ~ 65535	In the future, use this system data when add a function with DNS.	53
17	VoIP NIC Port Setting	0 = MDI 1 = MDI-X		0
18	CPU MTU	1000 ~ 1500	The MTU value of CPU NIC.	1450
19	VoIP MTU	1000 ~ 1500	The MTU value of VoIP NIC.	1450
20	SSLv3 Setting	0 = Disable 1 = Enable	Set whether to use the SSLv3 in SMTP. 0 (Disable) is encrypted with TLSv1. This data requires a reset to apply changed data to the system.	1

Conditions

- The system must be reset for these changes to take affect.

Feature Cross Reference

None

Program 10 : System Configuration Setup

10-13 : In-DHCP Server Setup


Level:

SA

Description

Use Program 10-13 : In-DHCP Server Setup to setup the DHCP Server built into the CPU.

Input Data

Item No.	Item	Input Data	Description	Default
01	DHCP Server Mode	0 = Disable 1 = Enable	Enable or disable the use of the built-in DHCP Server. This program cannot be enabled if PRG10-63-01 is enabled.	0
02	Lease Time	Days 0 ~ 255	Lease Time of the IP address to a client.  Pressing the Hold Key increments to the next setting data.	0 day
		Hour 0 ~ 23		0 hour
		Minutes 0 ~ 59		30 minutes
05	Last DHCP Data	0 = Disable 1 = Enable	If 10-13-01 is enabled, this setting determines if DHCP resource is enabled or disabled.	1

Conditions

None

Feature Cross Reference

None

Program 10 : System Configuration Setup

10-14: Managed Network Setup

Level:

SA

Description

Use **Program 10-14 : Managed Network Setup** to set up the range of the IP address which the DHCP Server leases to a client.

Input Data

Item No.	Item	Input Data	Description	Default	Related Program
01	The Range of the IP address to Lease.	Minimum : 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254	When Maximum has not been entered, the maximum value equals the minimum value.	172.16.0.100	10-13-04
		Maximum : 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		172.16.5.254	

Conditions

None

Feature Cross Reference

None

Program 10 : System Configuration Setup

10-15: Client Information Setup

Level:

SA

Description

Use **Program 10-15 : Client Information Setup** to set up the client information when the DHCP server needs to assign a fixed IP address to clients.

Input Data

Client Number	1 ~ 128
---------------	---------

Item No.	Item	Input Data	Description	Default
01	MAC Address	MAC : 00-00-00-00-00-00 ~ FF-FF-FF-FF-FF-FF		00-00-00-00-00-00
	IP Address	1.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254	The IP address should be assigned out of the scope range set up in Program 10-14.	0.0.0.0

Conditions

None

Feature Cross Reference

None

Program 10 : System Configuration Setup


10-16: Option Information Setup

Level:

SA

Description

Use **Program 10-16 : Option Information Setup** to set up the option given from the DHCP server to each client.

 *The items highlighted in gray are read only and cannot be changed.*

Input Data

Item No.	Item	Input Data	Description	Default
01	Router	Code number 0 ~ 255	Set the Router IP address.	3 (Fixed)
		IP address 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		0.0.0.0
02	DNS Server	Code number 0 ~ 255	Set IP address of DNS Server.	6 (Fixed)
		IP address 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		0.0.0.0
03	TFTP Server Name	Code number 0 ~ 255	Set the name for the TFTP Server.	66 (Fixed)
		Maximum 64 character strings		No Setting
05	MGC IP Address	Code number 0 ~ 255		129 (Fixed)
		IP address 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		172.16.0.10
06	Client Host Name	Code number 0 ~ 255	Set the Client Host Name.	12 (Fixed)
		Maximum 64 character strings		No Setting
07	DNS Domain Name	Code number 0 ~ 255	Set the DNS Domain Name.	15 (Fixed)
		Maximum 20 character strings		No Setting
08	Download Protocol	Code number 0 ~ 255	Set Download Protocol used for AutoConfig (for 8IPLD-C1 Terminal).	43 (Fixed)
		Sub code number		163 (Fixed)
		1 = FTP 2 = HTTP		1
09	Encryption Information	Code number 0 ~ 255	Set an Encryption Information used for Auto-Config (for 8IPLD-C1 Terminal).	43 (Fixed)
		Sub code number		164 (Fixed)
		Fixed 128 character strings		No Setting

Item No.	Item	Input Data	Description	Default
10	FTP Server Address	Code number 0 ~ 255	Set a FTP Server Address used for AutoConfig.	43 (Fixed)
		Sub code number		141
		IP address 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		0.0.0.0
11	Config File Name	Code number 0 ~ 255	Set a File Name used for AutoConfig.	43 (Fixed)
		Sub code number		151
		Maximum 15 character strings		No Setting
12	Vender Class ID	Code number 0 ~ 255		60 (Fixed)
		Maximum 256 character strings		NEC DT700
13	SNMP Server IP Address	Code number 0 ~ 255		69 (Fixed)
		IP address 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		0.0.0.0
14	POP3 Server IP Address	Code number 0 ~ 255		70 (Fixed)
		IP address 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		0.0.0.0
16	SIP Server (IP Address)	Code number 0 ~ 255		120 (Fixed)
		IP address 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		172.16.0.10
17	SIP Server (Domain Name)	Code number 0 ~ 255	If there is setting in 10-16-16 this setting will be ignored	120 (Fixed)
		Maximum 20 character strings		No Setting
18	FTP Server IP Address	Code number 0 ~ 255		141 (Fixed)
		IP address 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		0.0.0.0
19	Config File Name	Code number 0 ~ 255		151 (Fixed)
		Maximum 15 character strings		No Setting
20	LDS Server 1 IP Address	Code number 0 ~ 255		162 (Fixed)
		IP address 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		0.0.0.0
21	LDS Server 2 IP Address	Code number 0 ~ 255		162 (Fixed)
		IP address 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		0.0.0.0
22	LDS Server 3 IP Address	Code number 0 ~ 255		162 (Fixed)
		IP address 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		0.0.0.0

Item No.	Item	Input Data	Description	Default
23	LDS Server 4 IP Address	Code number 0 ~ 255		162 (Fixed)
		IP address 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		0.0.0.0
24	Next Server IP Address	IP address 0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254		0.0.0.0
27	SIP Server Receive Port	Code number 0 ~ 255		168 (Fixed)
		Port: 1 ~ 65535		5080
28	Configuration File Name	Code number 0 ~ 255		43 (Fixed)
		Sub Code number 0 ~ 255		152
		Up to 15 characters		No Setting
29	Configuration File Name	Code number 0 ~ 255		43 (Fixed)
		Sub Code number 0 ~ 255		153
		Up to 15 characters		No Setting

Conditions

None

Feature Cross Reference

None

Program 10 : System Configuration Setup

10-19 : VoIP DSP Resource Selection

Level:

IN

Description

Use **Program 10-19 : VoIP DSP Resource Selection** to define the criteria for each DSP resource on the VoIPDB.

Input Data

Slot Number	0
DSP Resource Number	1 ~ 128

Item No.	Item	Input Data	Description	Default
01	VoIP DSP Resource Selection	0 = Common use for both IP extensions and trunks 1 = Use for IP extensions 2 = Use for SIP trunks 3 = Use for Networking 5 = Blocked 6 = Common without unicast paging 7 = Multicast paging 8 = Unicast paging	This program is used to assign the 128 resources of the VoIPDB. NEC recommends leaving the default settings as system default.	Resource 1 = 1 Resource 2 ~ 128 = 0

Conditions

None

Feature Cross Reference

None

Program 10 : System Configuration Setup

10-54 : License Configuration for Each Package

Level:

IN

Description

Use **Program 10-54 : License Configuration for Each Package** to set the license information for each board.

Input Data

Slot Number	0 ~ 12
-------------	--------

License Index Number	1 ~ 32
----------------------	--------

Item No.	Item	Input Data	Default
01	License Code	0000 ~ 9999	No Setting
02	License Quantity	0 ~ 128	0

Conditions

None

Feature Cross Reference

None

Program 10 : System Configuration Setup

10-62 : NetBIOS Setting


Level:

IN

Description

Use Program 10-62 : NetBIOS Setting to set the data of NetBIOS.

Input Data

Item No.	Item	Input Data	Description	Default
01	NetBIOS Mode	0 = Disabled 1 = Enabled		1
02	NetBIOS Name	Maximum 15 characters	 Please avoid using Space between the words. Also when you create name please use all upper letters.	SL2100

Conditions

None

Feature Cross Reference

None

Program 10 : System Configuration Setup

10-63 : DHCP Client Setting

Level:

IN

Description

Use Program 10-63 : DHCP Client Setting to set the data of DHCP Client.

Input Data

Item No.	Item	Input Data	Description	Default
01	DHCP Client Mode	0 = Disabled 1 = Enabled	If you are using IP phones/trunks it is recommended to not use the DHCP client function, a static IP address would be preferred. If you are going to still use the DHCP client function then the DHCP server should be setup so that the same IP address is always provided to the system.	1

Conditions

None

Feature Cross Reference

None

Program 15 : Extension, Basic Setup

15-05: IP Telephone Terminal Basic Data Setup

Level:

IN

Description

Use **Program 15-05 : IP Telephone Terminal Basic Data Setup** to set up the basic settings for an IP telephone.

Input Data

Extension Number	Maximum eight digits
------------------	----------------------

Item No.	Item	Input Data	Description	Default	Related Program
01	Terminal Type	1 = H.323 2 = SIP 3 = None 4 = IP MLT 5 = WebRTC (V1.5 added)		3	
02	IP Phone Fixed Port Assignment	MAC address 00-00-00-00-00-00 ~ FF-FF-FF-FF-FF-FF	MAC Address of registered SIP MLT phone is stored and/or can input the MAC address of an SIP MLT phone so when it comes online it is provided with the extension in which the MAC address matches.	00-00-00-00-00-00	15-05-01
04	Nickname	Up to 48 characters	Nickname section on Invite message. Example : Extension 100 has a Nickname set to PAUL. Extension 101 has command 15-05-17 set to Nickname. The inbound call to extension 101, from 100, shows PAUL. Nickname must be unique in the system.	No Setting	15-05-17
07	Using IP Address	0.0.0.0 ~ 255.255.255.255		-	15-05-01
09	Call procedure port	0 ~ 65535		-	15-05-01
11	IP MLT C/CTR Port	0 ~ 65535		-	
15	CODEC Type	1 = Type 1 2 = Type 2 3 = Type 3 4 = Type 4 5 = Type 5	Assign the CODEC Type of the SIP MLT.	1	84-24 84-11 15-05-01
16	Authentication Password	Up to 24 characters	Assign the authentication password for SIP single line telephones. Web pro indicates password as * mark.	No Setting	15-05-01

Item No.	Item	Input Data	Description	Default	Related Program
18	IP Duplication Allowed Group	0 = Disable 1 = Enable	When this program is 1: Enable, the duplication of an IP address is allowed at the time of SIP/IP Multiline Terminal registration. This PRG is valid, when PRG15-05-01 is SIP or IP Multiline Terminal.	0	15-05-01
19	Side Option Information	0 = No Option 1 ~ 3 = Not used 4 = EHS		0	
20	Bottom Option Information	0 = No Option 1 ~ 2 = Not Used 3 = WHA 4 = BCA	Shows the type of adapter installed.	0	10-03-10
26	IP MLT Terminal Type	0 = Not Set 1 = Not Used 2 = ITL-**D-1D/ ITL-24BT-1D/ ITL-24PA-1D (without 8LKI (LCD) -L) 3 = UT880 4 = Not Used 5 = Softphone 6 = CTI 7 ~ 8 = Not Used 9 = IP4WW-24TIXH 10 ~ 12 = Not Used 13 = ITZ-*-*D 14 = ITZ-*CG 15 = ITZ-**LDG/ITZ-**LD 16 = ITY-6D 17 = ITY-8LDX 18 = IP7WW-8IPLD-C1		0	
27	Personal ID Index	0 ~ 128	When the SIP Multiline telephone is using manual/auto registration, assign each phone a unique personal index. Then go to command 84-22 to assign the user name and password.	0	84-22
28	Addition Information Setup	0 = Do not inform 1 = Inform	Select whether to inform of additional information or not.	0	15-01-01 15-02-13 15-02-15 15-02-34
29	Terminal WAN-side IP Address	0.0.0.0 ~ 255.255.255.255		0.0.0.0	
30	DTMF Play during Conversation at Receive Extension	0 = Do Not Play 1 = Play		0	
31	Alarm Tone during Conversation (RTP packet loss alarm)	0 = Off 1 = On		1	
33	LAN Side IP Address of Terminal	0.0.0.0 ~ 255.255.255.255		0.0.0.0.	
35	Encryption Mode On/Off	0 = Off 1 = On		0	
36	IP MLT Firmware Version	00.00.00.00 ~ ff.ff.ff.ff	Indicate a current firmware Version.	00.00.00.00	
38	Paging Protocol Mode	0 = Multicast 1 = Unicast 2 = Auto	Sets the protocol mode for the Paging function.	0	
39	CTI Override Mode	0 = Disable 1 = Enable		0	

Item No.	Item	Input Data	Description	Default	Related Program
40	Calling name display info via trunk for standard SIP	0 = Both name and number 1 = Name only 2 = Number only 3 = None	* Trunk name is the first priority and abbreviated (SPD) name is second priority	0	
41	Time Zone(hour)	0 ~ 24 (- 12 ~ + 12 hour)		12	
43	Video Mode	0 = Disable 1 = Enable		0	
44	Using STD-SIP Display for CPN	0 = Disable 1 = Enable		0	
45	NAT plug & play	0 = OFF 1 = ON	Effect this program only when PRG 10-46-14 (for IP Multiline Terminals) or PRG 10-33-05 (for Standard SIP Terminal) are set to NAT mode. Effect this program only when PRG 10-46-14 (for IP Multiline Terminals) is set to NAT mode. If you are setting the SIP Terminal using remote router by turning this setting ON you don't need to set the Port Forward on remote router side. Select sending RTP port number to remote Router, use from negotiation result (0) or received RTP packet (1)	1	10-46-14
46	Door Phone Number	0 = Not door phone 1 ~ 6 = Door phone number		0	
47	Registration Expiry Timer for NAT	0 = Disable 60 ~ 65535 (sec)	On a per station basis, this setting defines the SIP registration expiry timer. This setting applies to IP Multiline Terminals or Standard SIP Terminal connected via NAPT. If this value is set to 0, for a NAPT terminal, the value in PRG 84-23-01 (for IP Multiline Terminals) or PRG 10-33-01 (for Standard SIP Terminal) are applied.	180	84-23-01
48	Subscriber Expiry Timer for NAT	0 = Disable 60 ~ 65535 (sec)	On a per station basis, this setting defines the SIP subscribe expiry timer. This setting only applies to IP Multiline Terminals or Standard SIP Terminal connected via NAPT. If this value is set to 0, for a NAPT terminal, the value in PRG 84-23-02 (for IP Multiline Terminals) or PRG 10-33-01 (for Standard SIP Terminal) are applied.	180	84-23-02
49	Receiving SIP INFO	0 = Disable 1 = Allowed any time 2 = Allowed while RTP is not available	Enables to receive a SIP INFO message from a standard SIP phone as a dial information.	2	
50	Peer to Peer Mode	0 = Off 1 = On		1	
51	Transport Protocol	0 = UDP 1 = TCP 2 = TLS	This program is the transport protocol. (Read only)	0	

Conditions

None

Feature Cross Reference

None

Program 84 : Hardware Setup for VoIPDB

84-09 : VLAN Setup

Level:

IN


Description

Use Program 84-09 : VLAN Setup to set up the VLAN data.

Input Data

Interface Number	1 ~ 2
------------------	-------

Item No.	Item	Input Data	Default
01	VLAN	0 = Disable (Off) 1 = Enable (On)	0
02	VLAN ID	0 ~ 4094	0
03	Priority	0 ~ 7	0

 *Interface No.2: The packets send from LAN I/F on VoIPDB is set the VLAN Tag (VoIPDB 32ch/64ch/128ch).*

Conditions

- System programming must be exited before these program options take affect.

Feature Cross Reference

None

Program 84 : Hardware Setup for VoIPDB

84-10 : ToS Setup

Level:

IN

Description

Use Program 84-10 : ToS Setup to set up the Type of Service data.

Input Data

Protocol Type	1 = Not Used 2 = Not Used 3 = Reserved 4 = H.323 5 = RTP/RTCP 6 = SIP 7 = Reserved 8 = SIP MLT 9 = SIP Trunk 10 = Reserved 11 = Reserved
---------------	--

Item No.	Item	Input Data	Description	Default
01	ToS Mode	0 = Disable (Invalid) 1 = IP Precedence 2 = Diffserv	When Input Data is set to 1, Item No. 07 is invalid. When Data is set to 2, Item No. 02 ~ 05 are invalid.	0
02	Priority, IP Precedence	0 ~ 7 0 = Low 7 = High	1 = Router queuing priority	0
03	Low Delay	0 ~ 1 0 = Normal Delay 1 = Low Delay	1 = Optimize for low delay routing	0
04	Wideband (Throughout)	0 ~ 1 0 = Normal Throughput 1 = High Throughput	1 = Optimize for high bandwidth routing	0
05	High Reliability	0 ~ 1 0 = Normal Reliability 1 = Low Reliability	1 = Optimize for reliability routing	0
07	Priority (D.S.C.P. - Differentiated Services Code Point)	0 ~ 63	DSCP (Differentiated Services Code Point)	0

Conditions

- The system must be reset for these program options to take affect.

Feature Cross Reference

None

Program 84 : Hardware Setup for VoIPDB

84-33 : FAX over IP Setup

Level:

IN

Description




This program sets the parameter of FAX over IP Function.

Input Data

Type	1 = H323 Trunk 2 = Networking 3 = SIP Trunk 4 = SIP Extension 5 = Reserved 6 = Reserved
------	--

Profile	1 ~ 6
---------	-------

Item No.	Item	Input Data	Description	Default
01	FAX Relay Mode	0 = Disable 1 = Enable 2 = Each Port Mode		0
02	T.38 Protocol mode	0 = R/U 1 = U/R 2 = RTP 3 = UDPTL		1
04	Maximum Jitter Buffer	0 ~ 300 ms (for VoIPDB mode) 10 ~ 300 ms* (for Built-In VoIP mode)		160
05	T.38 RTP Format Payload Number	96 ~ 127		100
06	T.38 FAX Max Speed	0 = V.27ter; 4800 bps 1 = V.29; 9600 bps 2 = V.17; 14400 bps		2
07	T.38 Data Error Correction Mode	0 = Redundancy 1 = FEC		0
08	T.38 Error protection depth for Signaling	0 ~ 2	This item is only available when you use VoIPDB. It is unavailable when you use Built-in VoIP, which depends on the data of Item No. 09.	0
09	T.38 Error protection depth for Data	0 ~ 2		0
10	T.38 TCF Method	1 = VOIPDB 2 = G3FE		1
11	T.38 ECM(Error Correction Mode) Mode	0 = Disable 1 = Enable		1

Item No.	Item	Input Data	Description	Default
12	FAX Codec	1 = G.711 a-law 2 = G.711 u-law 3 = G726		2
13	Payload Size	1 ~ 4 (10ms base)		2
14	Jitter Buffer Mode	1 = Static 2 = Self adjusting		1
15	Minimum Jitter Buffer	0 ~ 300 ms (for VoIPDB mode)		80
16	Average Jitter Buffer	10 ~ 300 ms* (for Built-In VoIP mode)		120
17	Maximum Jitter Buffer			160
18	FAX RTP Payload Type	96 ~ 127 (Not Sip Trunk) 0, 2, 8, 96 ~ 127 (SIP Trunk)	 When the G,711 a-law is selected in Item 12, it is possible to set "8" in Item 18  When the G,711 u-law is selected in Item 12, it is possible to set "0" in Item 18  When the G,726 is selected in Item 12, it is possible to set "2" in Item 18	103
19	FAX over IP Type	0 = Type 1 1 = Type 2	SIP Trunk : Type 1 : T.38 Type 2 : Path through	0

Conditions

None

Feature Cross Reference

None

Program 90 : Maintenance Program

90-23 : Deleting Registration of IP Telephones

Level:

IN

Description



This program is available via telephone programming and not through PC Programming.

Use **Program 90-23 : Deleting Registration of IP Telephones** to delete the registered IP telephone from the system.

Input Data

Extension Number	Up to eight digits
------------------	--------------------

Item No.	Item	Input Data	Description	Default
01	Delete IP Telephone	1→Hold	This assignment removes the station number association with the MAC address of the IP station. [Del.IP-Phone] : Dial 1 + press Hold (Press Hold only to cancel.)	-

Conditions

None

Feature Cross Reference

None

Program 90 : Maintenance Program

90-34 : Firmware Information

Level:

IN

Description

Use **Program 90-34 : Firmware Information** to list the package type and firmware boards installed in the system.

Input Data

Slot Number	00 ~ 12
-------------	---------

Item No.	Item	Input Data	Default
01	Package Name	PKG Name (Up to 15 characters)	-
02	Firmware Version Number	00.00 ~ 15.15	-
03	VOIPDB Software Version	DEV/PR/REL - 00.00.00.00.00.00 DEV/PR/REL - FF.FF.FF.FF.FF.FF	-
04	DSP Project Number	00000000 - FFFFFFFF	-
05	Vocoder Firmware Version	00.00.00.00 - FF.FF.FF.FF	-
06	OCT1010ID Version	00.00.00.00 - FF.FF.FF.FF	-

Conditions

None

Feature Cross Reference

None

MEMO

Network Design Considerations

Section 1 INTRODUCTION

This chapter explains some issues that should be considered when planning a NEC SL2100 VoIP installation. This is a generalized explanation and therefore does not discuss vendor-specific issues and solutions. Typically, different solutions are implemented by different manufacturers.

Section 2 QoS

Quality of Service (QoS) is one of the most important factors for VoIP. This refers to the perceived quality of speech and the methods used to provide good quality speech transmission. Several factors that affect speech quality and several mechanisms can be used to ensure QoS.

This chapter also describes the problems that can occur and some possible solutions. Each network equipment manufacturer (NEC, 3Com, Cisco, etc.) has slightly different methods of implementing QoS and these are not discussed in this document. This chapter provides an overview to classify voice traffic on the NEC SL2100 so that the network equipment can impose QoS.

2.1 QoS Definitions

This section lists common definitions used with QoS for VoIP.

Latency (Delay):

If at any point the usage on the network exceeds the available bandwidth, the user experiences delay, also called latency. In more traditional uses of an IP data network, the applications can deal with this latency. If a person is waiting for a web page to download, they can accept a certain amount of wait time. This is not so for voice traffic. Voice is a real time application, which is sensitive to latency. If the end-to-end voice latency becomes too long (150ms, for example), the call quality is usually considered poor. It is also important to remember that packets can get lost. IP is a best effort networking protocol. This means the network tries to get the information there, but there is no guarantee.

Delay is the time required for a signal to traverse the network. In a telephony context, end-to-end delay is the time required for a signal generated at the talker's mouth to reach the listener's ear. Therefore, end-to-end delay is the sum of all the delays at the different network devices and across the network links through which voice traffic passes. Many factors contribute to end-to-end delay, which are covered next.

The buffering, queuing, and switching or routing delay of IP routers primarily determines IP network delay. Specifically, IP network delay is comprised of the following:

- **Packet Capture Delay**

Packet capture delay is the time required to receive the entire packet before processing and forwarding it through the router. This delay is determined by the packet length and transmission speed. Using short packets over high-speed networks can easily shorten the delay but potentially decrease network efficiency.

- **Switching/Routing Delay**
Switching/routing delay is the time the router takes to switch the packet. This time is needed to analyze the packet header, check the routing table, and route the packet to the output port. This delay depends on the architecture of the switches/routers and the size of the routing table.
- **Queuing Time**
Due to the statistical multiplexing nature of IP networks and to the asynchronous nature of packet arrivals, some queuing, thus delay, is required at the input and output ports of a packet switch. This delay is a function of the traffic load on a packet switch, the length of the packets and the statistical distribution over the ports. Designing very large router and link capacities can reduce but not completely eliminate this delay.

Jitter

Delay variation is the difference in delay exhibited by different packets that are part of the same traffic flow. High frequency delay variation is known as jitter. Jitter is caused primarily by differences in queue wait times for consecutive packets in a flow, and is the most significant issue for QoS. Certain traffic types, especially real-time traffic such as voice, are very intolerant of jitter. Differences in packet arrival times cause choppiness in the voice.

All transport systems exhibit some jitter. As long as jitter falls within defined tolerances, it does not impact service quality. Excessive jitter can be overcome by buffering, but this increases delay, which can cause other problems. With intelligent discard mechanisms, IP telephony/VoIP systems try to synchronize a communication flow by selective packet discard, in an effort to avoid the walkie-talkie phenomenon caused when two sides of a conversation have significant latency. NEC SL2100 incorporates a Jitter Buffer to avoid these problems.

Packet Loss

During a voice transmission, loss of multiple bits or packets of stream may cause an audible pop that can become annoying to the user. In a data transmission, loss of a single bit or multiple packets of information is almost never noticed by users. If packet drops become epidemic, the quality of all transmissions degrades. Packet loss rate must be less than five percent for minimum quality and less than one percent for toll quality.

2.2 Voice Quality Improvements

This section describes various techniques that can be used to improve the voice quality.

- **Increase available bandwidth:**
This can sometimes be the most basic solution and the easiest of the solutions. If running a System IP Phone using G.711 with a 30ms fill time over Ethernet, for only one call, 90Kbps of bandwidth is needed. If that same user only has a 64K line, they do not have a decent IP voice call. The user can increase the available bandwidth to slightly exceed the 90Kbps requirements and their voice quality dramatically increases. This solution might not be viable if no more bandwidth is available.
- **Use a different CODEC:**
The CODEC contains possible compression algorithms to be used on the voice. Let's take the example above again. The user only wants one voice line over a 64Kbps data connection. They also want to maintain their current fill time of 30ms. Change to a G.729. For one line, only 34Kbps is required for a call. This fits well within the 64Kbps of available bandwidth.
- **Increase the number of frames per packet:**
To continue with the example above, the user has moved to a G.729 CODEC. But now, the user wishes to add two more System IP Phones. Their current 64Kbps line can handle one call, because it is only 34Kbps. Two more System IP Phones would increase the total to 102Kbps so obviously there is not sufficient bandwidth.
The user can now increase the fill time to 50ms. This reduces the bandwidth per call to 19.8Kbps ($3 \times 19.8 = 59.4$ Kbps). The savings in bandwidth comes from the fact that with a longer fill time, fewer packets are needed to send the voice. With fewer packets, less header information needs to be attached and transmitted.

- **Change Layer 2 Protocols:**
Ethernet is most commonly used for IP packets. Unfortunately, Ethernet has a fairly large overhead of 34 bytes. So every IP voice packet going over Ethernet has a 34-byte Ethernet header attached to it. As the number of packets add up, this header data can become significant. Frame Relay has a 7-byte header and Point-to-Point Protocol (PPP) has a 6-byte header. With this decrease in header length at layer 2, some significant savings in bandwidth use can be achieved. The down side to this is that most networks may not have these services available, where Ethernet is very widely used. This is usually outside the control of the installer and therefore NEC strongly advises users to do more research on other layer 2 protocols before trying to implement them in their voice network.
- **Implement Quality of Service (QoS):**
Now, assume a derivative of the above example. The user needs only one voice line over their 64Kbps connection. They are using G.729 with a 30ms fill time. This requires 34Kbps of their available bandwidth. Also assume that this line is used at certain times of the day for data connectivity. This data connectivity is very light, only 20Kbps or so during most of the day, but does spike to 50Kbps during certain points of the day. This data is not time sensitive like the voice data, so if necessary it could be forced to wait. Therefore, the user can implement a Quality of Service mechanism on the IP network. At its most basic form, this denotes certain IP packets as being more important than others. So they would tell this 64Kbps line that IP packets with voice deserve a higher priority than those without voice. This allows the network devices to give priority to the other data, so the quality of the call is not compromised.

2.3 Types of Classifications for Traffic for QoS

Classification uses information from a packet (or frame) to define the type of data and therefore how the data should be handled for QoS on the network. Using packet classification, you can partition network traffic into multiple priority levels or Types of Service (ToS). NEC SL2100 supports methods of marking a packet with its classification information in the Layer 2 or 3 headers.

- **VLAN (802.1Q):**
Virtual LANs work at Layer 2 of the OSI model and can be equated to a broadcast domain. More specifically, VLANs can be seen as a group of end stations, perhaps on multiple physical LAN segments that are not constrained by their physical location and therefore, communicate as if they were on a common LAN. Packets can be marked as important by using layer 2 classes of service (CoS) settings in the User Priority bits of the 802.1Q header. Refer to Program [84-09 : VLAN Setup](#) for information for VLAN configuration.

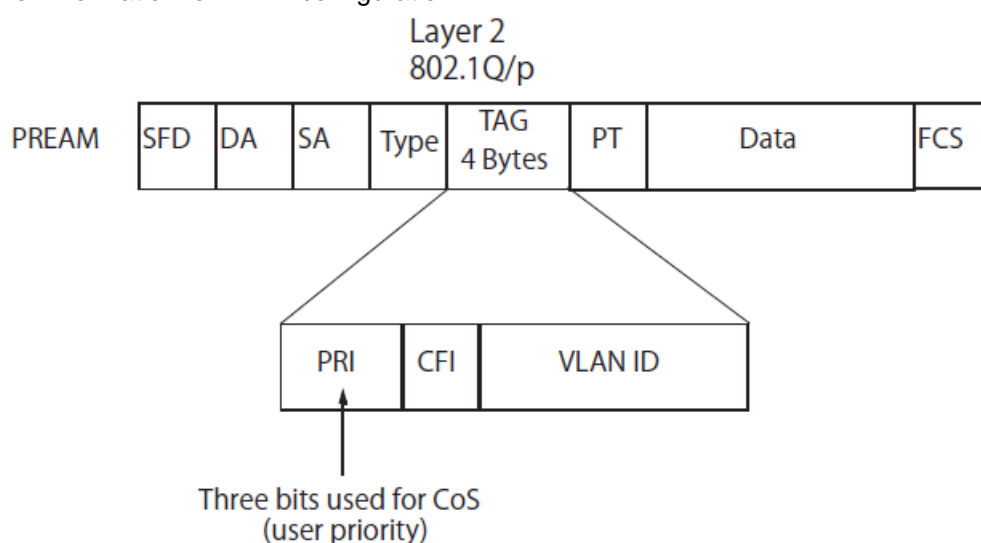


Figure 6-1 Layer 2 Diagram (802.1Q)

- **IP Precedence - Layer 3 QoS:**
Allows you to specify the class of service for a packet. You use the three precedence bits in the IPv4 header type of service (ToS) field for this purpose. Using the ToS bits, you can define up to six classes of service. Other devices configured throughout the network can then use these bits to determine how to treat the packet in regard to the type of service to grant it. These other QoS features can assign appropriate traffic-handling policies including congestion management and bandwidth allocation. By setting IP Precedence levels on incoming traffic and using them in combination with QoS queuing features, you can create differentiated service. (Refer to Program [84-10 : ToS Setup](#) for detailed programming information.)
- **Differentiated service (Diffserv) - Layer 3 QoS:**
Provides services differentiated on performance using weighted priority queuing. DiffServ requires that edge routers classify traffic flows into a member from a set of categories based on the TCP/IP header fields in what is called a micro flow. Because the Diffserv is present in every packet header, each node can provide differentiated services per-hop. Refer to Program [84-10 : ToS Setup](#) for detailed programming information.

Section 3 INTERNET BASED CONNECTIONS (XDSL, CABLE, ETC.)

Internet-based connections are becoming increasingly popular. This is mainly due to the speed and cost of xDSL and cable modem connections. For data applications, these types of connection are generally acceptable. For Voice over IP applications several issues should be taken into consideration.

Asymmetric Data Rates

On many Internet based connections, there are different data rates for upstream and downstream. For example 1Mbps down and 256Kbps up. This works well for Internet access, as generally you download files from the Internet to your PC and transmit less information in the other direction. For VoIP, speech uses the same amount of bandwidth in both directions, which means that the amount of simultaneous calls can not exceed the amount of “upstream” bandwidth available.

Contention

Most Internet based connections specify a contention ratio. This is typically 50:1 for home users or 20:1 for business users. This specifies the number of users subscribed to a single connection to the Internet Service Provider (ISP). This indicates how many users share the bandwidth with other users on the Internet, which means that the speeds that you are quoted are not necessarily accurate – you receive less than these figures.



It is unlikely that all subscribers are using a connection at the same time, so these figures are not quite as bad as they first seem.

Network Address Translation (NAT)

Usually, the equipment that your ISP provides (cable modem, ADSL router, etc.) uses Network Address Translation. This allows several devices to share one public IP address. The issues relating to the use of NAT are outlined in Firewalls and NAT below.

VPN

Due to the use of NAT, and non-routable IP addressing, it may be necessary to implement a VPN solution. This is outlined in VPN Tunneling below. (Refer to [Virtual Private Network \(VPN\) Tunneling](#).)

QoS

As discussed earlier, it is essential to have some form of Quality of Service implemented. With Internet based connections, we are not in control of the many routers, switches and other network hardware

that reside between our two VoIP endpoints. This means that we cannot specify any QoS parameter on these devices.

The only point where the QoS can be controlled is at the VPN or firewall. This allows VoIP traffic to be prioritized over any other data that is sent out to the Internet. This helps to maintain reasonable quality speech – but once the data has exited the local router/cable modem it is at the mercy of the Internet.

When implementing NEC SL2100 IP over Internet based connections it is very important that these factors are considered, and that the customer is made aware that neither the installer nor NEC are held responsible for any quality issues experienced.

Section 4 FIREWALLS AND NAT

The ways in which networks are designed to be secure (firewall, VPN services, proxy servers, etc.) and integration of NAT create problems for VoIP. This is due in part, to the endless number of different scenarios for non-real time protocols and their limited solutions.

4.1 Understanding the Infrastructure

The networks in place today look very different than the networks of yesterday. In the past, only computers and servers were connected to the network. The network was built to be as a best effort delivery mechanism, where delay and lost of information between devices was something we dealt with. Today, there is an over saturation of devices needing to gain access to the IP network. Desktop computers, fax machines, wireless PDAs, Servers, home appliances, video servers and now VoIP terminals all are fighting for bandwidth, precedence, and addresses on this converged network.

It is necessary to create some kind of Intranet environment (across the Internet), with fixed network characteristics, where VoIP solutions can tolerate some minor variations. IT personnel have been tasked with implementing different mechanisms in the network to support the new demands required on the converged network. Some solutions that have been implemented are:

- QoS devices to support precedence settings of voice packets.
- Elimination of hubs in place of switches to support 100Mbps full-duplex transmission.
- Firewall integration to protect the internal network from external attack.
- Network Address Translation (NAT) devices are widely deployed to support the addressing issues.
- Virtual Private Network (VPN) Servers were added to Enterprise networks to support the security and connectivity issues for remote users.

Some solutions, such as the hub replacement and integration of QoS, are done behind the scenes and should have no effect on the voice application. Other solutions such as NAT and Firewall cause major disturbance to VoIP.

4.2 Firewall Integration

Network security is always a concern when connecting the Local Area Network (LAN) to the Wide Area Network (WAN). There are many ways to integrate security in the network – the most popular are Firewalls and Proxy servers.

- Firewalls
Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets. All messages entering or leaving the Intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
- Proxy Server
Proxy server intercepts all messages entering and leaving the network. The proxy server effectively hides the true network address.

What should be noted is that no matter which security measure is implemented, the VoIP must have TCP/UDP ports open in the security wall (e.g., firewall/proxy) for the media and control streams to flow. If any point in the network prevents the ports from flowing from end-to-end, the VoIP application does not work.

The ports that need to be open on the firewall/proxy vary depending on the particular application being used. A list of these ports is shown below, however it should be noted that the preferred solution would be to allow all ports on the NEC SL2100 device to be open, or to place the NEC SL2100 outside of the firewall.

Applications	Rx Port	NEC SL2100 Programming
PC Programming	8000	90-54-02
Web Programming	80	90-54-01
DHCP Server	67	
SIP MLT Listening Port	5080 5081	10-46-06 10-46-13
SIP Trunk Listening Port	5060	10-29-04
SIP Single Line Stations	5070	84-20-01
Realtime Transport Protocol	10020~10146	84-26-02
Realtime Transport Control Protocol (RTCP)	10021~10147	84-26-03

4.3 Virtual Private Network (VPN) Tunnelling

A Virtual Private Network is a private data network that maintains privacy through using a tunneling protocol and security procedures. Allowing for remote networks (including VoIP devices), which reside behind NATs and/or Firewalls to communicate freely with each other.

The idea of the VPN is to connect multiple networks together using public (i.e., Internet) based connections. This type of connection is ideal for those commuters, home workers, or small branch offices needing connectivity into the corporate backbone. It is possible to connect these remote networks together using private links (such as leased lines, ISDN, etc.) but this can be very expensive and there is now a high demand for low cost Internet connectivity.

Companies today are exploring the use of VPN for a variety of connectivity solutions, such as:

- Remote User to Corporate Site VPN
Allows employees to use their local ISP fastest connection such as cable modems, DSL, and ISDN. For traveling users, all they need to do is dial into their ISP local phone number.
- Site-to-site VPN
Allows companies to make use of the Internet for the branch-to-branch connections, cutting the cost of the expensive point to point leased line service.
- Extranet
Extranet describes one application using VPN technology. The concept allows a company and a vendor/supplier to access network resources at each site. For example, a customer may have access to a suppliers intranet for access to product information.

VPNs can be implemented in hardware or software. Single users, such as traveling sales personnel, may have a software based VPN client on their laptop computer. This connects back to the Head Office VPN server. For larger sites, the VPN is typically implemented using a hardware VPN – this is often incorporated in to a firewall solution.

The diagram below is example of how a VPN tunnel may be implemented. The red lines in the diagram show the tunnels that are created through the Internet. Each network can connect to the others as though they are connected with private connections (kilostream, etc.), without the issues relating to NAT.

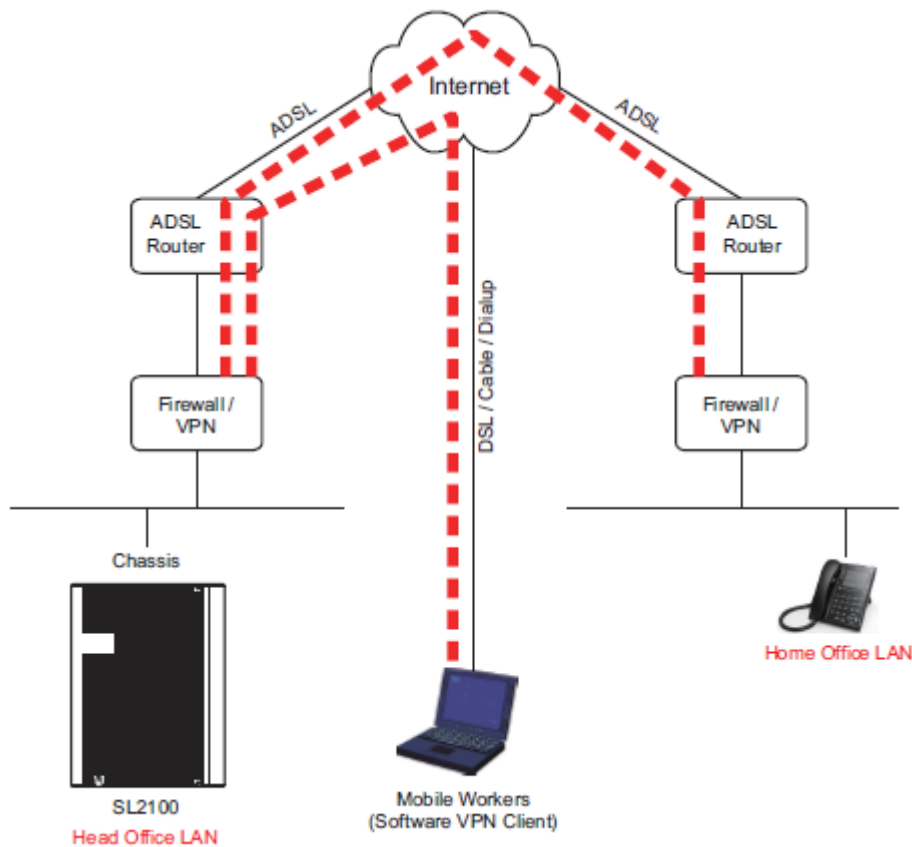



Figure 6-2 Virtual Private Network (VPN) Example

When IP address translation is applied to a VoIP packet, the application fails and the communication path is broken. VoIP packets contain the IP address information and the ports used as part of its payload. When NAT is applied, only the header parameter is changed, not the payload data that affects the process of data packets within the VoIP switch and terminal.

The common scenario for remote IP deployment is:

- Implementation of an IP Phone with a public IP address talking with an NEC SL2100 behind NAT. An example would be a telecommuter.
Implementation of an IP Phone behind a NAT, which connects to the Internet, terminates in a NEC SL2100 behind a different NAT.

When selecting VPN equipment it is important to consider Quality of Service. Generally, VPN hardware is connected to Internet connections which are unreliable and out of the control of the customer. However, it is possible to set prioritization on some VPN units for voice traffic. This does not solve the unreliability of the Internet, but helps to ensure that the data traffic to and from the LAN do not impair the quality of the voice traffic. (Refer to [QoS](#)).

 *NEC strongly recommends that any VPN hardware used for VoIP has the facility to prioritize voice traffic.*

Section 5 CODEC AND BANDWIDTH

This section describes CODEC and bandwidth and their application with the NEC SL2100 system.

5.1 CODECS

CODEC (COder/DECoder) uses the technology of encoding and decoding a signal. For VoIP, this specifically refers to the algorithm used to convert analog speech to digital data for transmission on an IP network.

The NEC SL2100 system supports three different CODECs:

- G.711
This is the ITU-T recommendation for coding of speech at 64kbps using PCM (pulse code modulation). This CODEC is often described as uncompressed as it uses the same sampling rate as Time-Division Multiplexing (TDM). G.711 has a MOS^{**1} score of 4.2 but uses a large bandwidth for transmission. This CODEC is not commonly used due to the bandwidth required, although it can be acceptable in LAN environment (i.e., IP Phones connected over a 100Mbps LAN).
- G.722
G.722 is an ITU standard CODEC that provides 7kHz wideband audio at data rates from 48 to 64kbps. This is useful in a fixed network Voice Over IP applications, where the required bandwidth is typically not prohibitive, and offers a significant improvement in speech quality over older narrowband CODECs such as G.711, without an excessive increase in implementation complexity.
- G.726
G.726 is an ITU-T ADPCM speech CODEC standard covering voice transmission at rates of 16, 24, 32, and 40kbit/s. It was introduced to supersede both G.721, which covered ADPCM at 32kbit/s, and G.723, which described ADPCM for 24 and 40kbit/s. G.726 also introduced a new 16kbit/s rate. The four bit rates associated with G.726 are often referred to by the bit size of a sample as 2-bits, 3-bits, 4-bits, and 5-bits respectively.
- G.729A
This ITU-T recommendation describes the algorithm for coding of speech signals at 8kbps using CS-ACELP (conjugate-structure algebraic code-excited linear prediction). This CODEC samples the analog signal at 8000Hz and uses a frame size of 10ms. This CODEC has a MOS score of 4.0. G.729 is the most commonly used CODEC for NEC SL2100 VoIP installations. This is due to the fact that it offers high compression (and therefore low bandwidth) while maintaining good speech quality.

Packet Size:

Each CODEC has a set frame length. This is the time that the frame encapsulates. For G.729 and G.711 the frame length is 10ms. It is possible to configure the packet size in the NEC SL2100 programming. To do this, we tell the NEC SL2100 how many frames to encapsulate into each packet for transmission.

For example, the G.729 has a frame length of 10ms - the packet size is set to 3 (in Program 84-11-01). This gives a 10ms x 3 = 30ms packet.

5.2 Bandwidth

The bandwidth required for VoIP calls depends on several factors, including:

- Number of simultaneous calls
- CODEC used
- Frame Size
- Data Networking Protocol used

The more frames encapsulated into each packet, the less bandwidth is required. This is because each packet transmitted has the same header size. Therefore, if numerous very small packets are sent then

^{**1}. The Mean Opinion Score (MOS) provides a numerical measure of the quality of human speech at the destination end of the circuit. The scheme uses subjective tests (opinionated scores) that are mathematically averaged to obtain a quantitative indicator of the system performance.

bandwidth is also being used for a large amount of header information. If we add several frames to the packet, less packets are transmitted and therefore have less header information sent.

If we add many voice frames to each packet, less bandwidth is being used. However, this does have disadvantages. If there is a large packet size, and a particular voice packet is lost, this has a greater impact on the speech quality. If a small quantity of voice frames per packet is being used, the effect of losing a packet is reduced.

As a general rule: The more frames per packet, the less bandwidth is used, but the quality is also lower.

Examples:

Example 1: CODEC: G.729 Frame Size: 10ms Voice Frames per Packet: 2 Voice Sample Size: 20ms (frame size x Voice Frames) Bandwidth Required: 24Kbps

Example 2: CODEC: G.729 Frame Size: 80ms Voice Frames per Packet: 8 Voice Sample Size: 80ms (frame size x Voice Frames) Bandwidth Required: 12Kbps

Section 6 QUALITY OF SERVICE (QoS) IMPLEMENTATION

Section [Voice Quality Improvements](#) discusses some of the problems associated with voice quality. This section describes how QoS can be implemented on data networks to provide the “best case” for VoIP traffic.

Not all network hardware supports QoS and each manufacturer has their own methods of implementing QoS. The explanations below are as generic as possible. The installer/maintainer of the data network should be familiar with the QoS characteristics of their equipment and should be able to configure the equipment accordingly.

Quality of Service is commonly used to describe the actual implementation of prioritization on network hardware. This prioritization (at Layer 2 and Layer 3 of the OSI model) is described in [Figure 6-1 Layer 2 Diagram \(802.1Q\)](#).

6.1 Prioritization

When data is transmitted through a network, bottlenecks can occur causing the available bandwidth to be reduced or the data to increase. This impacts the packet delivery.

Consider data communication between the two computers shown in the diagram [Figure 6-1 Layer 2 Diagram \(802.1Q\)](#). The Hosts can transmit data at 100 Mbps. When a packet from Host A, destined for Host B, reaches the router, the available bandwidth is reduced to 256Kbps and the packet flow must be reduced. [Figure 6-3 Network Bottleneck Example](#) shows a diagram of this condition.

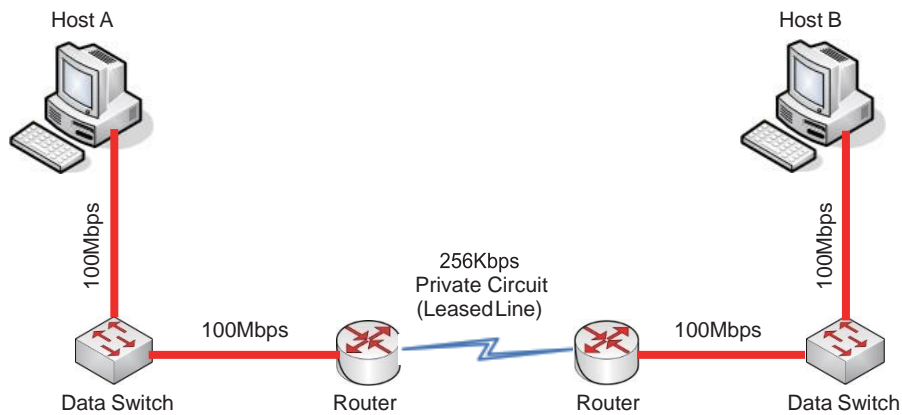


Figure 6-3 Network Bottleneck Example

For this example, each end of the network has only one host. Typically, many hosts are sending data over the narrow bandwidth. The routers buffer packets and transmit them over the WAN lines as efficiently as possible. When this occurs, certain packets are dropped by the router and some packets are delayed.

For most data applications this packet loss/delay is not critical. For example, a delay of one to five seconds to transmit an email is imperceptible. When VoIP is implemented, this loss/delay has a massive impact on the voice quality. The resulting gaps in speech, distortion and delay are unacceptable for voice traffic.

To avoid this problem, it is possible to prioritize the VoIP packets. The router examines all packets received, determines the priority level of the packet, and forwards it accordingly. The data**1 is assigned lower priority and the voice is transmitted before the data. This can have a negative impact on the data network if a lot of voice is transmitted.

Figure 6-4 Voice and Data Network Implementation shows how a voice and data network can be implemented.

***1. This description discusses voice and data. These terms are commonly used when describing QoS, although in the case of VoIP, the voice is actually converted to IP and transmitted as data. Therefore, everything transmitted on a Data Network is data, but logically we think of this as voice and data traffic.*

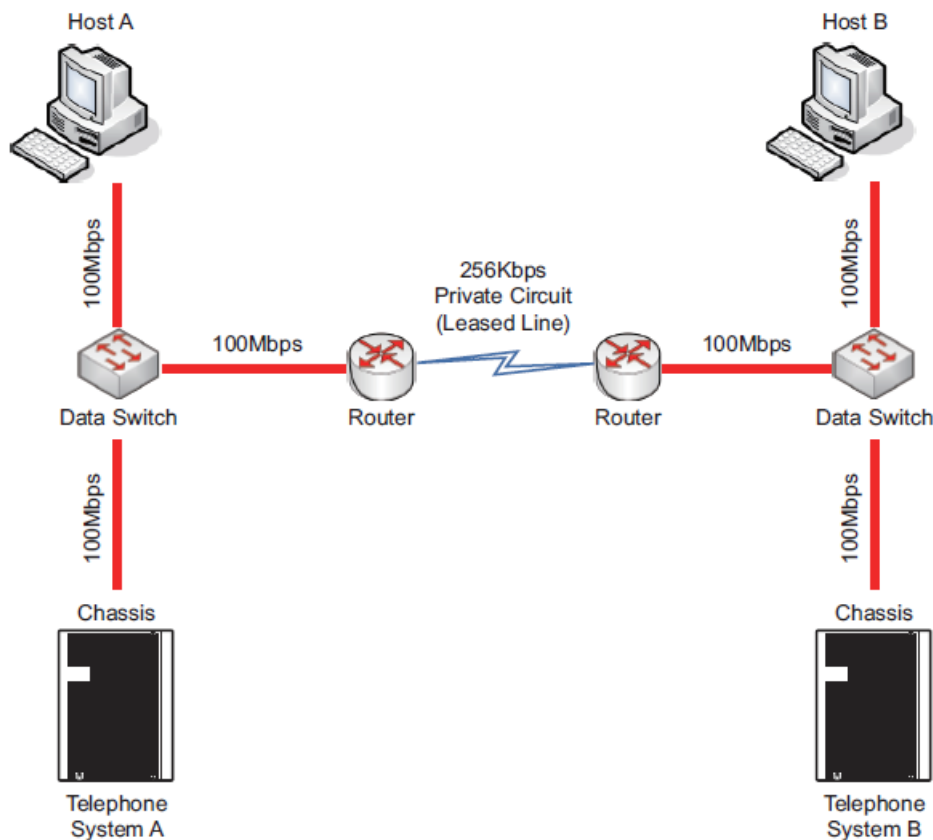


Figure 6-4 Voice and Data Network Implementation

After the router is configured for QoS, it examines incoming packets and allocates a priority to the packet. [Figure 6-5 Priority Queuing on Voice and Data Networks](#) shows the affect priority queuing has on voice and data networks. The packets arrive randomly. They are processed and output according to the QoS policy. The VoIP traffic is output first.

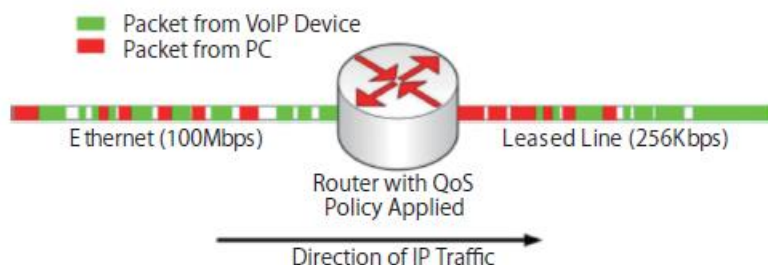


Figure 6-5 Priority Queuing on Voice and Data Networks

To enable this type of queuing it is necessary to:

1. Configure the VoIP equipment to mark its packets with a specific value so that the switches/routers can identify that it is voice – Called Marking.
2. Configure the network equipment to recognize the difference between the different Marked packets – Called Classification. (i.e., informs the router what a voice packet looks like.
3. Configure the network equipment to give priority to the packets that have been classified as voice – Called Priority Queuing.

6.2 Layer 2 QoS (802.1pq)

QoS is most commonly implemented at Layer 3 of the OSI model. This layer deals with IP addresses, and is usually handled by Routers. However, sometimes it is necessary to implement Layer 2 QoS – usually in large LAN environments with many IP phones.

Layer 2 devices work with Ethernet frames (encapsulated IP packets) rather than IP addresses. Layer 2 QoS uses the Priority field of the Ethernet frame. This field has three bits and can have eight possible values (000 to 111 in binary). Some switches can be configured to prioritize traffic based on these values. This field is available only if the Ethernet device is configured for VLAN (IEEE 802.1q) operation (VLAN is outside the scope of this document).

Protocol Structure - IEEE 802.1p: LAN Layer 2 QoS

Table 6-1 Protocol Structure for Layer 2 QoS shows the format of an Ethernet frame and the User Priority field that is used for Layer 2 QoS.

Table 6-1 Protocol Structure for Layer 2 QoS

IEEE 802.1Q Tagged Frame for Ethernet								
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	2 Bytes	2 Bytes	42~1496 Bytes	4 Bytes
Preamble	SFD	DA	SA	TPID	TCI	Type Length	Data	CRC

Expanded View of TCI Field		
3 Bits	1 Bit	12 Bits
User Priority	CFI	Bits of VLAN ID (VID) to identify possible VLANs

The following define the fields used for the protocol structure:

Preamble (PRE) - The PRE is an alternating pattern of ones and zeros that tells receiving stations a frame is coming, and synchronizes frame-reception portions of receiving physical layers with the incoming bit stream.

Start-of-frame delimiter (SFD) - The SFD is an alternating pattern of ones and zeros, ending with two consecutive 1-bits indicating that the next bit is the left-most bit in the left-most byte of the destination address.

Destination Address (DA) - The DA field identifies which station(s) should receive the frame.

Source Addresses (SA) - The SA field identifies the sending station.

Tag Protocol Identifier (TPID) - The defined value of SL2100 in hex. When a frame has the EtherType equal to SL2100, this frame carries the tag IEEE 802.1Q / 802.1P.

Tag Control Information (TCI) - The field including user priority, Canonical format indicator and VLAN ID.

User Priority - Defines user priority, giving eight priority levels. IEEE 802.1P defines the operation for these three user priority bits.

CFI - Canonical Format Indicator is always set to zero for Ethernet switches. CFI is used for compatibility reason between Ethernet type network and Token Ring type network.

VID - VLAN ID is the identification of the VLAN, which is basically used by the standard 802.1Q. It allows the identification of 4096 VLANs.

Length/Type - This field indicates either the number of MAC-client data bytes that are contained in the data field of the frame, or the frame type ID if the frame is assembled using an optional format.

Data - Is a sequence of bytes of any value. The total frame minimum is 64 bytes.

Frame Check Sequence (FCS) - This sequence contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending MAC and is recalculated by the receiving MAC to check for damaged frames.

Example Ethernet Frame with Layer 2 QoS Enabled

The example below shows an Ethernet Frame containing one RTP (speech) packet. The Frame is VLAN tagged, has a VLAN ID of 99 and a VLAN Priority of 5. It is also possible to see that the Layer 3 QoS has not been set.

Ethernet Frame Example - Layer 2 QoS Enabled

```

Source Destination Protocol
172.16.0.101 172.16.0.21 RTP
Info
Payload type=ITU-T G.729, SSRC=701655963, Seq=28165, Time=21520
Frame 160 (78 bytes on wire, 78 bytes captured)
Arrival Time: Jan 18, 2005 13:55:44.842738000
Time delta from previous packet: 0.008241000 seconds
Time since reference or first frame: 2.910072000
seconds Frame Number: 160
Packet Length: 78 bytes
Capture Length: 78 bytes
Ethernet II, Src: 00:60:b9:c6:6e:45, Dst: 00:60:b9:c1:ab:a3
Destination: 00:60:b9:c1:ab:a3 (Nitsuko_c1:ab:a3)
Source: 00:60:b9:c6:6e:45 (Nitsuko_c6:6e:45)
Type: 802.1Q Virtual LAN (0xSL2100)
802.1q Virtual LAN
101. .... = Priority: 5 (Layer 2 Priority = 5)
...0 .... = CFI: 0
... 0000 0110 0011 = ID: 99
Type: IP (0x0800)
Internet Protocol, Src Addr: 172.16.0.101 (172.16.0.101), Dst Addr:
172.16.0.21 (172.16.0.21)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default
(0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 60
Identification: 0x0086 (134)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 30
Protocol: UDP (0x11)
Header checksum: 0x4391 (correct)
Source: 172.16.0.101 (172.16.0.101)
Destination: 172.16.0.21 (172.16.0.21)
User Datagram Protocol, Src Port: 10022 (10022), Dst Port: 10020 (10020)
Source port: 10022 (10022)
Destination port: 10020 (10020)
Length: 40
Checksum: 0x0581 (correct)
Real-Time Transport Protocol
Stream setup by SDP (frame
1) Setup frame: 1
Setup Method: SDP
10.. .... = Version: RFC 1889 Version (2)
..0. .... = Padding: False
...0 .... = Extension: False
... 0000 = Contributing source identifiers count: 0
0... .... = Marker: False
.001 0010 = Payload type: ITU-T G.729 (18)
Sequence number: 28165
Timestamp: 21520
Synchronization Source identifier: 701655963
Payload: 76AC9D7AB6ACE2510B3A3338646DA738...

```

6.3 Layer 3 QoS

QoS is most commonly implemented at Layer 3. This allows the VoIP packets to be prioritized by routers, before they are forwarded to their next hop.

Layer 3 QoS uses the Type of Service (ToS) field of the IP packet. This is an 8-bit field in the header of the IP packet. The field can be used by Diffserv or IP Precedence. Although these are two different standards, the actual field in the IP packet is the same – Only the method of evaluating the bits differs.

QoS does not function only by using the ToS field (i.e., Marking the VoIP packets). It is an end-to-end process and requires configuration on all networking devices.

Packet Marking is the first step in this process and is often the only step that the NEC dealer performs.

Table 6-2 Layer 3 QoS Example

Protocol Structure - IP/Pv4 Header (Internet Protocol Version 4)

4 Bits	4 Bits	8 Bits	16 Bits	
Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
Time to Live	Protocol	Header Checksum		
Source Address				
Destination Address				
Option + Padding				
Data				

Type of Service Field (Diffserv)

6 Bits	2 Bits
Differentiated Services Code Point	ECN (Not QoS related)

Type of Service Field (IP Precedence - Ref. RFC 1349)

3 Bits	1 Bit	1 Bit	1 Bit	1 Bit	1 Bit
IP Precedence Value	Delay	Throughput	Reliability	Cost	MBZ (must be zero)

Listed below are the fields used in [Table 6-2 Layer 3 QoS Example](#).

Version – the version of IP currently used.

IP Header Length (IHL) – datagram header length. Points to the beginning of the data. The minimum value for a correct header is 5.

Type-of-Service – Indicates the quality of service desired by specifying how an upper-layer protocol would like a current datagram to be handled, and assigns datagrams various levels of importance. This field is used for the assignment of Precedence, Delay, Throughput and Reliability.

Total Length – Specifies the length, in bytes, of the entire IP packet, including the data and header. The maximum length specified by this field is 65,535 bytes. Typically, hosts are prepared to accept datagrams up to 576 bytes.

Identification – Contains an integer that identifies the current datagram. This field is assigned by sender to help receiver to assemble the datagram fragments.

Flags – Consists of a 3-bit field of which the two low-order (least-significant) bits control fragmentation. The low-order bit specifies whether the packet can be fragmented. The middle bit specifies whether

the packet is the last fragment in a series of fragmented packets. The third or high-order bit is not used.

Fragment Offset – This 13-bit field indicates the position of the fragment data relative to the beginning of the data in the original datagram, which allows the destination IP process to properly reconstruct the original datagram.

Time-to-Live – This is a counter that gradually decrements down to zero, at which point the datagram is discarded. This keeps packets from looping endlessly.

Protocol – Indicates which upper-layer protocol receives incoming packets after IP processing is complete.

Header Checksum – Helps ensure IP header integrity. Since some header fields change, e.g., Time To Live, this is recomputed and verified at each point that the Internet header is processed.

Source Address – Specifies the sending node.

Destination Address – Specifies the receiving node.

Options – Allows IP to support various options, such as security.

Data – Contains upper-layer information.

6.4 IP Precedence

IP Precedence is a QoS method that combines a priority value with different on/off parameters; Delay, Throughput, Reliability and Cost. The MBZ (Must be Zero) bit is not used.

Using the ToS bits, you can define up to eight classes of service. Other devices configured throughout the network can then use these bits to determine how to treat the packet in regard to the type of service to grant it. These other QoS features can assign appropriate traffic-handling policies including congestion management and bandwidth allocation. By setting IP Precedence levels on incoming traffic and using them in combination with QoS queuing features, you can create differentiated service.

Table 6-3 Type of Service Field (IP Precedence - i Ref. REC 1349)

3 Bits	1 Bit	1 Bit	1 Bit	1 Bit	1 Bit
IP Precedence Value	Delay	Throughput	Reliability	Cost	MBZ (must be zero)

IP Precedence Value

Value	Binary Value	Description
0	000	Routine
1	001	Priority
2	010	Immediate
3	011	Flash
4	100	Flash Override
5	101	CRITIC/ECP
6	110	Internetwork Control
7	111	Network Control

Throughput

Value	Description
0	Normal Throughput
1	High Throughput

Reliability

Value	Description
0	Normal Reliability
1	High Reliability

Delay

Value	Description
0	Normal Delay
1	Low Delay

Cost

Value	Description
0	Normal Cost
1	Low Cost

6.5 Diffserv (Differentiated Service)

Differentiated Services (Diffserv) uses the ToS field in an IP header. Diffserv is now commonly used instead of IP Precedence (refer to [IP Precedence](#)) as it provides greater flexibility. This method uses six bits of the ToS field to determine the priority – which provides up to 64 possible values. The combination of binary digits is known as the Diffserv Codepoint (DSCP).

Table 6-4 Diffserv Parameters

6 bits	2 bits
Differentiated Services Code Point	ECN (Not QoS related)

The example below shows an Ethernet Frame containing one RTP (speech) packet. The IP Packet has the ToS field set to 101000 (binary) which is the equivalent of Class Selector 5. The router(s) in this network should be programmed to prioritize based on CS5.

Ethernet Frame Example - Containing One RTP (Speech) Packet

```
Source Destination Protocol
172.16.0.21 172.16.0.101 RTP
Info
Payload type=ITU-T G.729, SSRC=732771006, Seq=30885, Time=20560
Frame 159 (65 bytes on wire, 65 bytes captured)
Arrival Time: Jan 18, 2005 13:55:44.834497000
Time delta from previous packet: 0.000445000 seconds
Time since reference or first frame: 2.901831000 seconds
Frame Number: 159
Packet Length: 65 bytes
Capture Length: 65 bytes
Ethernet II, Src: 00:60:b9:c1:ab:a3, Dst: 00:60:b9:c6:6e:45
Destination: 00:60:b9:c6:6e:45 (Nitsuko_c6:6e:45)
Source: 00:60:b9:c1:ab:a3 (Nitsuko_c1:ab:a3)
```

```

Type: IP (0x0800)
Internet Protocol, Src Addr: 172.16.0.21 (172.16.0.21), Dst Addr: 172.16.0.101
(172.16.0.101)
Version: 4
Header length: 20 bytes
Diff Services Field: 0xa0 (DSCP 0x28: Class Selector 5; ECN: 0x00)
1010 00.. = Diff Services Codepoint: Class Selector 5 (0x28)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 44
Identification: 0x0069 (105)
Flags: 0x00
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
..0. = More fragments: Not set
Fragment offset: 0
Time to live: 30
Protocol: UDP (0x11)
Header checksum: 0x431e (correct)
Source: 172.16.0.21 (172.16.0.21)
Destination: 172.16.0.101 (172.16.0.101)
User Datagram Protocol, Src Port: 10020 (10020), Dst Port: 10022 (10022)
Source port: 10020 (10020)
Destination port: 10022 (10022)
Length: 24
Checksum: 0x5293 (correct)
Real-Time Transport
Protocol
Stream setup by SDP (frame 112)
Setup frame: 112
Setup Method: SDP
10.. .... = Version: RFC 1889 Version (2)
..1. .... = Padding: True
...0 .... = Extension: False
.... 0000 = Contributing source identifiers count: 0
0... .... = Marker: False
.001 0010 = Payload type: ITU-T G.729 (18)
Sequence number: 30885
Timestamp: 20560
Synchronization Source identifier: 732771006
Payload: 3ED0
Padding data: 00
Padding count: 2

```

6.6 Comparison of IP Precedence and Diffserv Values

As stated earlier, IP Precedence and Diffserv use the same 8-bit ToS field in the IP header to mark packets. It is possible to have the same ToS value for either method which means that the two methods can work alongside each other.

For example, if the VoIP equipment supports IP Precedence and the router can prioritize only using the DSCP they can be set to the same value. Refer to [Table 6-5 IP Precedence and Diffserv Values Comparison](#) for the values.

Table 6-5 IP Precedence and Diffserv Values Comparison

DSCP Decimal	DSCP Binary	IP Precedence	Description
0	000000	0	Class Selector 0
1	000001		
2	000010		
3	000011		
4	000100		
5	000101		
6	000110		
7	000111		

DSCP Decimal	DSCP Binary	IP Precedence	Description
8	001000	1	Class Selector 1
9	001001		
10	001010		AF11 (Assured Forwarding)
11	001011		
12	001100		AF12 (Assured Forwarding)
13	001101		
14	001110		AF13 (Assured Forwarding)
15	001111		
16	010000	2	Class Selector 2
17	010001		
18	010010		AF21 (Assured Forwarding)
19	010011		
20	010100		AF22 (Assured Forwarding)
21	010101		
22	010110		AF23 (Assured Forwarding)
23	010111		
24	011000	3	Class Selector 3
25	011001		
26	011010		AF31 (Assured Forwarding)
27	011011		
28	011100		AF32 (Assured Forwarding)
29	011101		
30	011110		AF33 (Assured Forwarding)
31	011111		
32	100000	4	Class Selector 4
33	100001		
34	100010		AF41 (Assured Forwarding)
35	100011		
36	100100		AF42 (Assured Forwarding)
37	100101		
38	100110		AF43 (Assured Forwarding)
39	100111		
40	101000	5	Class Selector 5
41	101001		
42	101010		
43	101011		
44	101100		
45	101101		
46	101110		EF (Expedited Forwarding)
47	101111		
48	110000	6	Class Selector 6
49	110001		
50	110010		

DSCP Decimal	DSCP Binary	IP Precedence	Description
51	110011		
52	110100		
53	110101		
54	110110		
55	110111		
56	111000	7	Class Selector 7
57	111001		
58	111010		
59	111011		
60	111100		
61	111101		
62	111110		
63	111111		

6.7 Programming QoS in the NEC SL2100 System

6.7.1 Marking Voice Traffic - Program 84-10-XX

Before programming the NEC SL2100 system, discuss the requirements with the network engineering staff or the managed network provider. If the ToS markings that are used are not specifically configured into the network equipment, the voice traffic is handled by the default queue and is given lowest priority.

6.7.2 NEC SL2100 Voice Protocols

The NEC SL2100 system supports the following types of VoIP traffic.

Number	Protocol Type	Description
1	H.323	Communication from VoIPDB to Network
2	RTP/RTCP	Voice (RTP) and Call Quality Data (RTCP)
3	SIP	Communication from VoIPDB to Standard SIP device.
4	SIP MLT	Communication from VoIPDB to SIP Multiline Terminal.
5	SIP Trunks	Communication from VoIPDB to Network

6.7.3 Configuring Diffserv


Use Program 84-10-10 to select the logic for marking the ToS field. The choices are:

Number	ToS Mode	Programs Enabled
0	None	None – ToS bits are: 00000000

Number	ToS Mode	Programs Enabled
1	IP Precedence	84-10-02 Priority – 0=Lowest ~ 7=Highest (ToS bits: 0~2) 84-10-03 Delay – 0=Normal, 1=Low (ToS Bit: 3) 84-10-04 Throughput – 0=Normal, 1=High (ToS Bit: 4) 84-10-05 Reliability – 0=Normal, 1=High (ToS Bit: 5) ToS Bit 7: Always 0 <i>Typically, only one of bits 3~6 is set to 1 and the other three bits are set to 0. For example, to maximize route reliability, set 84-10-05 to 1 and leave 84-10-03, 84-10-04 and 84-10-06 at 0 (default).</i>
2	Diffserv	84-10-07 DSCP Value in Decimals: 0~63 (ToS bits: 0~5) ToS Bits 6 & 7 are not evaluated

6.7.4 Configuration Examples for Classification and Queuing

Figure 6-6 Common Network with Cisco Router shows a typical network scenario and an example of a Cisco router configuration.

 This document provides a general description of VoIP technology, but it does not discuss individual manufacturer solutions. This sample configuration is provided as a common scenario. It is a good example of how QoS can be implemented on a router. NEC does not endorse or provide support on any third party equipment unless it is supplied by NEC.

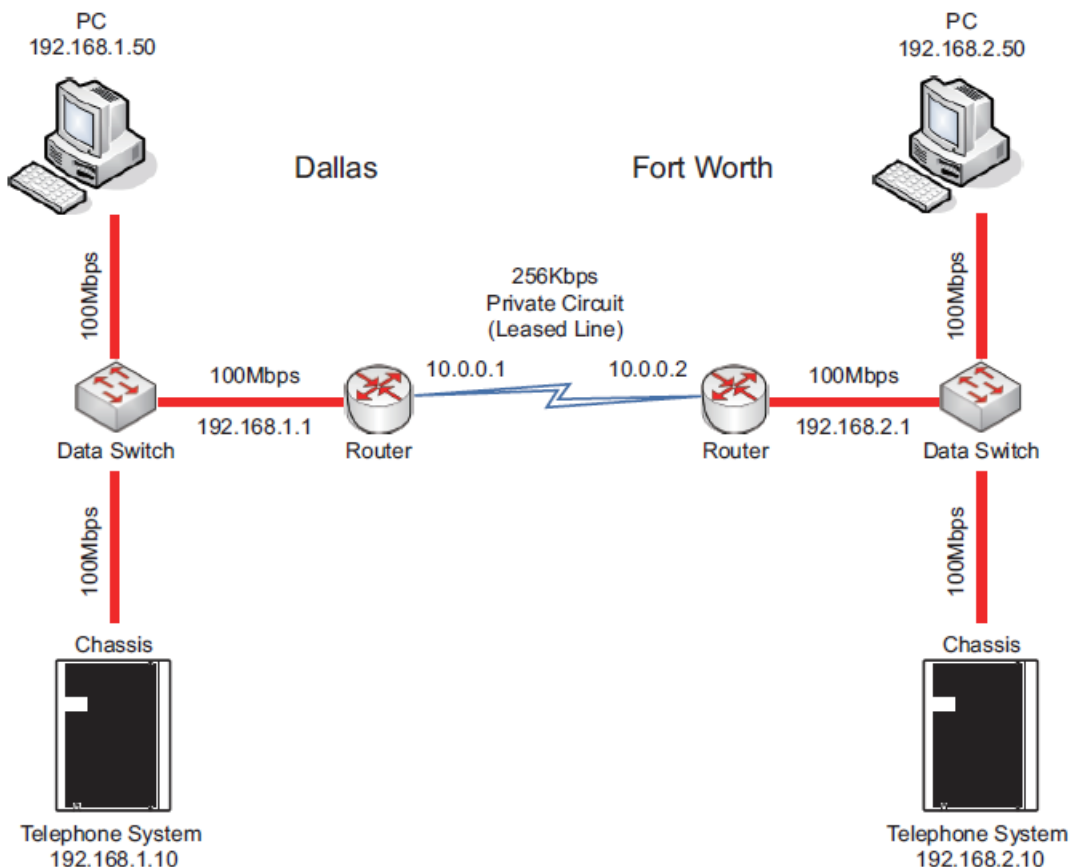


Figure 6-6 Common Network with Cisco Router

See Table 6-6 Cisco Router Configuration Example for configuration information about the Cisco 2621 router. A description of key commands follows.

Table 6-6 Cisco Router Configuration Example

```

Current Configuration : 2023 bytes
version 12.3
hostname Cisco2621
|
class-map match-any VoIPClass (1)
match ip dscp cs5 (2)
policy-map VoIPPolicy (3)
class VoIPClass(4)
priority 50(5)
class class-default(6)
fair-queue(7)
|
interface FastEthernet0/0
description Connects to Dallas LAN
ip address 192.168.1.1 255.255.255.0
|
interface Serial0/0
description Connects to Fort Worth via Kilostream
bandwidth 256(8)
ip address 10.0.0.1 255.255.0.0
service-policy output VoIPPolicy(9)
encapsulation ppp
|
ip route 0.0.0.0 0.0.0.0 10.0.0.2

```

Configuration Example Explanation:

1. Defines a Class Map called VoIPClass.
2. Matches any packets that have the ToS field set to IP Precedence 5 / DSCP 40 and assigns them to VoIPClass.
3. Defines a Policy Map called VoIPPolicy.
4. Creates a Class called VoIPClass and assigns this to the VoIPPolicy.
5. Allocates 50Kbps of bandwidth to the VoIPClass.
- 6 & 7. Determines that any data that does not match VoIPClass should be processed using the "fair-queue" method (i.e., No Prioritization).
8. Determines the amount of bandwidth available on the Serial interface – essential for the QoS calculations.
9. Applies the VoIP Policy to any packets that exit the serial interface. This means that data being received (input) does not use this policy.

Section 7 PORT DESIGNATIONS

Following table shows an IP Port related in the SL2100 System.

The assigning IP port number cannot be duplicated in the same port number listed below.

For the detailed programming information, refer to the programming manual.

Table 6-7 Port number list of SL2100 System

Well-known port or Fixed port ("-" is fixed port (cannot change))	IP Port Numbers	Description
well-known port	22	ssh
well-known port	53	domain
well-known port	67	bootps
well-known port	68	bootpc
well-known port	115	sftp
well-known port	123	ntp
well-known port	137	netbios-dgm

Well-known port or Fixed port ("-" is fixed port (cannot change))	IP Port Numbers	Description
well-known port	161	snmp
well-known port	162	snmptrap
-	1718	
-	5555	
-	6666	
-	1900	
-	2567	Lua application
-	3000	For InDECTPro
-	7080	For InDECTPro
-	20020 ~ 20274	Reserved
-	20100	
-	20200	
-	20300	
-	20400	
-	27998	For InDECTPro
-	27999	For InDECTPro
-	33512	Lua application
-	33516	Lua application
-	33518	For InDECTPro
-	33519	Lua application
-	57000	Reserved
-	58000	
-	58001	
-	58002	
-	59000 ~ 59063	
-	60050	Lua application
-	60060	Lua application
-	60300	Lua application
-	63516	Lua application
-	63517	Lua application
-	63518	For InDECTPro
-	63519	Lua application
Related IP Port programming		
Program Number	Default	Description
10-20-01 CTI Server	0	
10-20-01 ACD-MIS	4000	
10-20-01 Networking System	30000	
10-20-01 SMDR Output	0	
10-20-01 DIM Output	0	
10-20-01 UC Web Application	0	
10-20-01 1st Party CTI	0	
10-20-01 O&M Server	8010	
10-20-01 Traffic Report Output	0	

Well-known port or Fixed port ("-" is fixed port (cannot change))	IP Port Numbers	Description
10-20-01 Room Data Output for Hotel Service	0	
10-20-01 IP-DECT Directory Access	0	
10-20-01 Presence	0	
10-23-03 (Cannot be changing)	1720	
10-29-04	5060	SIP Trunk
10-29-07	5060	
10-46-06	5080	SIP MLT
10-46-12	30000	
10-46-13	5081	SIP MLT
10-47-01	6080	
20-64-03	0	
20-64-06	0	
20-64-07	0	When it is not 0, 512 port which continues from a set port is reserved. For example, when this port number is 50000, 50000 ~ 50511 ports are reserved.
20-64-08	0	When it is not 0, 460 port which continues from a set port is reserved. For example, when this port number is 10020, 10020 ~ 10479 ports are reserved.
42-06-01	5129	PMS Service
84-02-33	1730	
84-02-36	20001	
84-14-06	[profile 1]: 5060 [profile 2]: 5062 [profile 3]: 5090 [profile 4]: 5092 [profile 5]: 5094 [profile 6]: 5096	
84-20-01	5070	SIP SLT
84-26-02	10020	RTP: 10020 ~ 10275
84-26-03	10021	RTCP: 10021 ~ 10276
84-27-06	10100	
84-27-07	4000	
90-54-01	80	WebPro (HTTP)
90-54-02	8000	PCPro
90-54-03	443	WebPro(HTTPS)

MEMO

SIP Trunking

Section 1 VoIP

VoIP (Voice over Internet Protocol or Voice over IP) allows the delivery of voice information using the Internet protocol (sending data over the Internet using an IP address). This means that digital voice information can be sent in packets over the Internet rather than using the traditional public switch telephone network (CO lines). A major advantage of VoIP is that it avoids the tolls charged by ordinary telephone service.

Using VoIP equipment at a gateway (a network point that acts as an entrance to another network), the packetized voice transmissions from users in the company are received and routed to other parts of the company intranet (local area or wide area network) or they can be sent over the Internet using CO lines to another gateway. ^{**1}

Section 2 IP NETWORKING

IP Networking uses VoIP technology to connect two or more telephone systems together. This allows calls to be made between sites without using the public telephone network. This can save money and make communication between sites much easier.

The following Networking modes are available on the NEC SL2100 system:

- SIP TIE lines
- SIP Trunks (to a SIP Trunk Provider)

Section 3 SIP TRUNKING

3.1 Introduction

SIP (Session Initiation Protocol) is used for Voice over IP. It is defined by the IETF (Internet Engineering Task Force) in RFC2543 and RFC3261. SIP trunking is the term used for linking a PBX, such as the NEC SL2100 system, to the public telephone network by means of VoIP. This provides the ability for users to place and receive communications and services from any location and for networks to identify the users wherever they are located.

SIP analyzes requests from clients and retrieves responses from servers then sets call parameters at either end of the communication, handles call transfer and terminates.

The NEC SL2100 system implementation and programming for SIP are very similar. The call routing, call features and speech handling (RTP) are the same. Only the signaling protocol is different.

***1. The voice quality of VoIP depends on variables such as available bandwidth, network latency and Quality of Service (QoS) initiatives, all of which are controlled by the network and Internet Service Providers. Because these variables are not in NEC control, it cannot guarantee the performance of the user's IP-based remote voice solution. Therefore, NEC recommends connecting VoIP equipment through a local area network using a Private IP address.*

With the NEC SL2100 system, SIP trunks can receive incoming calls with Caller ID, place outgoing calls, and transfer SIP trunks to IP, SIP, analog and digital stations, and across a network.

Currently, however, SIP Centrex Transfer is not supported.

If a common carrier supports SIP, the NEC SL2100 can connect the SIP Carrier and outgoing calls to the PSTN (Public Switched Telephone Network) network and the common IP network using an NEC SL2100 SIP trunk.

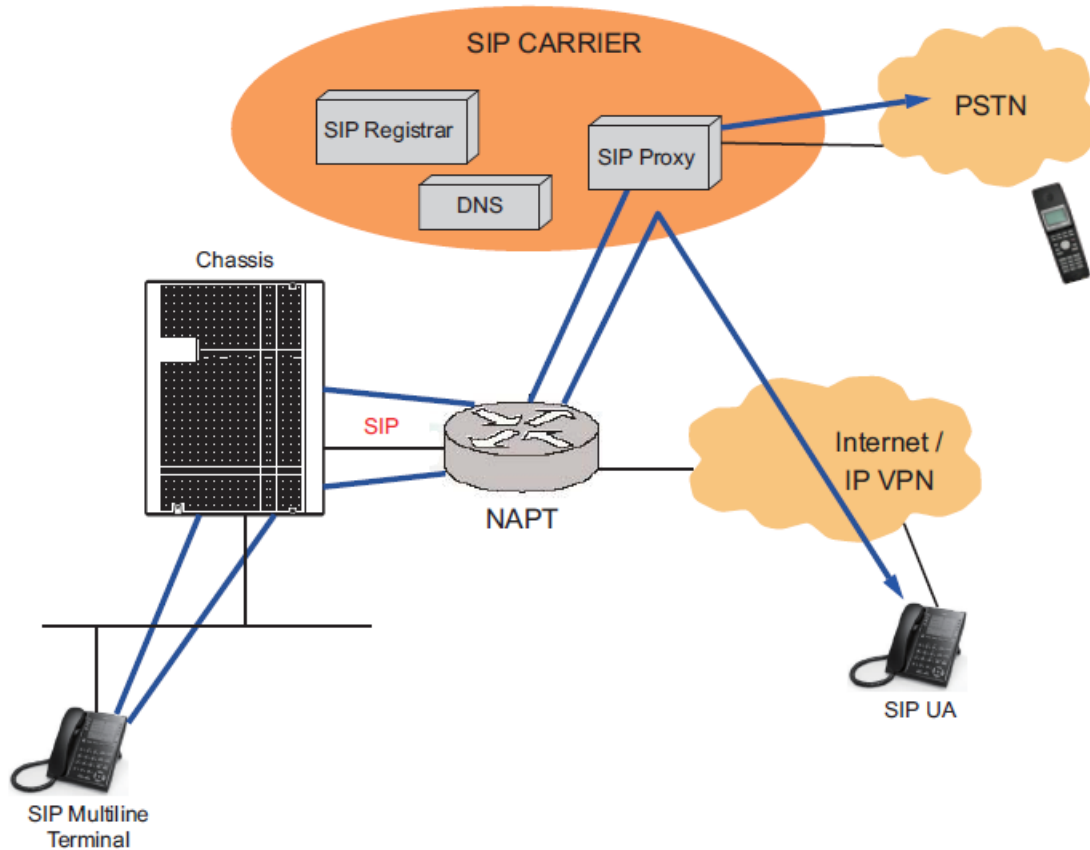


Figure 7-1 Common IP Network using NEC SL2100 SIP Trunk

3.1.1 SIP Trunking Requirements

The following are required when using the SIP trunk on the NEC SL2100 system:

- CPU-C1 software
- VOIPDB (VoIP Daughter Board) Programming Conditions



The VoIPDB is only a requirement if more than the built in (8) DSP resources on the CPU are required. Adding the VoIPDB provides an additional (8) DSP resources for a total of (16). If more than (16) DSP resources are required, additional IP Channel licenses are required.

The following conditions apply when programming the NEC SL2100 system for SIP Trunking:

- If entries are made in Program 10-29-xx for a SIP Server and the SIP Server is then removed or not used, the entries in Program 10-29-xx must be set back to their default settings. Even if **Program 10-29-01 : SIP Proxy Setup – Outbound Proxy** is set to 0, the NEC SL2100 system checks the settings in the remaining 10-29 programs.

- SIP Multi-profile support is added. The simultaneous use of a SIP trunk interconnection and a SIP trunk carrier connection or six SIP carriers at the same time is supported.
Limitations:
 - Each profile requires a different number for every SIP trunk port set in PRG 84-14-06.
 - Six carriers must be connected using a single route. The system only supports one gateway.
 - Only one DNS server can be set for the SL2100 to connect to six different SIP Carriers.
- The NEC SL2100 system restricts an outgoing call under the following conditions:
 - SIP configuration failed
 - SIP registration failed
 - CPU-C1/VOIPDB daughter board link down
 - Lack of VOIPDB DSP resource
 - Lack of bandwidth

3.1.2 SIP Trunking Setup

Use the following steps to initially set up SIP Trunking for the NEC SL2100 system:

1. By default, the NEC SL2100 is assigned a static IP address and runs behind a NAT router.



When using an NEC SL2100 on a LAN behind an NAPT router, forward port 5060 to the IP address of the NEC SL2100 CPU-C1 (commonly called the SL2100 CPU) since the signaling is handled by the CPU-C1. Then, since the media stream (the speech) uses a large range of ports for the RTP packages, forward the ports (10020~10147) to the IP address of the VOIPDB. Or, use the DMZ option for the VOIPDB. This means that the VOIPDB is not actually behind the firewall. This is achieved by connecting the VOIPDB to a physical or virtual DMZ port. You can also achieve the same result by port forwarding 10020 to 10147.

2. Define the SIP Carrier account information (user name, password, domain name/IP address to the provider).
3. Define the trunk ports as SIP.
4. Set the Expire Time.

Section 4 SIP TRUNK OVERVIEW

This section is an overview of basic SIP trunk behavior, protocols, supported SIP trunking methods and options, supported CODEC as well as other supported functions of SIP Trunking.

4.1 General Information

The NEC SL2100 SIP Trunks behave like some SIP User Agents (UA). UA is the client application used with a particular network protocol.

The NEC SL2100 provides a maximum of 31 register IDs and can register these IDs with any SIP server.

A maximum number of 64 SIP trunks can be used with the NEC SL2100 system. The maximum number of simultaneous VoIP calls is 128 and is determined by the number of resources available on the VoIPDB.

The NEC SL2100 can connect any SIP server over a NAPT router by one static global IP address. The NEC SL2100 system supports a DNS resolution access and an IP address direct access for SIP servers and supports the sub-address feature with SIP trunk interconnection.

4.2 Supported Protocols

The following protocols are supported:

- SIP (RFC2543 bis04)
- SIP RFC3261 Supported [updated version of RFC2543]
- The SIP stack has been updated from RFC2543 Base to RFC3261 Base
- SDP
- RTP/RTCP
- UDP
- IPv4
- T.38 (draft-ietf-sipping-realtimefax-02.txt)

4.3 Supported SIP Methods

The following SIP methods are supported with the NEC SL2100 system:

- REGISTER
- INVITE
- BYE
- CANCEL
- ACK
- PRACK
- Response 1xx 2xx, 3xx, 4xx, 5xx, 6xx

The following features are available:

- **Support the 401 response for the Initial Invite**
If 401 message is sent for the Initial Invite, with previous software, the system cannot respond to the message correctly.
- **Support the 401/407 response for the Invite of Session Timer**
If 401/407 response is sent for the invite of Session Timer, the system can send the Invite message with Authentication header.
- **Support the 128 byte size of Nonce max value sent by the 401/407 message**
The Nonce maximum size sent by the 401/407 message is expanded to 128 byte. With previous software, 64 byte size can be received.

4.4 Supported SIP Trunking Options

The options listed below are supported with SIP Trunking.

- 100rel
- Session Timer
- Early Media

4.5 Supported CODEC

SIP Trunking can use the following CODECs.

- G.729. Low bandwidth requirement, and is used on most Wide Area Network links.
 - VAD
 - VIF size 20ms~30ms
- G.711 – High bandwidth requirement – usually used on Local Area Networks.
- G.722 – This CODEC is useful in fixed network, Voice over IP applications, where the required bandwidth is typically not prohibitive.
- G.726 – is an ITU-T ADPCM speech coded standard covering the transmission of voice at rates of 16, 24, 32, and 40Kbps.

Section 5 SUPPORTED SIP TRUNKING FUNCTIONS

The functions in this section are supported by NEC SL2100 SIP Trunking.

5.1 Address Resolution

If using any SIP Proxy Server, the NEC SL2100 always sends messages to an external SIP server.

If not using any SIP Proxy Server, the NEC SL2100 uses the internal address table (Program 10-23 : SIP System Interconnection Setup).

When a user creates an interconnection network with SIP trunks, **Program 10-29-14 : SIP Server Information Setup - SIP Carrier Choice** must be set to 0 (default).

5.2 Authentication Process

When using an external SIP Server provided by a carrier, an authentication process is usually needed.

NEC SL2100 SIP trunks support HTTP digest authentication process (MD5). This process is done on a Register process and Initial INVITE process.

5.3 Caller ID

Caller ID for SIP Trunks is set by **Program 21-17 : IP Trunk (SIP) Calling Party Number Setup for Trunk**.

Caller ID for SIP Extensions is **Program 21-19 : IP Trunk (SIP) Calling Party Number Setup for Extension**.

Programs follow program priority as follows: 21-19 > 21-17 > 10-36-02

With a trunk-to-trunk transfer and Trunk-to-Trunk Outgoing Caller ID Through Mode enabled (**Program 14-01-24**), the Caller ID/sub-address (received from the incoming trunk) is sent. If a SIP trunk is connected to any SIP carrier, the sub-address is not transferred.

Calling Party Name is not provided for outgoing calls on SIP trunks.

5.4 Carrier Support

If a common carrier supports SIP, the NEC SL2100 can connect:

- the SIP Carrier
- the outgoing call to the PSTN network
- the common IP network via an NEC SL2100 SIP trunk.

A conformity test with a carrier's SIP server is recommended.

5.5 Early Media

When the NEC SL2100 receives the response *18x w/SDP* and the CODEC negotiation is a success, the NEC SL2100 starts to send/receive RTP packets.

5.6 Fault Tolerance

When the NEC SL2100 uses an external SIP Server and if the registration process fails, the NEC SL2100 blocks outgoing calls with SIP trunks. All SIP trunk ports are placed into a busy status.

If the NEC SL2100 has trunk groups that include both SIP trunks and ISDN trunks, and all SIP trunks are busy, a user can make an outgoing call using an ISDN trunk as a bypass.

5.7 Network Address Port Translation (NAPT)

NEC SL2100 SIP trunk can pass through a NAPT router. The related system data is **Program 10-12-06 : CPU-C1 Network Setup – NAPT Router (On/Off)** and **Program 10-12-07 : CPU-C1 Network Setup – NAPT Router IP Address** (do not set with a dynamic router IP address).

Incorrect settings with these two programs can cause one-way audio problems.

The WAN global IP is set in the system data by the user or automatically using the NAT traversal feature (UPnP). The related system data is **10-37-01 : UPnP Setup – UPnP Mode (On/Off)** and **10-37-02 : UPnP Setup – UPnP Interval (polling timer)**.

5.8 Quality of Service (QoS)

NEC SL2100 SIP trunks support Type of Service (ToS) (**Program 84-10 : ToS Setup**, protocol type = 9 (SIP Trunk)).

5.9 Registration

5.9.1 Registration Process

When the NEC SL2100 system registers its own IDs with an external SIP server, the following system data are sent:

Register ID #	User ID	Authentication ID	Authentication Password
Register ID 0	10-36-02	10-36-03	10-36-04
Register ID 1	10-36-02	10-36-03	10-36-04
:	10-36-02	10-36-03	10-36-04
:			
Register ID 31	10-36-02	10-36-03	10-36-04

The NEC SL2100 sends the REGISTER Message when the system starts up, register timer expires, CPU LAN links and recover timer expires.






5.9.2 Registration Recover Process

The NEC SL2100 has a registration recovery process for registration failure. When a registration fails, the NEC SL2100 sets an internal recover timer. When the timer expires, the NEC SL2100 sends a REGISTER message per register ID again.

The recover timer is either five minutes or 30 minutes. Typically, five minutes is used.


Section 6 SIP TRUNK PROGRAMMING

6.1 SIP Trunk Basic Setup

Program/ Item No.	Description/ Selection	Assigned Data	Comments
10-28-01	SIP System Information Set-up – Domain Name	64 characters maximum Default not assigned  <i>Select SIP Profile 1-6.</i>	Define the domain name. This information is generally provided by the SIP carrier.
10-28-02	SIP System Information Set-up – Host Name	48 characters maximum Default not assigned  <i>Select SIP Profile 1-6.</i>	Define the Host name. This information is generally provided by the SIP carrier.
10-28-03	SIP System Information Set-up – Transport Protocol	0 = UDP 1 = TCP 2 = TLS Default = 0  <i>Select SIP Profile 1-6.</i>	Define the Transport type. This option will always be set to UDP.
10-28-05	SIP System Information Set-up – Domain Assignment	0 = IP Address 1 = Domain Name Default = 0  <i>Select SIP Profile 1-6.</i>	Define the Domain Assignment. This entry is determined by what information the SIP carrier provides. If the SIP carrier provides a server name: SIPconnect-sca@L0.cbeyond.net the domain would be: @L0.cbeyond.net and the host name would be: SIPconnect-sca.
10-29-14	SIP Server Information Setup – SIP Carrier Choice	0 = Default 1 = Carrier A 2 = Carrier B 3 = Carrier C 4 = Carrier D 5 = Carrier E 6 = Carrier F 7 = Carrier G 8 = Carrier H 9 = Carrier I 10 = Carrier J 11 = Carrier K 12 = Carrier L 13 = Carrier M 14 = Carrier N 15 = Carrier O 16 = Carrier P 17 = Carrier Q 18 = Carrier R 19 = Carrier S 20 = Carrier T 21 = Carrier U 22 = Carrier V 23 = Carrier W 24 = Carrier X 25 = Carrier Y 26 = Carrier Z Default = 0  <i>Select SIP Profile 1-6.</i>	Define the SIP Carrier Choice.
10-68-01	IP Trunk Availability – Trunk Type	0 = None 1 = SIP 2 = H.323 3 = Reserved	Assign the trunk type as (1) SIP.

Program/Item No.	Description/Selection	Assigned Data	Comments
10-68-02	IP Trunk Availability – Start Port	0~128	Assign the Start Port for your SIP trunks.
10-68-03	IP Trunk Availability – Number of Port	0~128	Assign the number of SIP port trunks.
14-18-05	IP Trunk Data Setup – SIP Profile (SIP Only)	1 = Profile 1 2 = Profile 2 3 = Profile 3 4 = Profile 4 5 = Profile 5 6 = Profile 6 Default = 1	Define the SIP profile for each SIP trunk.
22-02-01	Incoming Call Trunk Setup	0 = Normal 1 = VRS (second dial tone if no VRS installed) 2 = DISA 3 = DID 4 = DIL 5 = Tie line 6 = Delayed VRS 7 = ANI/DNIS 8 = DID Mode Switching Default = 0	Define the SIP trunks as type 3 (DID). In addition to the SIP trunk programming, refer to the Direct Inward Dialing (DID) feature in the NEC SL2100 Features and Specifications Manuals and the NEC SL2100 Programming Manual for detailed information.


6.2 IP DSP Resource

 *If any IP Address or NIC settings are changed, the system must be reset for the changes to take affect.*



Program/Item No.	Description/Selection	Assigned Data	Comments
10-03-01	VoIPDB Configuration – Logical Port Number	0 ~ 128	The CPU-C1 automatically assigns each blade during installation. READ ONLY
10-03-02	VoIPDB Configuration – Trunk Type	0 = H.323 1 = SIP Default = 1	Assign each trunk type for each DSP Resource.
10-19-01	VoIP DSP Resource Selection –VoIP DSP Resource Selection	0 = Commonly used for both IP Extensions and Trunks 1 = Use for IP Extensions 2 = Use for SIP Trunks 5 = Blocked 6 = Common without Unicast Paging 7 = Multicast Paging 8 = Unicast Paging Default: Resource 1 = 1 Resources 2~128 = 0	Define the criteria for each DSP resource on the VoIP blade.
14-05-01	Trunk Group	Trunk Group = 0~50 Priority = 1 ~ 128 Default = Group1 for all trunk ports and priorities	Default priorities for trunks 1~128 is 1~128. Assign Trunks to Trunk Groups/ Outbound Priority
22-02-01	Incoming Call Trunk Setup	0 = Normal 1 = VRS (second dial tone if no VRS installed) 2 = DISA 3 = DID 4 = DIL 5 = Tie line 6 = Delayed VRS 7 = ANI/DNIS 8 = DID Mode Switching Default = 0	Set the feature type for the trunk you are programming. (Second dial tone for option 1 if no VRS is installed)












Program/Item No.	Description/Selection	Assigned Data	Comments
84-26-01	VoIP Basic Setup – IP Address	XXX.XXX.XXX.XXX	Assign the VOIPDB Gateway IP Address. 172.16.0.20
84-26-02	VoIP Basic Setup – RTP Port Number	0 ~ 65534	Default: 10020
84-26-03	VoIP Basic Setup – RTCP Port Number (RTP Port Number + 1)	1 ~ 65535	Default: 10021











6.3 SIP Caller ID












Program/Item No.	Description/Selection	Assigned Data	Comments
14-01-24	Basic Trunk Data Setup – Trunk-to-Trunk Outgoing Caller ID Through Mode	0 = Disable 1 = Enable Default = 0	Enable/Disable the Trunk-to-Trunk Outgoing Caller ID Through Mode. This option allows Caller ID from the original outside caller to be displayed when a trunk is forwarded off premise. This option can be used only with PRI and SIP trunks.
21-17-01	IP Trunk (SIP) Calling Party Number Setup for Trunk	1 ~ 0, *, # (to equal up to 16 digits) Default not assigned	This program assigns the Caller Party Number for each IP trunk. The assigned number is sent to the central office when the caller places an outgoing call. If the Calling Party Number is assigned by both 21-17 and 21-18/21-19, the system uses the entry in 21-18/21-19.
21-19-01	IP Trunk (SIP) Calling Party Number Setup for Extension	1 ~ 0, *, # (to equal up to 16 digits) Default not assigned  Select SIP Profile 1-6.	Assign the Calling Party Number for each extension. The assigned number is sent to the central office when the caller places an outgoing call. If the Calling Party Number is assigned by both Program 21-17 and 21-18/21-19, the system uses the data in Program 21-18/21-19.



6.4 SIP CODEC Trunk

Program/Item No.	Description/Selection	Assigned Data	Comments
84-13-01	SIP Trunk CODEC Information Basic Setup – G.711 Audio Frame Number	1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms Default is 2  Select SIP Profile 1-6.	Set the G.711 Audio Frame Number.
84-13-02	SIP Trunk CODEC Information Basic Setup – G.711 Voice Activity Detection Mode	0 = Disable 1 = Enable Default is 0  Select SIP Profile 1-6.	Enable/Disable the G.711 VAD Detection Mode.

Program/Item No.	Description/ Selection	Assigned Data	Comments
84-13-03	SIP Trunk CODEC Information Basic Setup – G.711 Type	0 = A-law 1 = μ -law Default is 1  Select SIP Profile 1-6.	Define the G.711 type.
84-13-04	SIP Trunk CODEC Information Basic Setup - G.711 Jitter Buffer (min)	0 ~ 255ms Default is 20  Select SIP Profile 1-6.	Set the minimum G.711 Jitter Buffer.
84-13-05	SIP Trunk CODEC Information Basic Setup – G.711 Jitter Buffer (average)	0 ~ 255ms 40ms = Default is 40  Select SIP Profile 1-6.	Set the average G.711 Jitter Buffer.
84-13-06	SIP Trunk CODEC Information Basic Setup – G.711 Jitter Buffer (max)	0 ~ 255ms Default is 80  Select SIP Profile 1-6.	Set the maximum G.711 Jitter Buffer.
84-13-07	SIP Trunk CODEC Information Basic Setup – G.729 Audio Frame Number	1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms 5 = 50ms 6 = 60ms Default is 2  Select SIP Profile 1-6.	Set the G.729 Audio Frame Number.
84-13-08	SIP Trunk CODEC Information Basic Setup – G.729 Voice Activity Detection Mode	0 = Disable 1 = Enable Default is 0  Select SIP Profile 1-6.	Enable/Disable the G.729 VAD Detection Mode.
84-13-09	SIP Trunk CODEC Information Basic Setup –G.729 Jitter Buffer (min)	0 ~ 300ms Default is 20  Select SIP Profile 1-6.	Set the minimum G.729 Jitter Buffer.
84-13-10	SIP Trunk CODEC Information Basic Setup – G.729 Jitter Buffer (average)	0 ~ 300ms Default is 40  Select SIP Profile 1-6.	Set the average G.729 Jitter Buffer.
84-13-11	SIP Trunk CODEC Information Basic Setup – G.729 Jitter Buffer (max)	0 ~ 300ms Default is 80  Select SIP Profile 1-6.	Set the maximum G.729 Jitter Buffer.
84-13-17	SIP Trunk CODEC Information Basic Setup – Jitter Buffer Mode	1 = Static 3 = Self adjusting Default is 3  Select SIP Profile 1-6.	Set the Jitter Buffer Mode.
84-13-18	SIP Trunk CODEC Information Basic Setup – VAD Threshold	Entries 0 ~ 30 (-20dBm~10dBm) 1 = -19dB (-49dBm) : 20 = 0dB (-30dBm) : 29 = 9dB (-21dBm) 30 =10dB (-20dBm) Default is 20  Select SIP Profile 1-6.	Set the VAD (voice activity detection) threshold.

Program/Item No.	Description/ Selection	Assigned Data	Comments
84-13-28	SIP Trunk CODEC Information Basic Setup – Audio Capability Priority	0 = G.711_PT 1 = Not Used 2 = G.729_PT 3 = G.722 4 = G.726 5 = Not Used 6 = G.711 Only 7 = G.729 Only Default is 0  Select SIP Profile 1-6.	Define the CODEC Priority.
84-13-33	SIP Trunk CODEC Information Basic Setup – Number of G.722 Audio Frames	1~4 1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms Default is 3  Select SIP Profile 1-6.	
84-13-35	SIP Trunk CODEC Information Basic Setup – G.722 Jitter Buffer (min)	0~300ms Default is 30  Select SIP Profile 1-6.	
84-13-36	G.722 Jitter Buffer (average)	0~300ms Default is 60  Select SIP Profile 1-6.	
84-13-37	G.722 Jitter Buffer (max)	0~300ms Default is 120  Select SIP Profile 1-6.	
84-13-38	Number of G.726 Audio Frames	1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms Default is 3  Select SIP Profile 1-6.	
84-13-39	G.726 VAD Mode	0 = Disable 1 = Enable Default is 0  Select SIP Profile 1-6.	
84-13-40	G.726 Jitter Buffer (min)	0~300ms Default is 30  Select SIP Profile 1-6.	
84-13-41	G.726 Jitter Buffer (average)	0~300ms Default is 60  Select SIP Profile 1-6.	
84-13-42	G.726 Jitter Buffer (max)	0~300ms Default is 120  Select SIP Profile 1-6.	

Program/Item No.	Description/ Selection	Assigned Data	Comments
84-13-49	RTP Filter	0 = Disable 1 = IP 2 = IP + SSRC Default is 1  Select SIP Profile 1-6.	Set the FAX Relay Mode.
84-33-01	FAX Relay Mode	0 = Disable 1 = Enable 2 = Each Port Mode Default is 0  Select SIP Profile 1-6.	
84-33-02	T.38 Protocol mode	0 = R/U 1 = U/R 2 = RTP 3 = UDPTL Default is 1  Select SIP Profile 1-6.	
84-33-05	T.38 RTP Format Payload Number	96 ~ 127 Default is 100  Select SIP Profile 1-6.	
84-33-06	T.38 FAX Max Speed	0 = V.27ter: 4800 bps 1 = V.29: 9600 bps 2 = V.17: 14400 bps Default is 2  Select SIP Profile 1-6.	
84-33-08	T.38 Error protection depth for Signaling	0 ~ 2 Default is 0  Select SIP Profile 1-6.	
84-33-09	T.38 Error protection depth for Data	0 ~ 2 Default is 0  Select SIP Profile 1-6.	
84-33-10	T.38 TCF Method	1 = VOIPDB 2 = G3FE Default is 1  Select SIP Profile 1-6.	
84-13-65	VAD Negotiation on SDP	0 = Disable 1 = Enable Default is 0  Select SIP Profile 1-6.	
84-13-66	Voice Band Data (VBD)	0 = Disable 1 = Enable Default is 0  Select SIP Profile 1-6.	
84-13-67	VBD Payload Type	96 ~ 127 Default is 97  Select SIP Profile 1-6.	

Program/Item No.	Description/ Selection	Assigned Data	Comments
84-34-01	DTMF Relay Mode	0 = Disable 1 = RFC2833 2 = H.245 Default is 0  Select SIP Profile 1-6.	
84-34-02	DTMF Payload Number	96 ~ 127 Default is 110  Select SIP Profile 1-6.	


6.5 SIP NAPT Router Setup







Program/Item No.	Description/ Selection	Assigned Data	Comments
10-12-07	CPU Network Setup – NAPT Router IP Address	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.254.255.254 192.0.0.1 ~ 223.255.255.254 Default is 0.0.0.0	Set the NAPT Router IP address. With SIP trunking, the IP address of the WAN side of the router must be entered.
10-12-08	CPU Network Setup – ICMP Redirect	0 = Disable 1 = Enable Default is 0	Enable/Disable ICMP (Internet Control Message Protocol) Redirect.

6.6 SIP System Interconnection Setup



Program/Item No.	Description/ Selection	Assigned Data	Comments
10-23-01	SIP System Interconnection Setup – System Interconnection	0 = Disable 1 = Enable Default is 0	Enable/Disable system interconnection.
10-23-02	SIP System Interconnection Setup – IP Address	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254 Default is 0.0.0.0	Define the IP address of another system.
10-23-04	SIP System Interconnection Setup – Dial Number	Up to 12 digits (0 ~ 9) Default not assigned	Determine another system call control port number.





6.7 SIP Protocol

Program/Item No.	Description/ Selection	Assigned Data	Comments
84-14-06	SIP Trunk Basic Information Setup – SIP Trunk Port Number	1 ~ 65535 Default is 5060 = Profile 1 5062 = Profile 2 5090 = Profile 3 5092 = Profile 4 5094 = Profile 5 5096 = Profile 6  Select SIP Profile 1-6.	Set the SIP UA (User Authorized) Trunk port number (Receiving Transport for NEC SL2100 SIP).







Program/Item No.	Description/ Selection	Assigned Data	Comments
84-14-07	SIP Trunk Basic Information Setup – Session Timer Value	0 ~ 65535 seconds Default is 0  Select SIP Profile 1-6.	Set the Session Timer Value. 0 means session timer is Off
84-14-08	SIP Trunk Basic Information Setup – Minimum Session Timer Value	0 ~ 65535 seconds Default is 1800  Select SIP Profile 1-6.	Set the Minimum Session Timer Value.
84-14-09	SIP Trunk Basic Information Setup – Called Party Information	0 = Request URI 1 = To Header Default is 0  Select SIP Profile 1-6.	Set the Called Party Information.
84-14-10	SIP Trunk Basic Information Setup – URL Type	0 = SIP-URL 1 = TEL-URL Default is 0  Select SIP Profile 1-6.	
84-14-11	SIP Trunk Basic Information Setup – URL/To Header Setting Information	0 = Proxy Server Domain 1 = SIP UA Domain Default is 0  Select SIP Profile 1-6.	
84-14-15	SIP Trunk Basic Information Setup – 100rel Settings	0 = Use Default Settings (100rel included) 1 = Use Opposite Settings (100rel not included) Default is 0  Select SIP Profile 1-6.	


6.8 SIP Server Information Setup

Program/Item No.	Description/ Selection	Assigned Data	Comments
10-29-01	SIP Server Information Setup – Default Proxy (Outbound)	0 = Off 1 = On Default is 0  Select SIP Profile 1-6.	Define the SIP Proxy setup, Default Proxy (Outbound). When SIP trunking is used, this must be on. If entries are made in Program 10-29-xx for a SIP Server and the SIP Server is then removed or not used, the entries in Program 10-29-xx must be set back to their default settings. Even if 10-29-01 is set to 0, the NEC SL2100 still checks the settings in the remaining 10-29 programs.
10-29-02	SIP Server Information Setup – Default Proxy (Inbound)	0 = Off 1 = On Default is 0  Select SIP Profile 1-6.	Define the Default Proxy (inbound).

Program/Item No.	Description/ Selection	Assigned Data	Comments
10-29-03	SIP Server Information Setup – Default Proxy IP Address	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.225.255.254 Default is 0.0.0.0  Select SIP Profile 1-6.	Enter the default Proxy IP Address if the SIP carrier is using an IP Address for the Proxy. In most cases, this is left at the default entry as the domain name is used.
10-29-04	SIP Server Information Setup – Default Proxy Port Number	0 ~ 65535 Default is 5060  Select SIP Profile 1-6.	Define the Proxy Port Number.
10-29-12	SIP Server Information Setup – Proxy Domain Name	64 characters maximum Default not assigned  Select SIP Profile 1-6.	Define the Proxy Domain Name (NEC SL2100 domain name).
10-29-13	SIP Server Information Setup – Proxy Host Name	48 characters maximum Default not assigned  Select SIP Profile 1-6.	Define the Proxy Host name (NEC SL2100 proxy name).

6.9 SIP Registrar Setup





Program/Item No.	Description/ Selection	Assigned Data	Comments
10-29-05	SIP Server Information Setup – Registrar Mode	0 = None 1 = Manual Default is 0  Select SIP Profile 1-6.	Define the Registrar Mode. This should always be set to manual when using SIP trunking.
10-29-06	SIP Server Information Setup – Registrar IP Address	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254 Default is 0.0.0.0  Select SIP Profile 1-6.	Define the Registrar IP Address. The carrier may provide an IP address. In most cases, a domain name will be used so this entry will be left at the default.
10-29-07	SIP Server Information Setup – Registrar Port Number	0 ~ 65535 Default is 5060  Select SIP Profile 1-6.	Define the Registrar Port Numbers.
10-29-11	SIP Server Information Setup – Registrar Domain Name	128 characters maximum Default not assigned  Select SIP Profile 1-6.	Define the Registrar Domain Name (normally provided by the SIP carrier). Example: SIPconnect-sca@L0.cbeyond.net
10-29-15	SIP Server Information Setup – Registration Expiry (Expire) Time	120 ~ 65535 seconds Default is 3600  Select SIP Profile 1-6.	Define the Registration Expire time – the time allowed to register with the SIP carrier. This should stay at the default entry.
10-29-20	Authentication Trial	0 ~ 9 0 = No Authentication Default is 1 (1 Authentication Attempt)  Select SIP Profile 1-6.	

Program/Item No.	Description/ Selection	Assigned Data	Comments
10-29-21	NAT Router	0 = Disabled 1 = Enabled Default is 0  Select SIP Profile 1-6.	

6.10 SIP Server Status

Program/Item No.	Description/ Selection	Assigned Data	Comments
90-10-01	System Alarm Setup – Alarm Type	Alarm 14 - CPU-LAN Link Error (IP Layer 1) Assign a Major or Minor alarm status for the LAN link. This program also assigns whether or not the alarm is displayed to a key telephone and whether or not the alarm information is reported to the predefined destination. Alarm 60 - SIP Registration Error Notification Assign a Major or Minor alarm status for the SIP Registration Error. This program also assigns whether or not the alarm information is reported to the predefined destination.	Define alarms 14 and 60.

6.11 SIP Trunk Registration Information Setup

Program/Item No.	Description/ Selection	Assigned Data	Comments
10-36-01	SIP Trunk Registration Information Setup – Registration	0 = Disable 1 = Enable Default is 0  Select SIP Profile 1-6.	Enable/Disable the SIP trunk registration.
10-36-02	SIP Trunk Registration Information Setup – User ID	32 characters maximum Default not assigned  Select SIP Profile 1-6.	Define the user ID.
10-36-03	SIP Trunk Registration Information Setup – Authentication User ID	64 characters maximum Default not assigned  Select SIP Profile 1-6.	Define the authentication user ID.
10-36-04	SIP Trunk Registration Information Setup – Authentication Password	32 characters maximum Default not assigned  Select SIP Profile 1-6.	Define the authentication password.

6.12 SIP UPnP

Program/Item No.	Description/ Selection	Assigned Data	Comments
10-37-01	UPnP Setup – UPnP Mode	0 = Disable 1 = Enable Default is 0	Determine whether UPnP (Universal Plug and Play) task starts. If UPnP task starts, it obtains a NAPT router WAN IP Address by using NAT traversal and saves it in Program 10-12-07 automatically.
10-37-02	UPnP Setup – Retry Time	0~3600 1~59 cannot be used. Default is 60	UPnP (Universal Plug and Play) task tries to obtain the WAN IP Address of the NAPT router at the interval defined in this option.

Section 7 SIP TRUNK E.164 SUPPORT

7.1 Description

With SIP Trunk E.164 Support enabled, the PBX is able to support SIP configurations where the number presentation within the SIP messages is formatted using the E.164 international numbering scheme. Specifically the system is able to handle the + digit when required as the International Access Code.

For example, a normal international SIP call can be dialed and displayed as follows:

Number dialed = 00441202223344

Request-URI: Invite sip: 00441202223344@172.16.18.100 SIP/2.0

With SIP Trunk E.164 Support enabled, the SIP call can be displayed once dialed as:

Request-URI: Invite sip:+441202223344@172.16.18.100 SIP/2.0

This display is a requirement of certain SIP ITSPs (Internet Telephony Service Providers) and may require that PBX handle these calls and modify any SIP messages to the correct format accordingly.

This feature uses the following SIP header fields:

To

From

P-Asserted Identity

P-Preferred

Identity

7.1.1 Condition

- E.164 support is applied on the SIP trunk interface.
- E.164 is supported for all carrier choices (Program 10-29-14).
- Netlink multi-carrier support uses E.164 support across all carrier configurations at the secondary nodes.

7.1.2 Default Settings

Disabled

7.2 System Availability

7.2.1 Terminals

All Multiline Terminals

7.2.2 Trunks

IP SIP

7.2.3 Required Component(s)

IP7()-CPU-C1

IP7WW-VoIPDB-C1

SL2100 IP CHANNEL-16 LIC






SL2100 IP TRUNK-01 LIC

7.3 Programming

Program Number	Program Name/Description	Input Data	Assigned Data	Level		
				1	2	3
10-02-01	Location Setup – Country Code Enter the country code.	Dial (maximum of four digits) 0 ~ 9, *, #	1	✓		
10-02-02	Location Setup – International Access Codes Enter the international access code.	Dial (maximum of four digits) 0 ~ 9, *, #	No Setting	✓		
44-01-02	System Options for ARS/F-Route – Dial Tone Simulation Dial digits to be analyzed by the system. Numbering plan for the dial needs to be configured as F-Route in Program 11-01.	Dial (maximum of one digit) 0 ~ 9, *, # cannot be used Profile (1 ~ 6)	No Setting	✓		
44-01-03	System Options for ARS/F-Route – Tone Type Set simulated DT to type which can change the tone used in Program 44-01-02 and Program 44-02-04.	0 = Internal Dial Tone 1 = External Dial Tone	0	✓		
84-14-13	SIP Trunk Basic Information Setup – Incoming/ Outgoing SIP Trunk for E.164 When this data is set to 1, then for any outbound SIP calls a + is added as a prefix to the Request-URI, To and From header fields of the SIP message. When it is set to 2 then if the dialed international access code matches the value in Program 10-02-02 this value is removed from the number dialed and the + added as a prefix to the Request-URI, To and From header fields of the SIP Message.	0 = Off 1 = Mode 1 2 = Mode 2 3 = Mode 3 Profile (1 ~ 6)	0	✓		

7.4 Operation

7.4.1 To Transfer a Call into a Conference:

1. While on a call, press **Hold** key.
2. Dial the Transfer to Conference service code (**PRG 11-12-58**, default = **624**).
 -  *If the telephone does not have the proper COS, a warning tone is sent. After the user hangs up, the system automatically places a Callback to the extension.*
 -  *The display shows the line Number, Number/Name and Extension Name/Number.*
3. Dial the extension number or press a **DSS** key of a telephone in a Conference call.
 -  *If an error tone is heard, Barge-In is disable for the extension and the call cannot go through. Retrieve the call by pressing the flashing line Key or hang up and the call recalls the extension.*
 -  *When the call is transferred into the Conference, an intrusion tone is heard by all parties in the conference, depending on the entries in PRG 20-13-17 and PRG 80-01, and all display Multiline Terminals show the joined party.*
 -  *To cancel the transfer, press the flashing line Key to retrieve the call.*
4. Hang up.

Section 8 SIP TRUNK E.164 CLIP ENHANCEMENT

8.1 Description

With SIP Trunk E.164 Support enabled, the PBX is able to support SIP configurations where the number presentation within the SIP messages is formatted using the E.164 international numbering scheme. Specifically the system is able to handle the + digit when required as the International Access Code.

For example, a normal international SIP call can be dialed and displayed as follows:

Number dialed = 00441202223344

Request-URI: Invite sip: 00441202223344@172.16.18.100 SIP/2.0

With SIP Trunk E.164 Support enabled, the SIP call can be displayed once dialed as:

Request-URI: Invite sip:+441202223344@172.16.18.100 SIP/2.0

This display is a requirement of certain SIP ITSPs (Internet Telephony Service Providers) and may require that PBX handle these calls and modify any SIP messages to the correct format accordingly.

This feature uses the following SIP header fields:

To

From

P-Asserted Identity

P-Preferred

Identity

8.1.1 Condition

- E.164 support is applied on the SIP trunk interface.

- E.164 is supported for all carrier choices (Program 10-29-14).
- Netlink multi-carrier support uses E.164 support across all carrier configurations at the secondary nodes.

8.1.2 Default Settings

Disabled

8.2 System Availability

8.2.1 Terminals

All Multiline Terminals

8.2.2 Trunks

IP SIP

8.2.3 Required Component(s)

IP7()-CPU-C1

IP7WW-VoIPDB-C1

SL2100 IP CHANNEL-16 LIC

SL2100 IP TRUNK-01 LIC

8.3 Programming

Program Number	Program Name/Description	Input Data	Assigned Data	Level		
				1	2	3
10-02-01	Location Setup – Country Code Enter the country code.	Dial (maximum of four digits) 0 ~ 9, *, #	1	✓		
10-02-02	Location Setup – International Access Codes Enter the international access code.	Dial (maximum of four digits) 0 ~ 9, *, #	No Setting	✓		
10-02-03	Location Setup – Other Area Access Code Enter the other area access code.	Dial (maximum of four digits) 0 ~ 9, *, #	9			
84-14-13	SIP Trunk Basic Information Setup – Incoming/ Outgoing SIP Trunk for E.164 When this data is set to 1, then for any outbound SIP calls a + is added as a prefix to the Request-URI, To and From header fields of the SIP message. When it is set to 2 then if the dialed international access code matches the value in Program 10-02-02 this value is removed from the number dialed and the + added as a prefix to the Request-URI, To and From header fields of the SIP Message.	0 = Off 1 = Mode 1 2 = Mode 2 3 = Mode 3 Profile (1 ~ 6)	0	✓		

Program Number	Program Name/Description	Input Data	Assigned Data	Level		
				1	2	3
84-14-16	<p>SIP Trunk Basic Information Setup – SIP Trunk SIP-URI E.164 Incoming Mode</p> <p>When this data is set to 1, then for any inbound SIP calls that include a + and a country code not defined in Program 10-02-01, delete the + and add the International Access Code in Program 10-02-02. If the country code is a match then delete both the + and country code but do not add the International Access code.</p> <p>When it is set to 2, then for any inbound SIP calls that include a + and a country code not defined in Program 10-02-01, delete the + and add the International Access Code in Program 10-02-02. If the country code is a match then delete both the + and country code and add the Caller ID Edit Code from Program 10-02-03.</p>	<p>0 = Disable 1 = Mode 1 2 = Mode 2 Profile (1 ~ 6)</p>	0	✓		

8.4 Operation

8.4.1 Delete the + only from an incoming SIP INVITE using E.164 numbering scheme:

Table 7-1 Delete + from Incoming SIP INVITE

Program 84-14-16	Program 84-14-13	Description
0: Off	0: Off Or 1: On	When a + is presented as the international access code in a SIP INVITE for incoming calls then delete the + only.

<Example Output>

Incoming call from: +4902131795770

Displayed in terminal incoming caller history as:

01:	4902131795770
*	3-5 11:17
↑	↓ Store DEL

Original

8.4.2 Delete and replace the + and matched country code from an incoming SIP INVITE using E.164 numbering scheme:

Table 7-2 Delete + and Country Code from Incoming SIP INVITE

Program 84-14-16	Program 84-14-13	Description
1: Mode 1	1: On	With a SIP INVITE for incoming calls. When a + is presented as the international access code along with a country code that DOES NOT match the value in Program 10-02-01, then delete the + and add the international access code value in Program 10-02-02 only. - Or - With a SIP INVITE for incoming calls. When a + is presented as the international access code along with a country code that DOES match the value in Program 10-02-01, then delete the + and country code but DO NOT add the international access code value.

<Example Output>

Incoming call from: +4902131795770

Program 10-02-02 = 00

Displayed in terminal incoming caller history as:

01:	4902131795770
*	3-5 11:17
↑	↓ Store DEL

Original

01:	004902131795770
*	3-5 11:17
↑	↓ Store DEL

Program 10-02-01 = 0

01:	02131795770
*	3-5 11:17
↑	↓ Store DEL

Program 10-02-01 = 49

Table 7-3 Delete + and Country Code from Incoming SIP INVITE

Program 84-14-16	Program 84-14-13	Description
2: Mode 2	1: On	With a SIP INVITE for incoming calls. When a + is presented as the international access code along with a country code that DOES NOT match the value in Program 10-02-01, then delete the + and add the international access code value in Program 10-02-02 only. - Or - With a SIP INVITE for incoming calls. When a + is presented as the international access code along with a country code that DOES match the value in Program 10-02-01, then delete the + and country code but DO NOT add the international access code value.

<Example Output>

Incoming call from: +4902131795770

Program 10-02-02 = 00

Program 10-02-03 = 9

Displayed in terminal incoming caller history as:

01:	4902131795770
*	3-5 11:17
↑	↓ Store DEL

Original

01:	004902131795770
*	3-5 11:17
↑	↓ Store DEL

Program 10-02-01 = 0

01:	902131795770
*	3-5 11:17
↑	↓ Store DEL

Program 10-02-01 = 49

8.4.3 Making an outgoing call from history of incoming calls:

1. From an idle multiline terminal.
2. Press soft key List.

3. Press soft key CID.
4. Press Speaker.

Section 9 SIP TRUNK KEEP ALIVE USING OPTION MESSAGE

9.1 Description

The SL2100 provides support for “SIP Trunk Keep Alive” using OPTION message for all six SIP Profiles, applicable to both IP System Interconnection and SIP Carrier mode.

9.1.1 Condition

- OPTION Keep Alive works for all SIP Carrier Type (PRG 10-29-14).
- Program 10-29-19 must be enabled for making OPTION Keep Alive to work for SIP Carrier mode.
- Program 10-23-05 must be enabled for making OPTION keep alive to work for IP system Interconnection mode.
- SL2100 sends the OPTION message at the interval of the value set in program 84-14-18.
- OPTION Keep Alive can be sent to the SIP carrier or IP system Interconnection of Net Link Secondary System.
- OPTION Keep Alive Call Restriction and Alarm of Net Link Secondary System are not supported.
- If SL2100 does not receive the 200-OK response from the SIP server then SL2100 would retry sending of OPTION message for 32 seconds.

9.1.2 Default Settings

None

9.2 System Availability

9.2.1 Terminals

None

9.2.2 Trunks

SIP Trunks

9.2.3 Required Component(s)

IP7WW-VoIPDB-C1

SL2100 IP CHANNEL-16 LIC

SL2100 IP TRUNK-01 LIC

9.3 Programming

Program Number	Program Name/Description	Input Data	Default
10-23-05	SIP System Interconnection Setup – Keep Alive Mode for SIP Enable/Disable OPTION Keep Alive Mode for IP system interconnection.	0 = Disable 1 = Option Keep Alive Mode	0
10-23-06	SIP System Interconnection Setup – SIP Profile Assign the Interconnection to a SIP Profile.	1 = Profile 1 2 = Profile 2 3 = Profile 3 4 = Profile 4 5 = Profile 5 6 = Profile 6	1
10-29-19	SIP Server Information Setup – Keep Alive by OPTION Message Enable/Disable support of keep alive by OPTION Message for SIP carrier mode.	0 = Disable 1 = Enable Profile (1 ~ 6)	0
84-14-18	SIP Trunk Basic Information Setup - Keep Alive by OPTION Interval Timer Define Keep Alive by OPTION Interval Timer. SL2100 sends the OPTION message at the interval of the value set in this program.	60 ~ 3600 (seconds) Profile (1 ~ 6)	180
84-14-19	SIP Trunk Basic Information Setup - Keep Alive by OPTION Fail Limit Define Keep Alive by OPTION fail limit.	1 ~ 5 Profile (1~6)	1
84-14-20	SIP Trunk Basic Information Setup - Option Keep Alive User ID Define Option Keep Alive User ID which is set in SIP URL of OPTION message.	Max. 32 String Profile (1 ~ 6)	ping

9.4 Operation

None

DHCP Client

Section 1 DHCP CLIENT

Warning: When the VoIPDB is installed on the CPU, the built-in LAN port on the CPU becomes disabled. Only the LAN port on the VoIPDB is operational.

DHCP client function is applicable to the CPU LAN port only. This function is enabled by default. If VoIPDB is installed then CPU LAN port will be disabled and DHCP client function will not be used even if it is enabled.

The system can receive the following information from the DHCP server: IP Address, Subnet Mask, and Default Gateway.

1.1 Conditions

- DHCP client function only applies to the CPU LAN port and is applicable only when VoIPDB is not installed.
- The CPU LAN port will receive the IP address information from DHCP server without having to reboot.
- PRG 10-12-13 and PRG 10-12-14 are not populated by DHCP assignment.
- It is mandatory to disable PRG 10-63-01 to change PRG 10-12-01 and PRG 10-12-02 manually.
- It is mandatory logout from WebPro after applying changes so as to write those changes.
- The DHCP Server should be configured to provide the system the same IP address every time. For example in the DHCP server extend the lease time to infinite or setup the server to provide the same IP address based on the systems MAC Address.
- DHCP client can set following programs automatically; however other IP related programs (such as PRG 84-26) have to set manually as required.
 - IP Addresses: PRG 10-12-01 (CPU)
 - Subnet Masks: PRG 10-12-02 (CPU)
 - Default Gateway: PRG 10-12-03
- DHCP Client (PRG 10-63) and existing DHCP Server feature (PRG 10-13) can not be used at the same time.

1.2 Default Settings

Enabled

1.3 System Availability

1.3.1 Required Component(s)

IP7[]-CPU-C1

IP7WW-VOIPDB-

C1

1.4 Guide to Feature Programming

Program Number	Program Name	Description/Comments	Assigned Data	Level		
				1	2	3
10-63-01	DHCP Client Setting - DHCP Client Mode	Enable/disable the DHCP Client feature.	0 = Disable 1 = Enable (default = 1)	✓		
10-12-01	CPU Network Setup - IP Address	Assigns the IP address of the CPU card.	192.168.0.10	✓		
10-12-02	CPU Network Setup - Subnet Mask	Assigns the Subnet Mask of the CPU card.	255.255.255.0	✓		
10-12-03	CPU Network Setup – Default Gateway	Assign the default gateway IP address for the CPU.	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254 (default = 0.0.0.0)	✓		
10-12-09	CPU Network Setup – VoIP IP Address	Set for VoIPDB.	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254 (default = 172.16.0.10)	✓		
10-12-10	CPU Network Setup – Subnet Mask-VoIPDB	Define the Media Gateway Subnet Mask Address.	128.0.0.0 192.0.0.0 224.0.0.0 240.0.0.0 248.0.0.0 252.0.0.0 254.0.0.0 255.0.0.0 255.128.0.0 255.192.0.0 255.224.0.0 255.240.0.0 255.248.0.0 255.252.0.0 255.254.0.0 255.255.0.0 255.255.128.0 255.255.192.0 255.255.224.0 255.255.240.0 255.255.248.0 255.255.252.0 255.255.254.0 255.255.255.0 255.255.255.128 255.255.255.192 255.255.255.224 255.255.255.240 255.255.255.248 255.255.255.252 255.255.255.254 255.255.255.255 (default = 255.255.0.0)	✓		

Section 2 DHCP SERVER CONFIGURATION EXAMPLE

The example below shows the necessary steps to add options to a Windows server so that the server will provide the IP Address of the SL2100 (PRG 10-12-09).

1. In the DHCP Server, right click on the actual server and select **Set Predefined Options**.

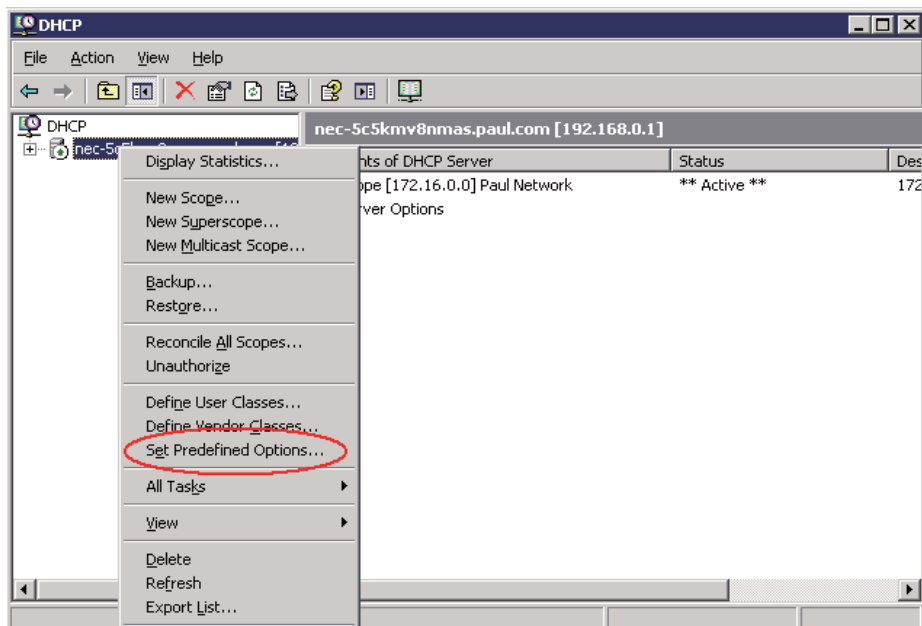
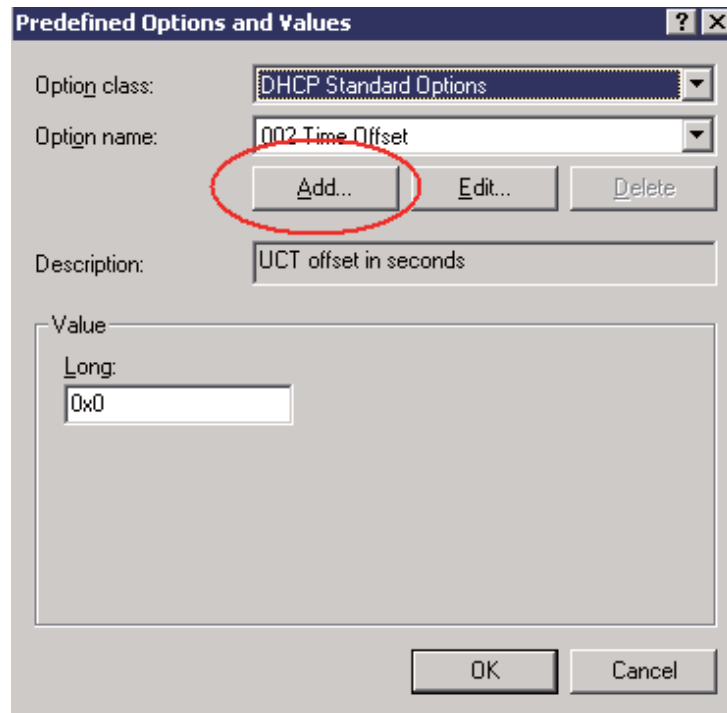


Figure 8-1 DHCP - Set Predefined Options

2. After clicking Set Predefined Options, a new window pops up. Select **Add** to create the new entry for the SL2100 system. Once the option type window is available, assign the following information:
 - Name = SIP Server
 - Data Type = Binary
 - Code = 120
 - Description = Any description you would like to enter



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 002 Time Offset

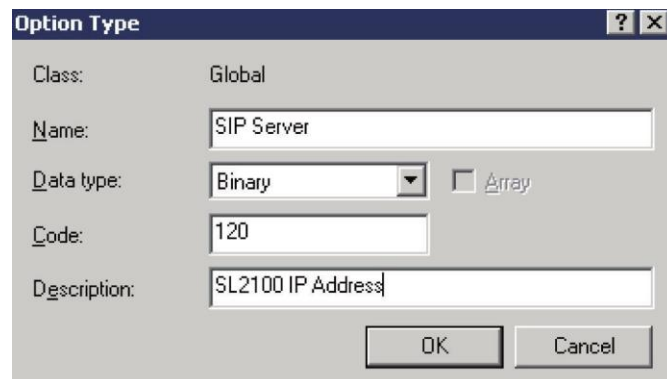
Add... Edit... Delete

Description: UCT offset in seconds

Value

Long: 0x0

OK Cancel



Option Type

Class: Global

Name: SIP Server

Data type: Binary Array

Code: 120

Description: SL2100 IP Address

OK Cancel

Figure 8-2 DHCP - Predefined Options and Values

- In the DHCP server, select the scope of options for the DHCP scope that is being configured. Right click on the **Scope Options**, and select **Configure Options**.

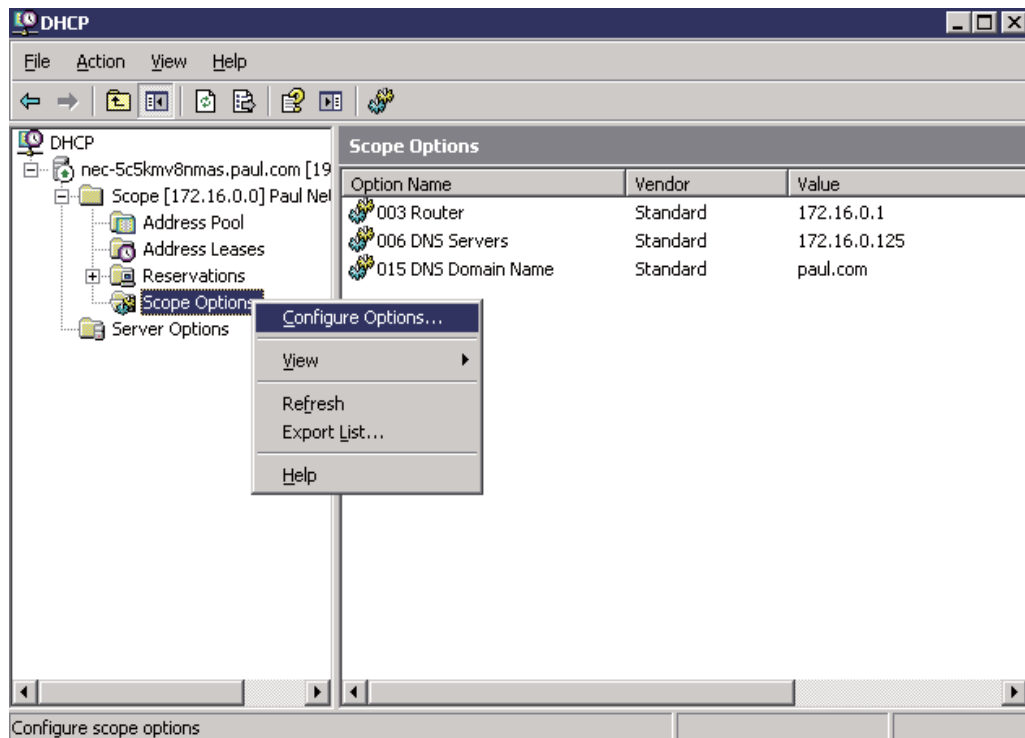


Figure 8-3 DHCP - Scope Options

- In the Scope Options window, scroll down and place a check mark next to 120 SIP Server. Once the server is added, the data field needs to be changed. In the Data Entry default delete the

default value 00 and add the IP address of the SL2100 system as a Hex value preceded by a 01, for the first SIP server. Listed is an example of what data is to be entered:

- 01 = 1st SIP Server
- AC = Hex for 172
- 10 = Hex for 16
- 00 = Hex for 0
- 0A = Hex for 10

This tells the system that the first SIP server's IP address is: 172.16.0.10. Once assigned, click on **Apply** to update the DHCP server.

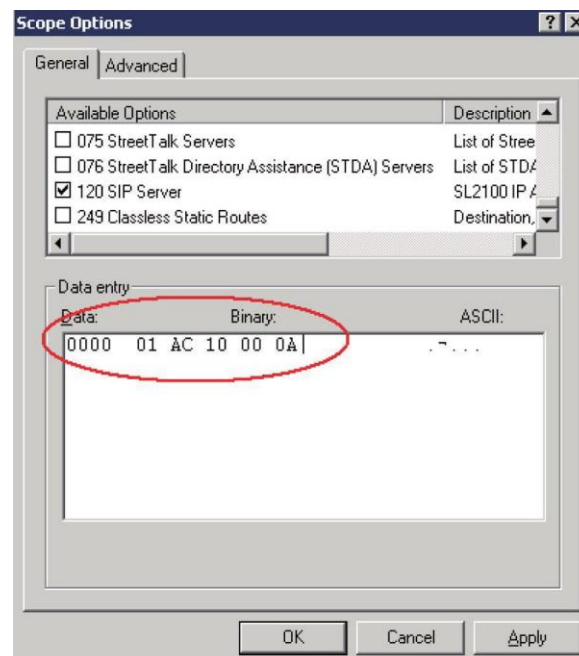
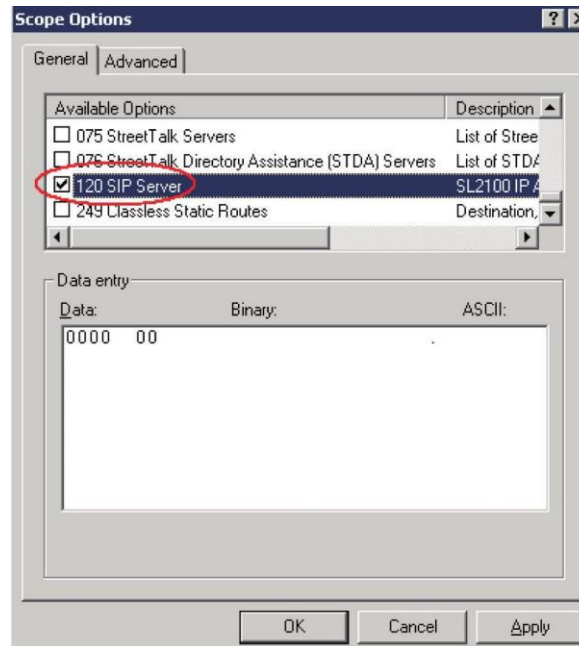


Figure 8-4 DHCP - Data Entry for 1st DHCP Server


IP Multiline Station (SIP)

Section 1 INTRODUCTION

The NEC SL2100 system supports IP extensions. These telephones have the same look and functionality as typical multiline telephones, but they are connected to the CPU via IP rather than by a hardwired connection to a station card.

The following terminal is supported.

- IP7WW-8IPLD-C1 TEL
- ITK-8LCX-1(BK)TEL

 *The voice quality of VoIP is dependent on variables such as available bandwidth, network latency and Quality of Service (QoS) initiatives, all of which are controlled by the network and Internet Service Providers. Because these variables are not in NEC control, it cannot guarantee the performance of the user's IP-based remote voice solution. Therefore, NEC recommends connecting VoIP equipment through a local area network using a Private IP address.*

Section 2 IP TO TDM CONVERSION

When an IP telephone calls a []TXH-B1 multiline telephone, single line telephone or trunk, the speech must be converted from IP to TDM (Time Division Multiplexing) technology. The VoIPDB daughter board provides this function.

It is possible for 8IPLD/DT900 IP Phones to talk directly to other 8IPLD/DT900 IP Phones without using a VoIP DSP resource. For more information, refer to [Peer-to-Peer](#).

2.1 8IPLD/DT900 IP Multiline Telephones

The IP multiline telephone operates in the same way as a digital multiline telephone. It has all features and flexibility you expect from a digital multiline telephone. The difference is that the IP telephone has an RJ-45 for connection to an IP network, rather than an RJ-11 for connection to a digital extension port.



Figure 9-1 8IPLD Telephone

2.2 Conditions

When using 8IPLD/DT900 IP phones, it is not recommended to assign the following features to a large number of phones (16 or more):

- The same Trunk Line assignment (squared key system)
- The same Virtual Extension assignment
- Paging key with LED ON assignment
- The same location Park key
- The same BLF key assignment
- Day Night Mode Change key assignment
- The same VM Mail Box key assignment
- Trunk Group key
- Trunk Group All Line Busy Indication
- One call cannot ring more than 8 simultaneous IP extensions at the same time if the call originates from a ring group or a virtual.

2.3 LAN Connection

As illustrated in [Figure 9-2 Typical Network IP Connection](#), the IP telephone has two RJ-45 connections on the back side marked PC and LAN. This allows the IP telephone and a PC to share one cable run and switch/hub port.

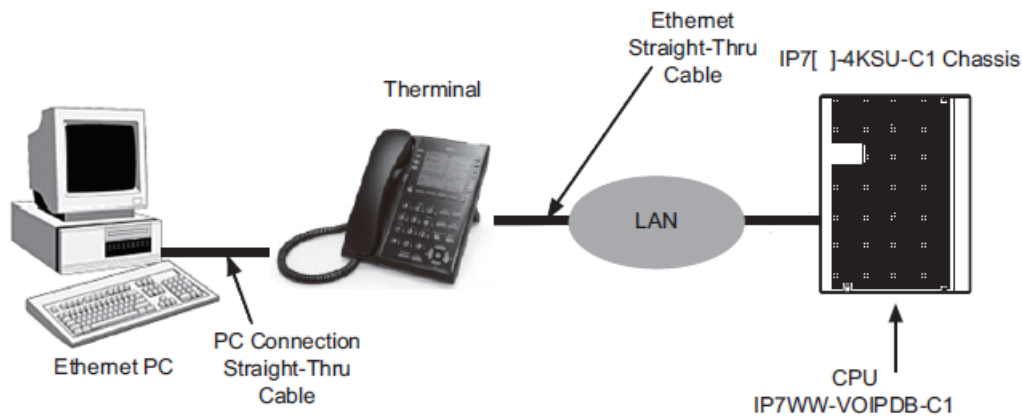


Figure 9-2 Typical Network IP Connection

If installing an IP telephone at a location that already has a PC connected to the data network, it is possible to use either of the following methods:

- Use a different cable and complete the following steps:
 - Leave the PC connected to the LAN.
 - Patch a switch port to a new cable run.
 - Connect a CAT 5 straight-through cable from the wall outlet to the LAN port on the IP telephone.
- Share the existing cable and complete the following steps:
 - Unplug the cable from the PC network card (NIC).
 - Connect that cable to the LAN port on the IP telephone.
 - Connect a new straight-through patch lead from the PC NIC to the PC port on the IP telephone.

Section 3 PROVIDING POWER

IP telephones require power to function. This can be provided by PoE only.

3.1 Power Over Ethernet (PoE)

A PoE switch provides power over the spare pairs. The switch can be used with any device (not just IP phones) and detects whether or not power is required. As all phones receive their power from one device, it is easy to protect the IP phones from loss of power (by connecting the PoE switch to a UPS).

Section 4 PEER-TO-PEER

An IP telephone can send and receive RTP packets to or from another IP telephone without using DSP resources on a VoIPDB. This operation supports only Intercom calls between the IP telephones.

If a 8IPLD/DT900 IP multiline telephone or trunk line is required, a DSP resource is needed and a VoIPDB must be installed. If a conference call is initiated while on a peer-to-peer call, the peer-to-peer connection is released and a new non peer-to-peer connection is created using the VoIPDB. If the third party drops out of the conversation, the call reverts to a peer-to-peer call. There is silence while this conversion is made by the system.

Although the peer-to-peer feature is supported for IP Station-to-IP Station calls, the NEC SL2100 Chassis must still have a registered VoIPDB installed in the system.

With Barge-In, a short silence may occur if the following occurs:

- Peer-To-Peer call receives a Barge-In without a Barge-In tone.
- Peer-To-Peer call receives a Barge-In with Monitor mode.
- Established Barge-In is disconnected.
- The Peer-to-Peer feature is a programmable feature that may be enabled or disabled by accessing Data Program 15-05-50 - Peer-to-Peer Mode.

Section 5 PROGRAMMING

The first step to connecting IP telephones to the NEC SL2100 system is to connect the NEC SL2100 system to the customer data network. Refer to [General IP Configuration](#). Next, program the VoIPDB and associated IP telephone settings. To complete the installation, program the IP telephone.

The programming commands required to complete this installation are located in [Programming](#). This section provides a brief description of the commonly used commands:

- **10-12-03 CPU Network Setup - Default Gateway**
If required, select the default gateway IP address to use when using a router (default: 0.0.0.0).
- **10-12-09 CPU Network Setup - IP Address**
Select the IP address for the IP connection
- **10-12-10 CPU Network Setup - Subnet Mask**
Assign the subnet mask for the VoIPDB
- **15-05-50 Peer to Peer Mode**
Enable/Disable the Peer-to-Peer feature between IP Stations.



Disabling this feature results in IP Station-to-IP Station calls using DSP Resources.

- **15-05-15 IP Telephone Terminal Basic Data Setup - CODEC Type**
For each IP telephone, set which CODEC Type to use.
- **84-26-01 VoIPDB Basic Setup - IP Address**
Enter the IP address for the VoIPDB.
- **84-26-02 VoIPDB Basic Setup - RTP Port Number**
Enter the RTP port number range.

5.1 Music on Hold

Music on Hold is provided by the IP telephone. The settings in Program 10-04 : Music on Hold Setup are ignored except to determine whether or not music is to be provided. If 10-04-02 is set to 0, no Music on Hold is heard. If 10-04-02 is set to 1 or 2, music is provided by the IP telephone.

Section 6 CONFIGURATION EXAMPLES

The examples below show typical scenarios and basic programming required. These examples assume that the programming steps below are performed on a default system (i.e., no existing configuration).

6.1 Example Configuration 1 - Static IP Addressing, One LAN

This example shows IP Phone connected to a single LAN (no routers), with static IP Addresses.

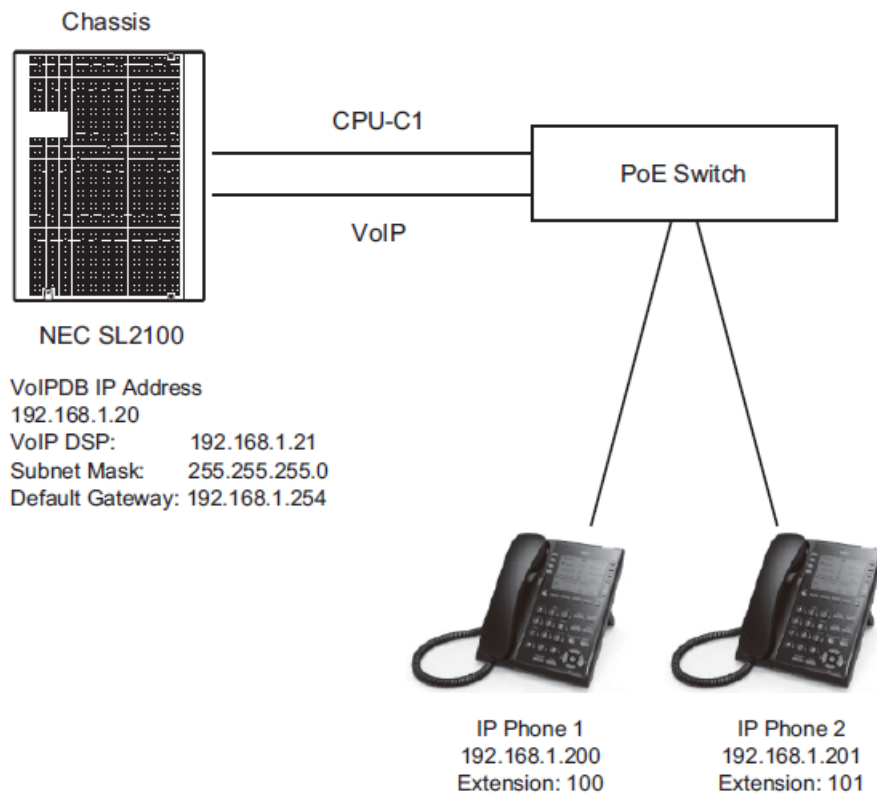


Figure 9-3 Example Configuration 1 - Static IP Addressing, One LAN

Programming - CPU:

10-12-01 : CPU Network Setup - IP Address (for CPU)	0.0.0.0
10-12-10 : CPU Network Setup - Subnet Mask	255.255.255.0
10-12-03 : CPU Network Setup - Default Gateway	192.168.1.254
10-12-09 : CPU Network Setup - VoIPDB IP Address	192.168.1.20

Programming - VoIP DSP Resource:

84-26-01 : VoIP Basic Setup - IP Address (Slot # - DSP)	192.168.1.21
---	--------------

Programming - IP Phones:

DHCP Mode	Disabled
IP Address	192.168.1.200
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
1st Server Address	192.168.1.20
1st Server Port	5080

6.2 Example Configuration 2 - Dynamic IP Addressing, One LAN

This example shows System IP Phones connected to a single LAN (no routers) with dynamic IP Addresses. The DHCP server could be:

- Customer supplied (e.g., Windows server)
- inDHCP internal DHCP server

In this case, additional programming would be required. Refer to [General IP Configuration](#).



Built-in VoIP (by CPU-C1) also be supported for In-DHCP feature.

6.2.1 In-DHCP Ethernet port Only Configuration

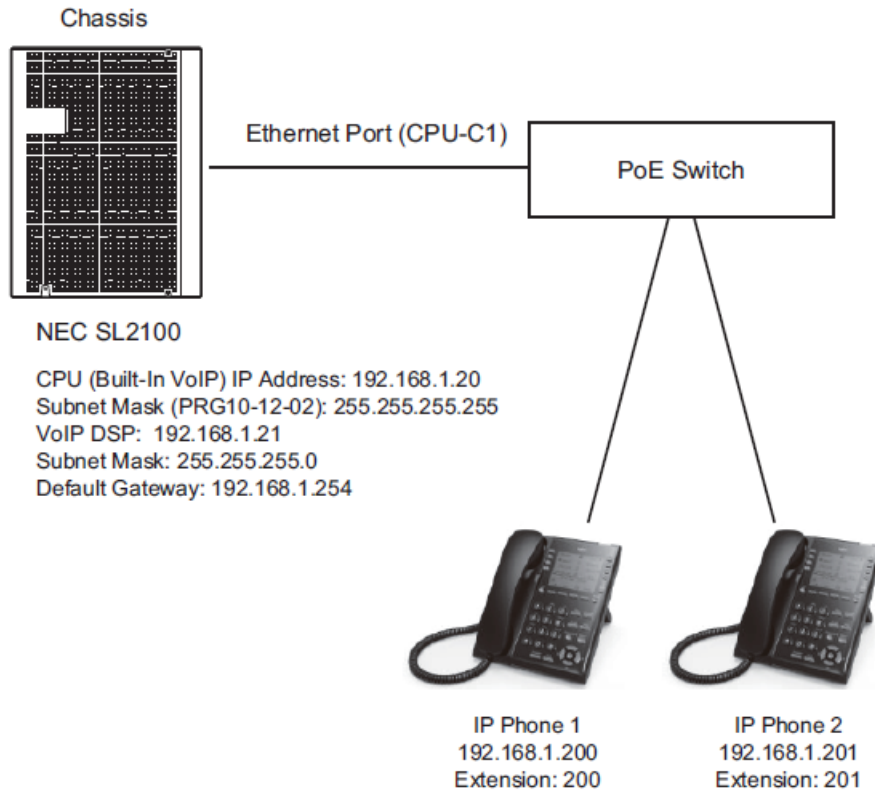


Figure 9-4 Example Configuration 2-1 - Dynamic IP Addressing, One LAN

Programming - CPU:

10-12-01 : IP Address (for CPU)	192.168.1.10
10-12-02 : Subnet Mask	255.255.255.255
10-12-03 : Default Gateway	192.168.1.254
10-12-09 : VoIP IP Address	192.168.1.20
10-12-10 : VoIP IP Subnet Mask	255.255.255.0
10-13-01 : DHCP Server Mode	Enable
10-14-01 : Min	192.168.1.200
10-14-02 : Max	192.168.1.250
10-16-16 : SIP Server IP Address	192.168.1.20
10-16-27 : SIP Server Receiver Port	5080

Programming - VoIP DSP:

84-26-01 : VoIP Basic Setup - IP Address	192.168.1.21
--	--------------

Programming - IP Phone 1:

DHCP Mode	Enabled
IP Address	192.168.1.200
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
1st Server Address	192.168.1.20
1st Server Port	5080

Programming - IP Phone 2:

DHCP Mode	Enable
IP Address	192.168.1.201

Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
1st Server Address	192.168.1.20
1st Server Port	5080

6.2.2 In-DHCP VoIPDB port Configuration

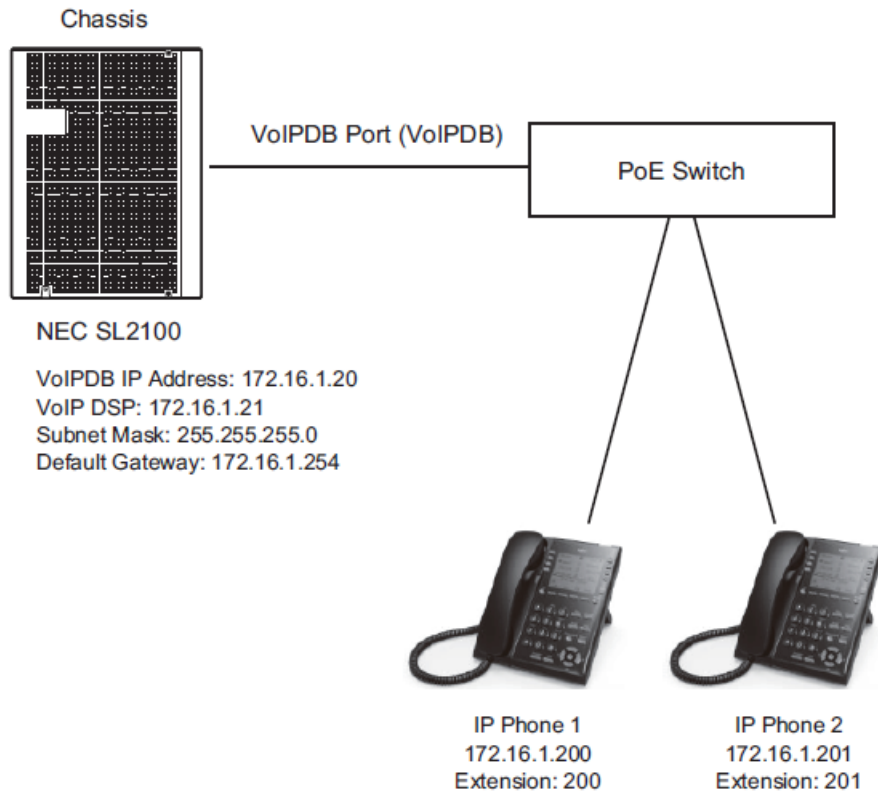


Figure 9-5 Example Configuration 2-2 - Dynamic IP Addressing, One LAN

Programming - CPU:

10-12-01 : IP Address (for CPU)	0.0.0.0
10-12-02 : Subnet Mask	-
10-12-03 : Default Gateway	172.16.1.254
10-12-09 : VoIP IP Address	172.16.1.20
10-12-10 : VoIP IP Subnet Mask	255.255.255.0
10-13-01 : In-DHCP Server Setup - DHCP Server Mode	Enable
10-14-01 : Min	172.16.1.200
10-14-02 : Max	172.16.1.250
10-16-16 : SIP Server IP Address	172.16.1.10
10-16-27 : SIP Server Receiver Port	5080

Programming - VoIP DSP:

84-26-01 : VoIPDB DSP IP Address	172.16.1.21
----------------------------------	-------------

Programming - IP Phone 1:

DHCP Mode	Enabled
IP Address	172.16.1.200
Subnet Mask	255.255.255.0

Default Gateway	172.16.1.254
1st Server Address	172.16.1.20
1st Server Port	5080
Programming - IP Phone 2:	
DHCP Mode	Enable
IP Address	172.16.1.201
Subnet Mask	255.255.255.0
Default Gateway	172.16.1.254
1st Server Address	172.16.1.20
1st Server Port	5080

6.3 Example Configuration 3 - Static IP Addressing, Routed WAN

This example shows IP Phones connected to an NEC SL2100 system over a Wide Area Network (WAN), with static IP addressing. This is a typical scenario - a small branch office connecting to the main office.

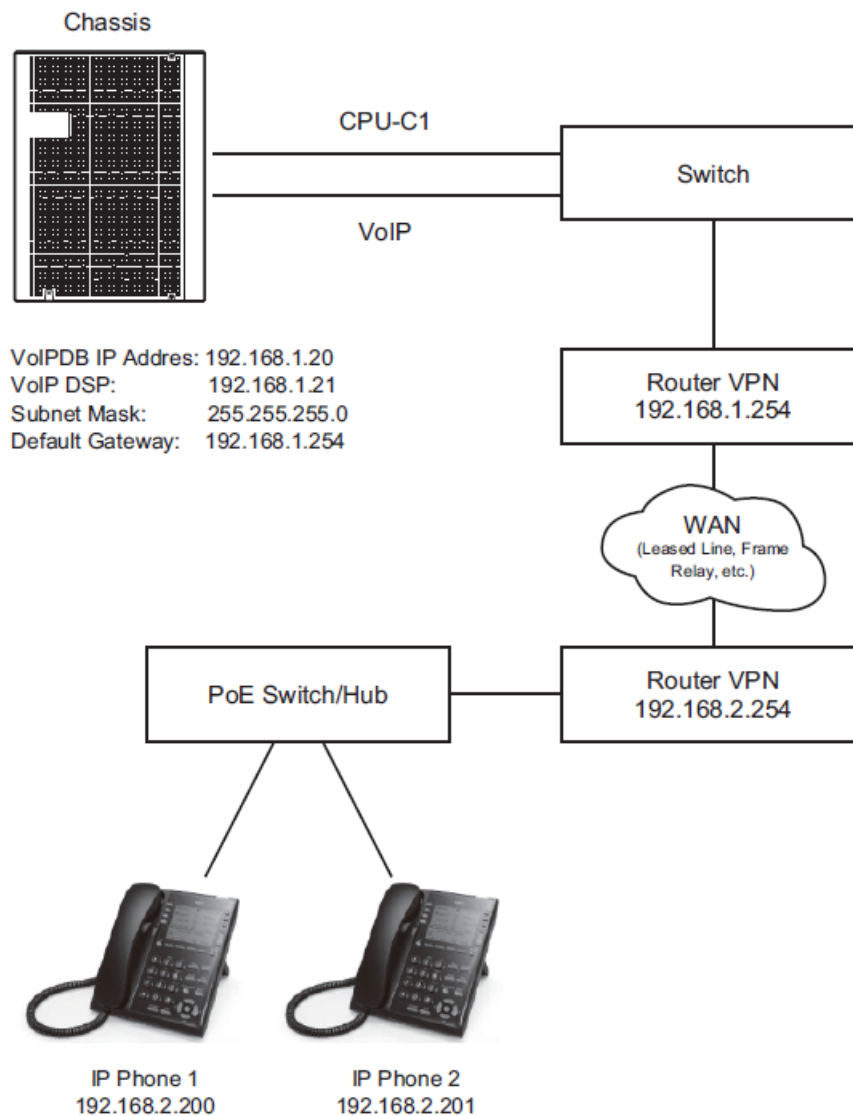


Figure 9-6 Example Configuration 3 Static IP Addressing, Routed WAN

Programming - CPU:

10-12-01 : CPU Network Setup - IP Address	0.0.0.0
10-12-10 : CPU Network Setup - Subnet Mask	255.255.255.0
10-12-03 : CPU Network Setup - Default Gateway	198.168.1.254
10-12-09 : CPU Network Setup - VoIPDB IP Address	192.168.1.20
Programming - VoIPDB DSP:	
84-26-01 : VoIPDB Basic Setup - IP Address (Slot # - DSP)	192.168.1.21
Programming - IP Phones:	
DHCP Mode:	Disabled
IP Address:	192.168.2.200
Subnet Mask:	255.255.255.0
1st Server Address:	198.168.1.20
1st Server Port:	5080

Section 7 IP PHONE PROGRAMMING INTERFACE

This section describes how to access the programming interface for IP Phones. The following describes how to access the User Menu.

1. Using a 8IPLD/DT900 telephone, press **HOLD-Transfer-*-#** buttons to enter program mode. The IP User Menu is displayed.
2. On the IP User Menu, enter the user name and password for the IP Phone. Settings are listed in [Table 9-1 IP Phone Programming Options User Menu](#).

Table 9-1 IP Phone Programming Options User Menu

Programming Option	Default
UserName	ADMIN
Password	6633222

Section 8 DHCP SERVER CONFIGURATION

It is possible to use either an external DHCP server (e.g., Windows Server) or the NEC SL2100 internal DHCP server. With IP Phones, either of these options requires the DHCP server to be configured to supply the IP terminal options.

If using the internal DHCP server, enable the DHCP server. Refer to [Example Configuration 2 - Dynamic IP Addressing, One LAN](#).

When using an external DHCP server, you must add a new Option Code to the DHCP scope for the VoIPDB IP address. The method for adding this service varies depending on the DHCP server used.

Section 9 CONFIGURING QUALITY OF SERVICE

NEC recommends configuring Quality of Service (QoS) to ensure that the speech quality is not affected by other data on the network. QoS is discussed further in [Network Design Considerations](#).

The NEC SL2100 system supports:

- IEEE802.1q (VLAN Tagging)
- IEEE802.1p (Priority)

With the VLAN tagging mode, the NEC SL2100 system can handle packets with or without a VLAN tag. If the VLAN ID of a packet is different from the registered one, that packet is dropped.

9.1 Layer 2 Priority Control

Layer 2 priority control can be enabled on an Ethernet switch, if it supports VLAN tagging. This allows layer 2 prioritization.

Using a switch that supports 802.1p allows:

- priority control
- reduction of unnecessary packets (e.g., broadcast packets) and provides circuitry by restricting a broadcast domain

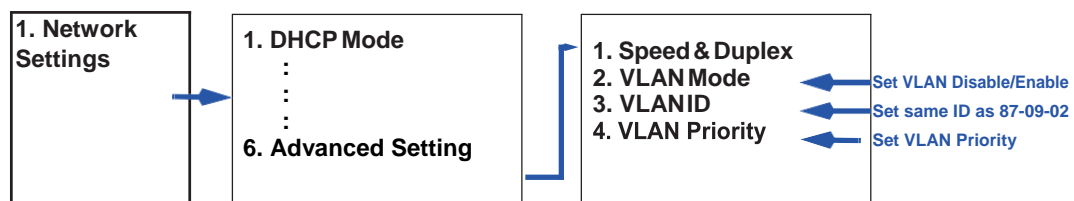
9.1.1 Programming Layer 2 Priority Control

To program Layer 2 Priority Control for IP Phones VLAN/QoS:

1. Press the **Menu** button on the IP Phone to enter the telephone program mode.



This enters the IP program mode to select the settings for the individual phone. The flashing item is the current selection.



2. Press **OK**, **EXIT**, **SAVE** softkeys to save the entries and return the telephone to idle.

9.2 Layer 3 (ToS) Priority Control

The router-supported ToS controls routing priority of packets by following the ToS field. You can give priority to the voice packet using the ToS field.

There are two types of ToS formats: DiffServ and IP Precedence. Before programming the router, make sure to check which type is supported by the router.

The NEC SL2100 system can set the ToS value for each protocol, and Voice Control. This setting allows flexible prioritization.

9.2.1 Programming Layer 3 Priority Control

To program Layer 3 VLAN/QoS use the following programs.

- **84-10-01 ToS Setup – ToS Mode**

For the Protocol type (1= Not Used, 2= Not Used, 3= Reserved, 4= H.323, 5= RTP/RTCP, 6= SIP, 7= Reserved, 8= SIP MLT, 9= SIP Trunk, 10=Reserved, 11=Reserved), select the ToS mode (Disable, IP Precedence or Diffserv).

- **84-10-07 ToS Setup – Priority (D.S.C.P. - Differentiated Services Code Point)**

For the Protocol type (1= Not Used, 2= Not Used, 3= Reserved, 4= H.323, 5= RTP/RTCP, 6= SIP, 7= Reserved, 8= SIP MLT, 9= SIP Trunk, 10=Reserved, 11=Reserved), if Program 84-10-01 is set to 2, select the Diffserv priority (0~63).

Section 10 IP TELEPHONE REGISTRATION AND DELETION

When an IP Phone connects to the NEC SL2100 system, it is assigned the first available port, starting from the value set in Program 11-02-01.

The ports are allocated in blocks of two.

For example:

- Insert a VoIPDB.
- Program 11-02-01 Extension Numbering.
- Configure a System IP Phone and connect to the LAN.

When connecting an IP Phone, the MAC address (ID) is automatically registered in Program 15-05-02. If the registration in Program 15-05-02 is made manually (before connecting the telephone) it uses the assigned port number when the telephone is connected. The MAC address is printed on the barcode label on the bottom of the telephone. It is a 12-digit alphanumeric number, ranging from 0~9 and A~F.

To delete a telephone registration:

Enter Program 90-23-01, and enter the extension number of the IP Phone. If connected to the SL2100 via Telephone Programming, enter a 1 to delete the IP phone and then press **Hold**. If connected to the SL2100 via Web Pro, place a check next to the extension and click **Apply**.

Section 11 SYSTEM IP PHONES AND ANALOG TRUNKS

Due to the nature of analog-to-digital conversion, considerable echo may be encountered when using Analog Trunks with IP Phones.

Due to all Analog trunks being different, padding of the Analog Trunks in PRG 81-07 and 14-01 may be necessary. Even after the pad changes are made, echo may still be present the first few seconds of the call while the echo cancellers are learning the characteristics of the circuit on this call.

It is recommended to use digital trunks when using IP phones for best performance.


Digital (ISDN, T-1, and SIP) trunks do not suffer from this problem.

When analog trunks are installed in an SL2100, PRG 90-68 (Side Tone Auto Setup) must be used. This program will automatically change the setting of 81-07 after multiple tests are performed on the analog line. During these tests the system will not be usable, and the system must be reset once the test are finished.

Anytime new analog trunks are added to the system, PRG 90-68 **MUST** be used.

Section 12 FIRMWARE UPGRADE PROCEDURE

A firmware for the IP Phones can be applied automatically or manually.

 *Automatically Upgrading Firmware is supported on IP7[]-8IPLD-C1 TEL. DT900 series are not supported.*

The upgrade requires using an FTP/TFTP server. This is a software package that runs on a PC. (These can be downloaded from the Internet, usually as freeware or shareware.)

12.1 Manually Upgrading Firmware

Manually upgrading the firmware uses an FTP/TFTP server, but requires the engineer visit each IP Phone individually. This may take longer, but is more controlled as the downloads can be staggered to avoid excessive bandwidth utilization.

To manually upgrade the firmware:

1. Install and configure an FTP/TFTP server.
2. Copy the firmware file **itlisipr.tgz** to the default FTP/TFTP directory.
3. To enter Programming Mode, press the **Hold, Transfer, *, #** button on the IP Phone.
4. To enter Maintenance Mode, press **3: Maintenance Settings**.
5. To access the Download menu, press **1**.
6. Enter the FTP/TFTP server IP address in Option 2 - Download Address.
7. To enter the protocol, press **#3** (Protocol FTP or TFTP).
8. To select download by file, press option **1** (Download File).
9. To boot the program, press **2** (Boot & Program).
10. Press the softkey.

The IP Phone downloads the firmware from the FTP/TFTP server and reboots when the download is complete.

12.2 Checking the Firmware Version

To check the IP Phone firmware version:

1. Press and hold the **HELP** button on the IP Phone.
2. Press **2** (System Information).
3. Press **5** (Keyset Information).
4. Press the **Next** softkey two times.

12.3 Upgrading Automatically

This procedure causes all IP Phones to attempt firmware upgrade the next time they connect to the CPU. This can make the upgrade procedure easier, as it is not necessary to visit every telephone to perform the upgrade.

This can cause problems if, for example, a PoE (Power over Internet) switch is used. When the PoE switch is powered up, all telephones connect to the FTP/TFTP server at the same time. This causes a large amount of data for the FTP/TFTP server to transfer over the data network.

To avoid this, connect the telephones to the PoE switch gradually, to allow time for each telephone to upgrade before connecting the next.

To enable automatic upgrade:

1. Install and configure an FTP/TFTP server.
2. Copy the firmware file **itlisipr.tgz** to the default FTP/TFTP directory.
3. Set the server mode to FTP/TFTP in Program 84-07-01 and specify the IP address of the FTP/ TFTP server (this is the PC where the FTP/TFTP software is installed) in Program 84-07-02.
4. In Program 84-28 program the Firmware Directory path on the FTP/TFTP server and assign the file name (itlisipr.tgz).
5. In Program 90-42, assign the software and hardware versions. An example of the hardware assignment would be 09.01.03.06, this is Hardware Version 9.1.3.6.

Section 13 IP STATION (SIP MULTILINE TELEPHONE)

13.1 Description

The NEC SL2100 system supports IP phones using Session Initiation Protocol (SIP). These IP telephones have the same look and functionality as typical multiline telephones, but they are connected to an VoIPDB card in the CPU rather than hardwired to a Digital Station port.

Some of the benefits of an IP phone over a traditional TDM phone are described in the following list:

- Reduced telephone re-location costs. Unplug an IP telephone at one location and plug it into another VoIP ready jack at another location. The extension number can stay with the telephone, if programmed to do so.
- Multiple users can share the same IP telephone but keep their own personal extensions. With an IP phone you have the ability to log the phone out, then log back in with another extension number. All of your personal settings follow the login ID of your extension.
- The cabling infrastructure can be simplified. There is no longer a need for separate cabling for the phone system. Built into the IP phones is a 2 port 10/100 manageable data switch. The data connection for the PC is available on the back of the IP phone. This built in data switch also supports 802.1Q and 802.1 P VLAN tagging abilities. The data and the voice can be tagged separately.
- Allows you to connect remote office workers with a telephone that has the look and same functionality as the telephones connected at the office.

SIP is used for VoIP as defined by the IETF (Internet Engineering Task Force) RFC3261. The NEC SIP MLT uses IP Multiline Station (SIP) (proprietary enhanced SIP protocol) to facilitate the multifunction, multiline telephone.

The SIP Multiline Telephone interfaces directly to the CPU that houses the VoIPDB daughter board. The VoIPDB provides the digital signal processors (DSPs) for IP stations and trunks.

- VoIPDB provides 128 DSPs

A DSP provides format conversion from circuit switched networks (TDM) to packet switched networks (IP). Each voice channel from the circuit switched network is compressed and packetized for transmission over the packet network. In the reverse direction, each packet is buffered for de-jittering, decompressed and sent to the circuit switched network. Each DSP converts a single speech channel from IP to TDM and vice versa.

The following are examples of DSP allocation.

- Calling from an IP phone to a TDM phone uses one DSP.
- Calling from an IP phone to another IP phone, registered to the same CPU, uses no DSPs.
- Calling from a TDM phone to another TDM phone uses no DSPs.
- Calling from a TDM phone and out an IP trunk uses one DSP.



An IP to IP call is peer-to-peer, and no DSP resource is used. When this feature is deactivated, an IP to IP call consumes two DSP resources.

13.2 IP Addressing

When a VoIPDB daughter board is installed in an SL2100 two IP addresses, in the same network, will be required. One IP Address will be for the VoIPDB and this address is assigned in Program 10-12-09. This IP Address is used for IP Phones/Trunks to register and pass signaling messages. The other IP Address is for the DSP's and this address is assigned in Program 84-26-01. This IP Address is used to pass voice traffic.

By default when an SL2100 with a VoIPDB is installed in a customer's network, the SL2100 will try and request IP Addressing information from the local DHCP server (DHCP Client Feature). The DHCP server can provide the SL2100 with the following information:

- IP Address for VoIPDB (PRG 10-12-09)
- Subnet Mask for VoIPDB (PRG 10-12-10)
- Default Gateway for VoIPDB (PRG 10-12-03)

The DHCP server will NOT provide the IP address for the DSP's (PRG 84-26-01). This IP Address will have to be manually configured.

The DHCP Client Feature can be disabled in Program 10-63-01. When this program is changed a reset of the SL2100 is required.

When the VoIPDB is installed, in the SL2100, the CPU NIC card is no longer available. All connections that previously were terminated to the CPU will now terminate to the VoIPDB. It is recommended when adding the VoIPDB to change the IP Address of the CPU NIC card (PRG 10-12-01) to be 0.0.0.0.

13.3 IP Phone Registration Modes

The SIP MLT supports three different registration modes.

- Plug and Play
- Automatic Login
- Manual Login

Plug and Play Registration

Plug and play registration mode allows for no authentication. As long as an IP terminal is configured with the proper IP addressing scheme, and plugged into the network, the phone comes on-line. In plug and play mode you may assign an extension number into the IP terminal or allow the system to automatically set an unused extension number for the station. When the system assigns unused extension numbers it starts searching for the first available port or starts at a preassigned port and works its way up from there.

Automatic Login

When set to automatic login the SIP user name and password must be entered in the configuration in the IP terminal. When the phone tries to register with the CPU it checks the user name and password against its database. If the user name and password match, the phone is allowed to complete registration. If the user name and password do not match, the phone cannot register with the CPU. The IP terminal displays an error message: *Unauthorized Auto Login*.

Manual Login

When set to manual login, no user name, password, or extension number is entered into the configuration of the telephone. The user is prompted to enter this user name and password into the IP phone. This information is cross referenced in the phone system to an associated extension number. If a match is found, the phone comes online. If there is no match, the phone cannot complete registration with the CPU. The IP terminal either returns to the login/password screen, or locks out the user and requires the administrator to unlock the IP terminal. Lockout on failed attempts is dependent on system programming. Manual mode is good for an environment where multiple users share the same IP phone at different times. As one user logs out the next user can login with their credentials and all of their associated programming follows.

In Manual mode a user can also logoff the IP phone to allow another user to login with their own login ID and password.

To logoff the IP Phone when the terminal is set to "Standard" softkey mode (PRG 15-02-60) use the following operation: Press the "Prog" softkey, press the "Down Arrow", press the "Down Arrow", press the "Down Arrow", and then press "Logoff". The IP Phone can also be logged off by resetting the IP terminal.

To logoff the IP Phone when the terminal softkey is set to "Advanced Mode 1/2" (PRG 15-02-60) the IP terminal must be reset.

Encryption

The SL2100 Supports AES 128-bit encryption between IP Multiline Terminals (8IPLD/DT900) and the VoIPDB.

Table 9-2 IP Multiline (8IPLD/DT900) Supported Encryption

Source	Destination	SRTP	Comment
IP Multiline	STD SIP (P2P)	N	
IP Multiline	STD SIP (Non P2P)	S	The encryption will be between the IP terminal and the VoIPDB. Once the voice leaves the SL2100 to third party SIP terminal the voice cannot be encrypted.
IP Multiline	IP Multiline	S	
IP Multiline	PSTN	S	The encryption will be between the IP terminal and the VoIPDB. Once the voice leaves the SL2100 to the public network it cannot be encrypted.
IP Multiline	IP Network (SIP)	S	The encryption will be between the IP terminal and the VoIPDB. Once the voice leaves the SL2100 to the SIP network it cannot be encrypted.
IP Multiline Encryption On	IP Multiline Encryption Off	N'	

S = Supported N = Not Supported

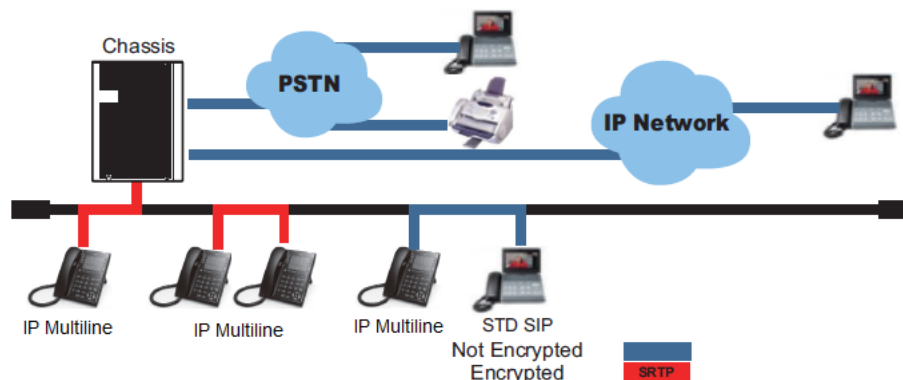


Figure 9-7 IP Multiline (8IPLD/DT900) Encryption

Conditions

- Encryption is not supported on 8IPLD/DT900 series phones that are connected via NAPT.
- If the encryption feature is enabled in terminal programming but not licensed, the terminal displays "Invalid server" and will not function.

13.4 General IP Configuration

The voice quality of VoIP depends on variables such as available bandwidth, network latency, and quality of service initiatives (QOS). These variables are controlled by the network and Internet service providers. Because these variables are not in NEC control, NEC cannot guarantee the performance of the users IP based voice solution. NEC recommends connecting the VoIP equipment through a local area network using private IP addresses.

To ensure a network meets the specific requirements for VoIP implementation, an IP ready check and a site survey must be completed at each site before VoIP implementation.

- One way delay must not exceed 100ms.
- Round trip delay must not exceed 200ms.
- Packet loss must not exceed 1%.
- Data switches must be manageable.
- Routers must provide QOS.
- There must be adequate bandwidth for estimated VoIP traffic. Refer to Section [Bandwidth](#).

Depending on how QOS policies are built in the network, assignments may be needed in both the CPU and IP terminal. The NEC SL2100 supports the flagging of packets at layer 2 (VLAN tagging 802.1Q/802.1P) and at layer 3 levels.

13.5 VLANs

A VLAN is used to logically break up the network and minimize broadcast domains. Without VLANs, the network must be physically segmented to break up broadcast domains. Each network segment is then connected through a routing device adding latency and cost. Latency is a delay in the transmission of data and is caused by routing packets from one LAN to another. In a VoIP environment latency must be kept to a minimum.

802.1Q allows a change in the Ethernet Type value in the Ethernet header tagging the Protocol ID 0x8100, identifying this frame as an 802.1Q frame. This inserts additional bytes into the frame that composes the VLAN ID (valid IDs = 1 ~ 4094).

802.1P allows you to prioritize the VLAN using a 3-bit priority field in the 802.1Q header. Valid VLAN priority assignments are 0 ~7. A tag of 0 is treated as normal data traffic giving no priority. Under normal circumstances the higher the tag numbers, the higher the priority. However this is left up to the network administrator as they could set the exact opposite where the lower tag numbers have a higher priority.

Tagging Voice and Data Packets

Built into the IP phones is a 2 port 10/100 manageable data switch allowing for a PC connection on the back of the IP phone. This built in data switch also supports 802.1Q and 802.1P VLAN tagging capabilities.

The following procedures describe two methods for tagging the voice packets and the data packets separately, using the PC, or using the phone keypad.

13.5.1 Logging In on the PC

1. Web browse to the IP address of phone.
2. To log in, enter default user name: **ADMIN**
3. Enter default password: **6633222**

4. Click **OK**.

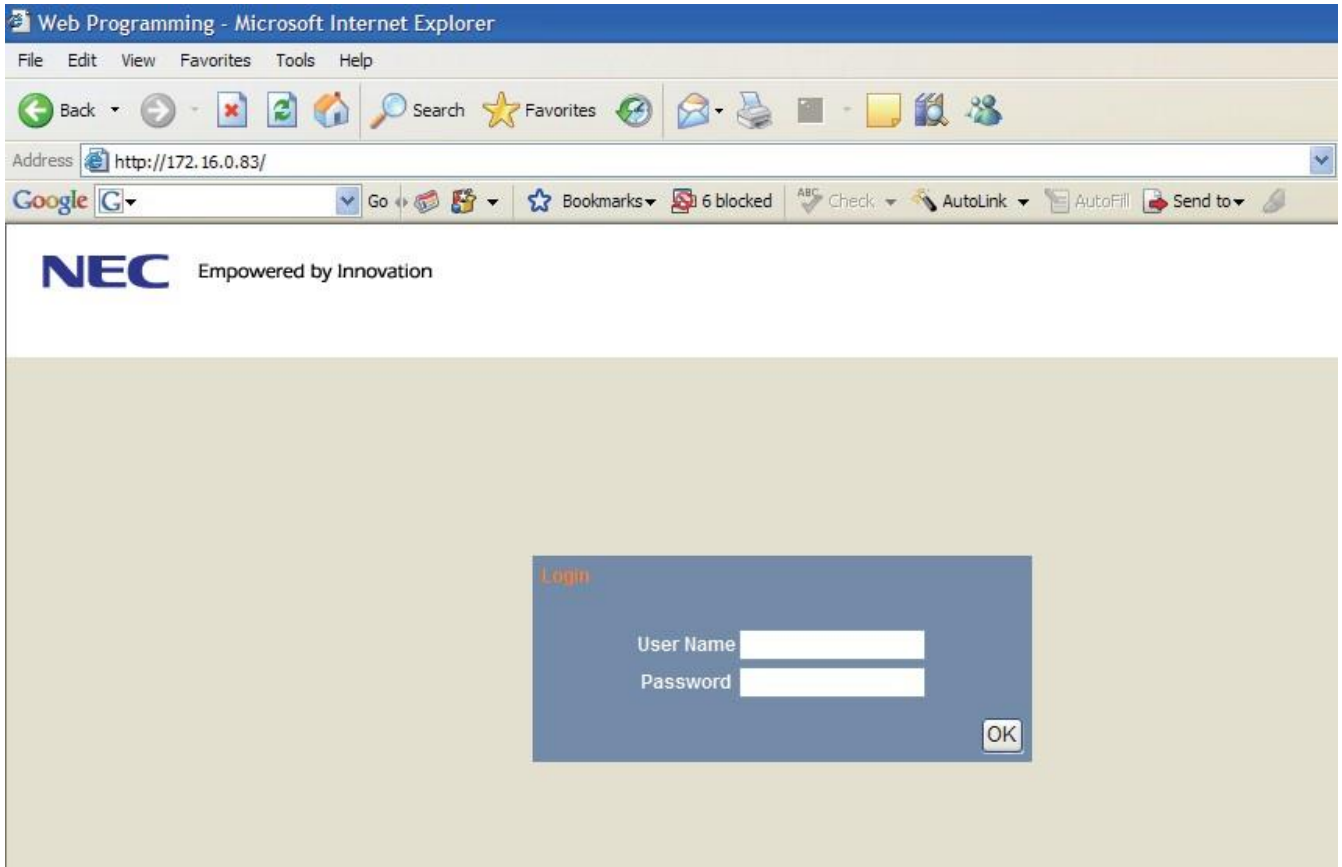


Figure 9-8 Log In to IP Phone

13.5.2 Tagging Voice Packets Using IP Phone

1. To apply a tag to the voice packets only, go to **Network Settings>Advanced Settings>LAN port settings**.

2. Access the following three menus to select options for LAN Port Settings:
 - VLAN Mode
 - VLAN ID
 - VLAN Priority

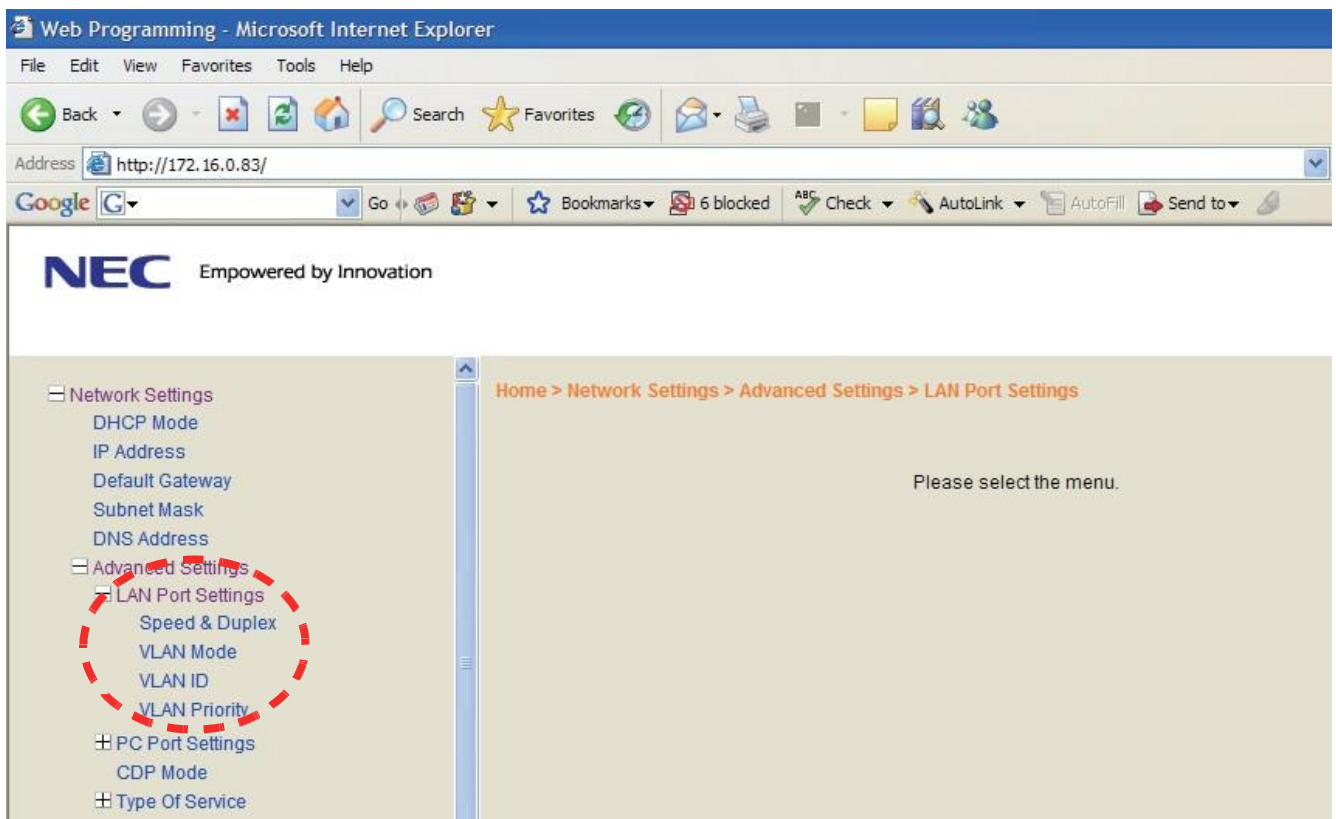


Figure 9-9 LAN Port Settings Window

3. Select the VLAN Mode to enable or disable this feature.
4. Select either Enable or Disable (default) and click **OK**.

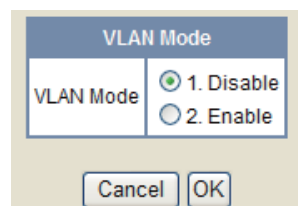


Figure 9-10 VLAN Mode

5. VLAN ID allows an entry of 1~4094 for the VLAN ID. VLAN Mode must be enabled for this entry to be valid.
Enter the VLAN ID and click **OK**.

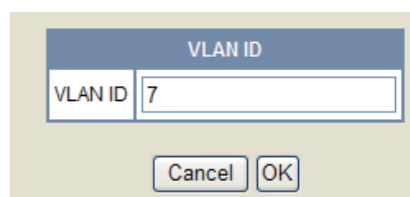


Figure 9-11 VLAN ID

- VLAN Priority allows an entry of 0~7 for the VLAN Priority. VLAN mode must be enabled for this entry to be valid.
Enter the required priority, and click **OK**.

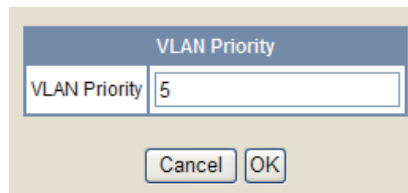


Figure 9-12 VLAN Priority

13.5.3 Tagging Data Packets Using IP Phone

- While logged in to the IP address of the phone on the PC, go to **Network Settings>Advanced Settings>PC Port Settings**. Refer to Section [Logging In on the PC](#).
- Access the following three menus to select options for PC Port Settings:
 - Port VLAN Mode
 - Port VLAN ID
 - Port VLAN Priority.

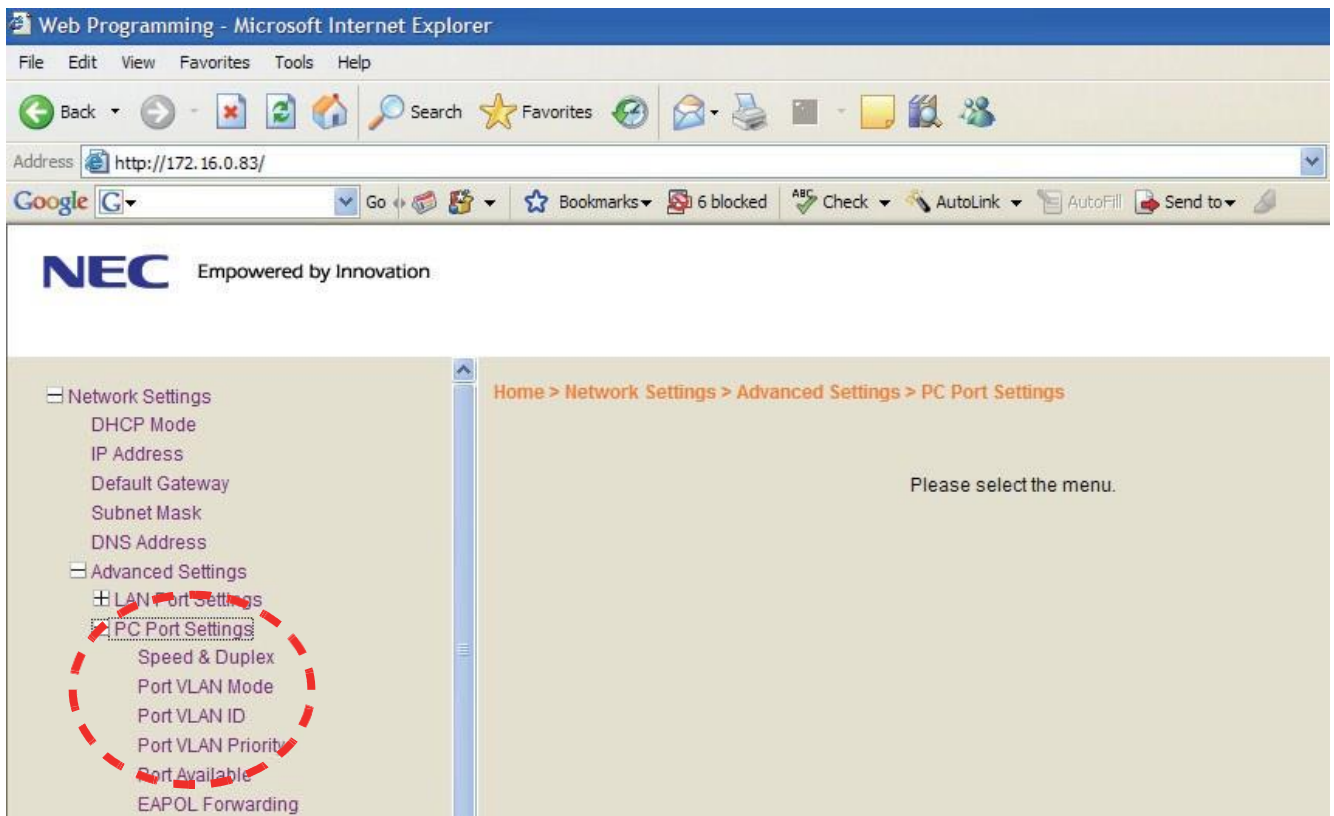


Figure 9-13 PC Port Settings Window

- Select the VLAN Mode to enable or disable this feature.

4. Select either Enable or Disable (default) and click **OK**.

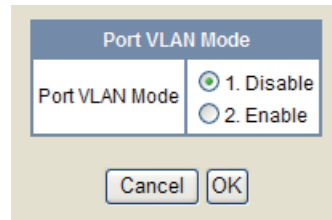



Figure 9-14 Port VLAN Mode

 *The remaining data packets settings for VLAN on the PC Port are the same as those for the voice packets.*

5. VLAN ID allows an entry of 1~4094 for the VLAN ID. VLAN Mode must be enabled for this entry to be valid.
Enter the VLAN ID, and click **OK**.

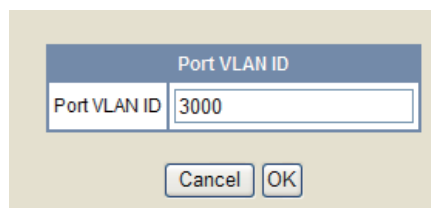


Figure 9-15 Port VLAN ID

6. VLAN Priority allows an entry of 0~7 for the VLAN Priority. VLAN mode must be enabled for this entry to be valid.
Enter the required priority, and click **OK**.

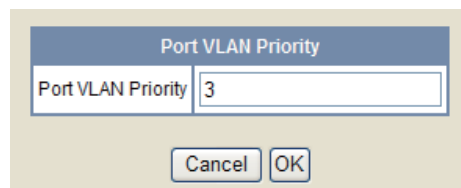


Figure 9-16 Port VLAN Priority

- Click **Save**.

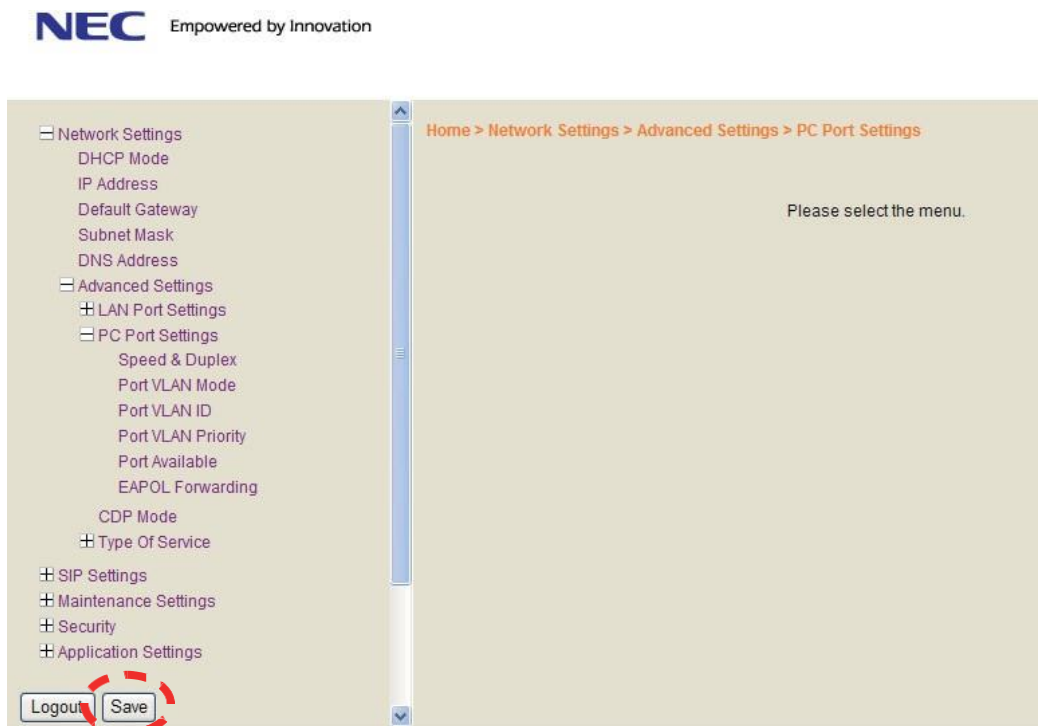


Figure 9-17 Save Network Settings

- After saving settings, click **OK** to confirm. Telephone reboots and applies the VLAN settings.

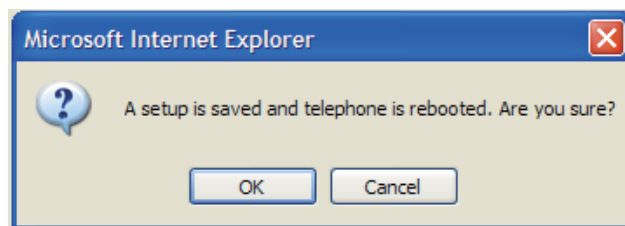


Figure 9-18 Save Confirmation Window

13.5.4 Entering VLAN Settings by Phone (Voice Packets Only)

- Press **Hold, Transfer, *, #** to enter programming mode.
- Enter the user name of **ADMIN** and password of **6633222**, then press the **OK** softkey.
- Dial **1** for Network Settings.
- Press **6** on the dial pad for Advanced Settings
- Press **1** on the dial pad for LAN Port Settings (VLAN for the voice packets only)
- Press **2** on the dial pad for VLAN Mode
- Press **1** or **2** to disable/enable the VLAN for the voice packets. Press the **OK** soft key after the setting is changed.
- Press **3** on the dial pad for VLAN ID
- Enter a valid VLAN ID of 1~4094. Press the **OK** soft key after the setting is changed.
- Press **4** on the dial pad for VLAN Priority
- Enter the VLAN priority of 0~7. Press the **OK** soft key after the setting is changed.
- If no more changes are made, press the **Exit** soft key three times. Then press the **Save** soft key, and the phone reboots.

13.5.5 Entering VLAN Settings for PC Port by Phone (Data Packets Only)

1. Press **Hold, Transfer, *, #** to enter programming mode.
2. Enter the user name of **ADMIN** and password of **6633222**, then press the **OK** softkey.
3. Press **1** on the dial pad for Network Settings.
4. Press **1** or **2** to disable/enable the VLAN for the data packets. Press the **OK** soft key after the setting is changed.
5. Press **3** on the dial pad for Port VLAN ID.
6. Enter a valid VLAN ID of 1~4094. Press the **OK** soft key after the setting is changed.
7. Press **4** on the dial pad for Port VLAN Priority.
8. Enter the VLAN priority of 0~7. Press the **OK** soft key after the setting is changed.
9. If no more changes are made, press the **Exit** soft key three times. Then press the **Save** soft key, and the phone reboots.

13.6 ToS Settings (Layer 3 QoS)

The marking of packets at layer 3 is done by marking the ToS byte in the IP header of the voice packet. The NEC SL2100 supports two methods for marking the ToS byte:

- IP precedence
- DSCP (Diffserv)

IP Precedence

IP Precedence uses the first 3 bits of the ToS field to give eight possible precedence values (0~7). Under normal circumstances the higher the number the higher the priority. However this is left to the network administrator for setup. The administrator may assign this in exactly the opposite manner with the lower values having a higher priority. Below are the eight common values for IP precedence.

- 000 is an IP precedence value of 0, sometimes referred to as routine or best effort.
- 001 is an IP precedence value of 1, sometimes referred to as priority.
- 010 is an IP precedence value of 2, sometimes referred to as immediate.
- 011 is an IP precedence value of 3, sometimes referred to as flash.
- 100 is an IP precedence value of 4, sometimes referred to as flash override.
- 101 is an IP precedence value of 5, sometimes called critical.
- 110 is an IP precedence value of 6, sometimes called internetwork control.
- 111 is an IP precedence value of 7, sometimes called network control.

Working in conjunction with IP precedence, the next 4 bits in the ToS field are designed to influence the delivery of data based on delay, throughput, reliability, and cost. However these fields are typically not used.

The following table shows the 8-bit ToS field and the associated IP precedence bits.

IP Precedence	IP Precedence	IP Precedence	Delay	Throughput	Reliability	Cost	Not Used
1(on) here = value of 4	1(on) here = value of 2	1(on) here = value of 1					

Differential Services Code Point (DSCP)

DSCP stands for Differential Services Code Point (or Diffserv for short). It uses the first 6 bits of the ToS field therefore giving 64 possible values.

The following list shows the most common DSCP code points with their binary values and their associated names:

DSCP Code Points	Binary Values	Names
000000	0	Best Effort (BE)
001000	8	Class Selector 1 (CS1)
001010	10	Assured Forwarding 11 (AF11)
001100	12	Assured Forwarding 12 (AF12)
001110	14	Assured Forwarding 13 (AF13)
010000	16	Class Selector 2 (CS2)
010010	18	Assured Forwarding 21 (AF21)
010100	20	Assured Forwarding 22 (AF22)
010110	22	Assured Forwarding 23 (AF23)
011000	24	Class Selector 3 (CS3)
011010	26	Assured Forwarding 31 (AF31)
011100	28	Assured Forwarding 32 (AF32)
011110	30	Assured Forwarding 33 (AF33)
100000	32	Class Selector 4 (CS4)
100001	34	Assured Forwarding 41 (AF41)
100100	36	Assured Forwarding 42 (AF42)
100110	38	Assured Forwarding 43 (AF 43)
101110	46	Expedited Forwarding (EF)
110000	48	Class Selector 6 (CS6)
111000	56	Class Selector 7 (CS7)

The following table shows the 8 bit TOS field and the associated Diffserv bits.

Diffserv	Diffserv	Diffserv	Diffserv	Diffserv	Diffserv	Not Used	Not Used
1(on) here = value of 32	1(on) here = value of 16	1(on) here = value of 8	1(on) here = value of 4	1(on) here = value of 2	1(on) here = value of 1		

IP Precedence/Diffserv Values Submitted in Command 84-10

Assignments for the IP Precedence/Diffserv values in the system are submitted in command 84-10. This setting data affects only the packets sent by the VoIPDB card. This does not affect the packets sent from the IP terminals.

System Data
84-10 : ToS Setup

Protocol Type	ToS Mode	IP Precedence Priority	IP Precedence Delay	IP Precedence Throughput	IP Precedence Reliability	Diffserve
Networking	Disabled	0	Normal	Normal	Normal	0
RTP/RTCP	Disabled	0	Normal	Normal	Normal	0
SIP	Disabled	0	Normal	Normal	Normal	0
DR700	Disabled	0	Normal	Normal	Normal	0
SIP Trunk	Disabled	0	Normal	Normal	Normal	0

Value should be in the range 0 to 7
This program sets the ToS Data.

Voice Packets (points to RTP/RTCP and DR700)

Signaling Packets (points to DR700)

Figure 9-19 84-10: ToS Setup

To set the IP Precedence/Diffserv bits for packets leaving the IP terminal there are the following two options:

- **System wide.** If all IP phones use the same ToS value, this can be assigned in commands 84-23-06 and 84-23-12. When an IP phone registers with the CPU, it looks for settings in these commands. If these are found, they override any previous individual settings.
- **Individual.** If different IP phones require different ToS assignments, due to the network configuration, these assignments must be set at each individual station

Command 84-23 requires a Hexadecimal representation of the 8 bit ToS field. For example, to assign the signaling packets an IP precedence value of 4 and the voice packets an IP precedence value of 5, it would be as follows. Refer to [Figure 9-20 SIP MLT Basic Setup](#).

- 80 in Hex is 10000000 - This represents the signaling packets leaving the IP phone
- A0 in Hex is 10100000 - This represents the voice packets leaving the IP phone

System Data

84-23 : DR700 Basic Setup

01 - Registration Expiry Time	<input type="text" value="180"/>
02 - Subscribe Expiry Time	<input type="text" value="3600"/>
03 - Session Expiry Time	<input type="text" value="180"/>
04 - Minimum Session Expiry Time	<input type="text" value="180"/>
05 - Invite Expiry Time	<input type="text" value="180"/>
06 - Type of Service	<input type="text" value="80"/>
07 - Registration Failure Display Time	<input type="text" value="0"/>
08 - Digest Authorization Registration Expiry Time	<input type="text" value="0"/>
10 - Password Retry Count	<input type="text" value="0"/>
11 - Password Lock Time	<input type="text" value="0"/>
12 - Inquiry Number	<input type="text"/>
13 - Media ToS	<input type="text" value="A0"/>
14 - Refer Expiry Time	<input type="text" value="60"/>

Value should be in the range 0 to 65535

Figure 9-20 SIP MLT Basic Setup

The following table shows the common IP Precedence/Diffserv values and their hexadecimal equivalent.

Table 9-3 Common IP Precedence/Diffserv Values and Hexadecimal Equivalent

IP Precedence Name	Hex Value
IP Precedence 1	20
IP Precedence 2	40
IP Precedence 3	60
IP Precedence 4	80
IP Precedence 5	A0
IP Precedence 6	C0
IP Precedence 7	E0
DSCP Name	Hex Value
DSCP 10	28
DSCP 12	30
DSCP 14	38
DSCP 16	40
DSCP 18	48
DSCP 20	50
DSCP 22	58
DSCP 24	60

DSCP 26	68
DSCP 28	70
DSCP 30	78
DSCP 32	80
DSCP 34	88
DSCP 36	90
DSCP 38	98
DSCP 46	B8
DSCP 48	C0
DSCP 56	E0

13.6.1 Enter Values on a Per Phone Basis

- By the web browser
- By configuration mode through the dial pad

To enter the values per phone, browse to the individual phone or enter the configuration mode through dial pad.

The following example describes assigning these fields via the web browser.

1. Log in on PC. Refer to Section [Logging In on the PC](#).
2. Go to **Network Settings >Advanced Settings >Type Of Service**.

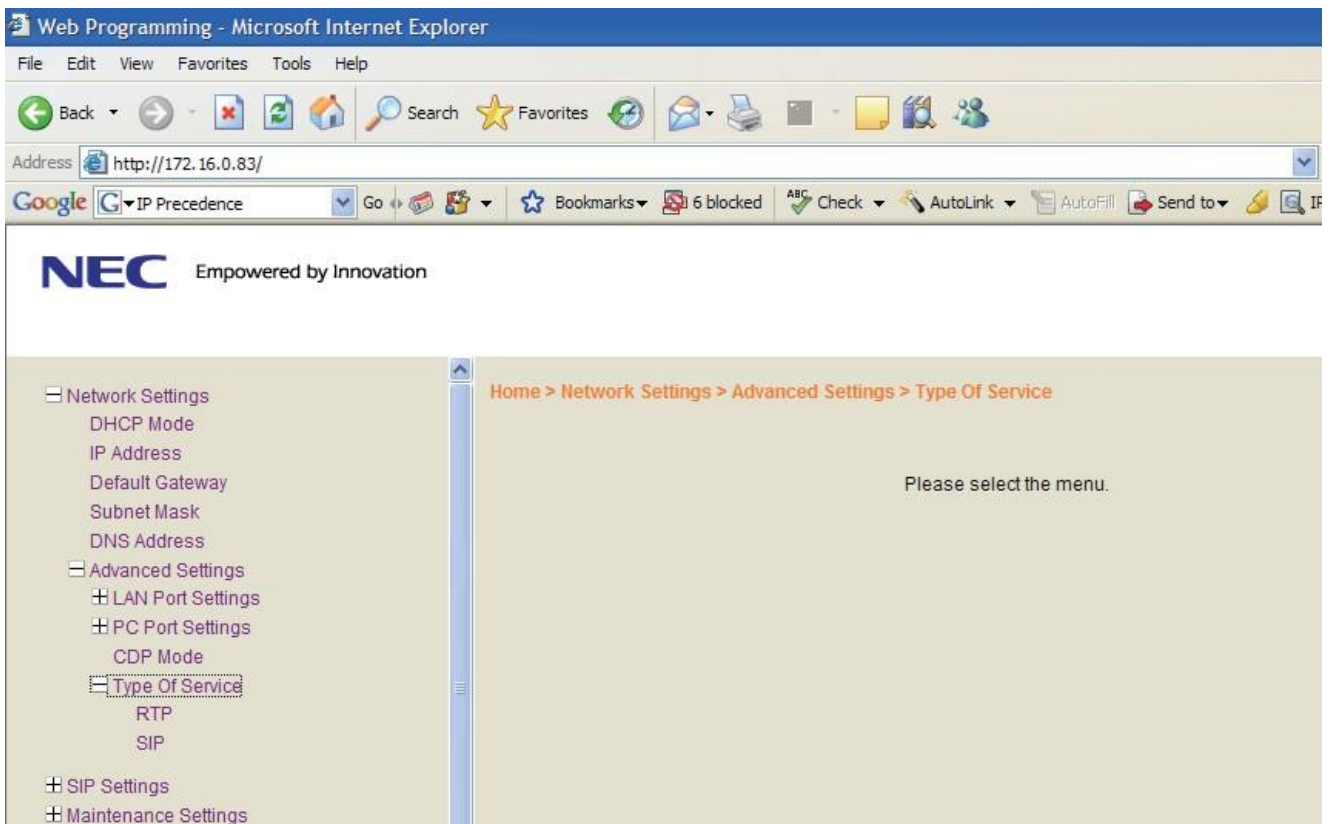


Figure 9-21 Type of Service Window

- There are two choices: RTP and SIP. RTP = voice packets and SIP = signaling packets. Select each field and assign the appropriate value. Then select **OK**. These fields are also looking for a Hexadecimal value as with command 84-23. Refer to [Table 9-3 Common IP Precedence/Diffserv Values and Hexadecimal Equivalent](#). Access the following menus to select options:

- RTP - Voice Packets
- SIP - Signaling Packets

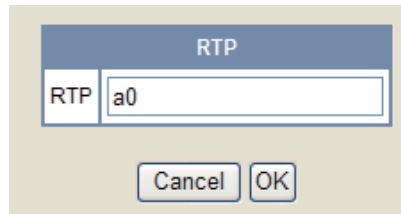


Figure 9-22 RTP - Voice Packets

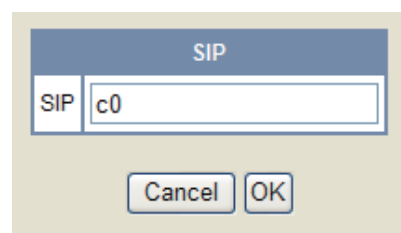


Figure 9-23 SIP - Signaling Packets

- After selecting **Save**, the following message appears.
- Select **OK** and the phone reboots. Once online, the phone tags all packets with the applied settings.

13.6.2 Assign Values on IP Terminal

The following is an example of assigning fields on the IP terminal.

- Press **Hold, Transfer, *, #**.
- Enter the user name of **ADMIN** and password of **6633222**, and press the **OK** softkey.
- Press **1** on the dial pad for Network Settings.
- Press **6** on the dial pad for Advanced Settings.
- Press **4** on the dial pad for Type of Service.
- There are two options (1) is RTP and (2) is SIP.
- Press **1** on the dial pad for RTP (voice packets), enter the hexadecimal value, and then press the **OK** soft key.
- Press **2** on the dial pad for SIP (Signaling packets), enter the hexadecimal value, and then press the **OK** soft key.
- If no more changes are to be made, press the **Exit** soft key three times, and then press the **Save** soft key. The phone reboots.

13.7 Bandwidth

The bandwidth required for VoIP calls depends on the following factors.

- Layer 2 media
- CODEC
- Packet Size
- RTP Header Compression

- Voice Activity Detection (VAD)
- Number of simultaneous calls

Layer 2 media is concerned with moving data across the physical links in the network. A few of the most common layer 2 media types are Ethernet, PPP, and Frame Relay.

CODEC stands for Coder/Decoder and is the conversion of the TDM signal into an IP signal and vice versa. A CODEC can also compress/decompress the voice payload to save on bandwidth.

Packet Size is the amount of audio in each PDU (protocol data unit) measured in milliseconds. The larger the packet the less bandwidth used. This is because sending larger packets (more milliseconds of voice) requires, overall, less packets to be sent. The downside of this practice is if a packet is dropped/lost a larger piece of voice is missing from the conversation as the system waits the additional delay for the next packet arrival.

RTP Header Compression compacts the RTP header from 40 bytes in size to 2 ~ 4 Bytes in size. RTP header compression is used only on low speed links. Regularly on every voice packet there is an IP/UDP/RTP header that is 40 bytes in length. Compressing this header, down to 2 ~ 4 bytes, can save a considerable amount of bandwidth. The following is an example of a VoIP packet without RTP header compression and one of a packet with RTP header compression.

Notice that the overall packet size, when using RTP header compression, is considerably smaller.

- VoIP packet without RTP header compression

IP Header 20 bytes	UDP Header 8 Bytes	RTP Header 12 bytes	VOICE PAYLOAD
-----------------------	-----------------------	------------------------	---------------

- VoIP packet with RTP header compression

Compressed Header 2 ~ 4 bytes	VOICE PAYLOAD
----------------------------------	---------------

Voice Activity Detection (VAD) is suppression of silence packets from being sent across the network. In a VoIP network all conversations are packetized and sent, including silence. On an average a typical conversation contain anywhere from 35% ~ 45% silence. This can be interrupted as 35% ~ 45% transmission of VoIP packets, as having no audio, using valuable bandwidth. With the VAD option enabled, the transmitting of packets stops after a threshold is met determining silence. The receiving side then injects comfort noise into the call so it does not appear the call has dropped.

Bandwidth Calculations

The first step in calculating the bandwidth of a call is determining how many bytes the voice payload is going to use. The amount is directly affected by the CODEC and packet size. Below are the supported default CODEC speeds for SIP Multiline telephones.

- G.711 = 64000bps
- G.722 = 64000bps
- G.729 = 8000bps

Payload Calculation Voice

- $(\text{Packet size} * \text{CODEC bandwidth}) / 8 = \text{Voice Payload in Bytes}$
- Example of G.711 with a 20ms packet size
- $(.020 * 64000) / 8 = 160 \text{ Bytes}$
- Example of G.729 with a 30ms packet size
- $(.030 * 8000) / 8 = 30 \text{ Bytes}$

Now that you have the voice payload in bytes you can calculate the overall bandwidth including the layer 2 media. Below are some of the common layer 2 media types and their overhead.

- Ethernet = 18 Bytes
- 802.1Q/P Ethernet = up to 32 bytes
- PPP = 9 Bytes
- Frame Relay = 6 Bytes
- Multilink Protocol = 6 Bytes

Bandwidth Calculation

$([\text{Layer 2 overhead} + \text{IP/UDP/RTP header} + \text{Voice Payload}] / \text{Voice Payload}) * \text{Default CODEC speed} = \text{Total Bandwidth}$

Example of a G.711 call over Ethernet using a 20ms packet size and not using RTP header compression

$(.020 * 64000) / 8 = 160$ Bytes for Voice Payload

$([18 + 40 + 160] / 160) * 64000 = 87200\text{bps}$

If VAD is not enabled each side of the conversation would be streaming 87.2kbps in one direction for a total of 174.4kbps.

The following chart shows the supported CODECS for IP phones with different packet sizes over PPP and Ethernet.

CODEC	Packet Size	PPP	Ethernet
G.711	10	103.2 kbps	110.4 kbps
G.711	20	83.6 kbps	87.2 kbps
G.711	30	77.1 kbps	79.5 kbps
G.711	40	73.9 kbps	75.6 kbps
G.722	10	103.2 kbps	110.4 kbps
G.722	20	83.6 kbps	87.2 kbps
G.722	30	77.1 kbps	79.5 kbps
G.722	40	73.9 kbps	75.6 kbps
G.729	10	47.2 kbps	54.4 kbps
G.729	20	27.6 kbps	31.2 kbps
G.729	30	21.1 kbps	23.5 kbps
G.729	40	17.8 kbps	19.6 kbps
G.729	50	15.9 kbps	17.3 kbps
G.729	60	14.5 kbps	15.7 kbps

13.8 Some Network Considerations

When adding the SL2100 to a customer's network there are many things to be aware of. Before implementation a detailed network diagram of the existing network must be obtained from the customer. This diagram may provide you with information about possible network conditions that can prevent or hinder the VoIP equipment from functioning correctly.

Firewalls

Another regular device in customer networks that can hinder VoIP performance is a firewall. Most corporate LANs connect to the public Internet through a firewall. A firewall is filtering software built into a router or a stand alone server unit. It is used to protect a LAN it from unauthorized access, providing the network with a level of security. Firewalls are used for many things, but in its simplest form, a firewall can be thought of as a one way gate. It allows outgoing packets from the local LAN to the Internet but blocks packets from the Internet routing into the local LAN, unless they are a response to query.

A firewall must be configured to allow specific traffic from the Internet to pass through onto the LAN. If an IP phone is deployed out over the Internet there is a very good chance it is passing through a firewall, either at the MAIN, the remote, or both locations.

The following diagram shows two IP phones on the corporate local LAN and one IP phone on a Remote network connected via the Internet. The two phones that are installed on the local LAN are functioning correctly. The IP phone at the remote site cannot register therefore it is not working.

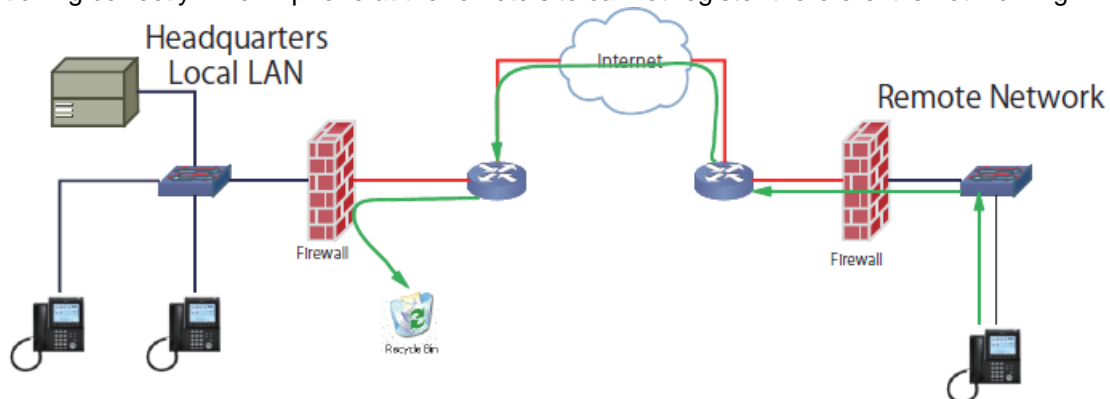


Figure 9-24 NEC SL2100 Network Example No. 1

The green arrow in the diagram above represents the data packets leaving the IP phone destined for the SL2100 on the Headquarters LAN. The firewall on the Headquarters network is not configured to recognize the UDP ports used by the NEC equipment thus blocking them and resulting in registration failure. To solve this issue the ports used by the NEC VoIP equipment must be opened in the firewall allowing the NEC traffic to pass through onto the SL2100.

The ports that are required to be opened on the headquarters locations are:

5080 and 5081 (UDP) for Signaling and 10020 ~ 10147 (UDP) for Voice.

The ports that need to be opened on the Remote network are **5060** (UDP) for signaling and ports **3462** and **3463** for voice (UDP).

VPN

Another common feature is the use of the Internet as the WAN between customer locations. When this is done VPNs are typically used between the locations. A VPN (Virtual Private Network) is a private data network that maintains privacy through the use of tunneling protocols and security features over the public Internet. This allows for remote networks (with private addresses), residing behind NAT routers and/or firewalls, to communicate freely with each other. When building the VPN tunnels, throughout the network, they must be assigned as a fully meshed network. This means that every network is allowed direct connection to each and every other network in the topology. Network equipment limitations may sometimes restrict this ability resulting in no voice path on VoIP calls between sites. When this happens Peer-to-Peer must be disabled in the SL2100. The downside to disabling Peer-to-Peer is using more DSPs and consumption of additional bandwidth at the MAIN location.

The following diagram shows three sites connected together via VPN. This network is not fully meshed due to the lack of a VPN tunnel between Sites B and C.

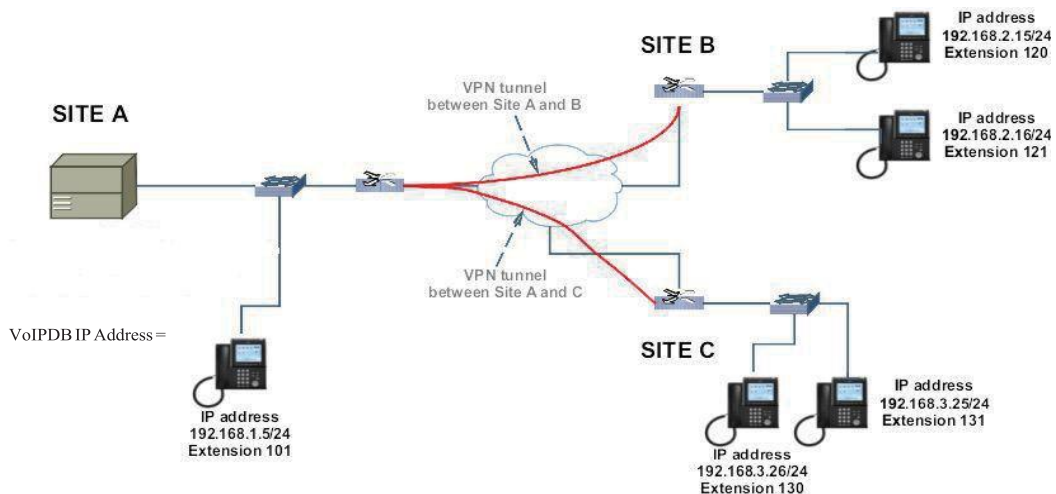


Figure 9-25 NEC SL2100 Network Example No. 2

With Peer-to-Peer enabled, the IP phones on site A can communicate with IP phones on sites B and C. IP Phones on sites B and C cannot communicate directly with each other though. The IP phone from site B can set up a call to the IP phone at site C, but there is no speech path. Here are the steps in the call scenario leading to the failed call.

- Extension 120 goes off hook and dials ext 130.
- An initial invite message is sent from 192.168.2.15 (ext 120) to 192.168.1.10 (VoIPDB).
- 192.168.1.10 (VoIPDB) forwards that message to 192.168.3.26 (ext 130).
- In the original setup message there is a field labeled SDP (Session Description Protocol). The SDP portion informs the IP phone where to send the media (voice) to. The SDP portion of this invite message contains the IP address of 192.168.2.15 (ext 120).
- 192.168.3.26 (ext 130) sends a 200 OK message to 192.168.1.10 (VoIPDB). In the 200 OK message is the SDP field reporting the IP address of 192.168.3.26 (ext 130).
- 192.168.1.10 (VoIPDB) forwards this message to 192.168.2.15 (ext 120).
- 192.168.2.15 (ext 120) sends an ACK message to 192.168.1.10 (VoIPDB).
- 192.168.1.10 (VoIPDB) forwards this message to 192.168.3.26 (130).
- At that point the two IP phones attempt to send voice packets directly to each other. As there is no VPN connection between these sites the call is set up with no voice path.

To correct this issue another VPN connection between sites B and C is required. If an additional VPN cannot be implemented, due to network limitations, the Peer-to-Peer feature can be disabled in the NEC SL2100. With Peer-to-Peer disabled, all packets (Signaling and Voice) route through the VoIPDB card. This also affects IP phones at the REMOTE locations calling other IP phones at the same location. Without Peer-to-Peer enabled the voice path must route to the MAIN location and then back to the REMOTE instead of directly between the two stations on the REMOTE network. This forces the use of additional bandwidth on the MAIN, and REMOTE locations. Peer-to-Peer is disabled in command 15-05-50 per IP Phone.



Figure 9-26 IP System Operation Setup

13.9 Guide to Feature Programming

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
10-12-03	CPU Network Setup – Default Gateway	VoIPDB uses the Default Gateway that is assigned here.	0.0.0.0~ 126.255.255.254 128.0.0.1~ 191.255.255.254 192.0.0.1~ 223.255.255.254 Default is 0.0.0.0	X		
10-12-09	CPU Network Setup – IP Address	Assign Layer 3 IP Address to the VoIPDB connected to CPU.	0.0.0.0~ 126.255.255.254 128.0.0.1~ 191.255.255.254 192.0.0.1~ 223.255.255.254 Default is 172.16.0.10	X		
10-12-10	CPU Network Setup – Subnet Mask	Assign Subnet Mask to the VoIPDB connected to CPU.	Default is 255.255.0.0	X		
84-26-01	VoIPDB Basic Setup – IP Address	Assign an IP Address for the VoIPDB DSP's.	Default Values: Slot 1 = 172.16.0.20	X		
84-26-02	VoIPDB Basic Setup – RTP Port Number		Range: 0 ~ 65534 Default Values: VoIP GW1 = 10020			X
84-26-03	VoIPDB Basic Setup – RTP Port Number (RTP Port Number +1)		Range: 1 ~ 65535 Default Values: VoIP GW1 = 10021 VoIP GW2 = 10053 VoIP GW3 = 10085 VoIP GW4 = 10117 VoIP GW5 = 10149 VoIP GW6 = 10181 VoIP GW7 = 10213 VoIP GW8 = 10245			X
10-46-01	IP MLT Server Information Setup – Register Mode	Define which of the three Registration modes you wish the SIP MLTs to use. Plug and Play When the phone boots up it will report the ext assigned in the phone or choose the next available extension in the system. No password required. Auto If set to auto then the SIP user name and password must be entered into the actual IP phone. These settings have to match Programs 84-22/15-05-27 or the phone does not come on-line. Manual When the phone boots up it prompts you to enter a user ID and password before logging in. It checks this user ID/password against Programs 84-22/15-05-27. If there is not a match, the phone does not come on-line.	0 = Plug and Play 1 = Automatic 2 = Manual Default is 0		X	
10-46-04	IP MLT Server Information Setup – Server Name	USER ID of the SIP URL if Program 10-46-05 is set to domain name. A SIP URL is made up of three parts. Domain name, host name, and server name. e.g. At default the server name is sipphd. The URL could look like the following: sipphd@voipu.nec.com	Up to 32 characters. Default is sipphd		X	

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
10-46-06	IP MLT Server Information Setup – Register Port	Port the SIP messages are sent to on the VoIPU card. This same port number must be assigned in the SIP Multiline terminals. Changing this command also requires a CPU reset.	Range = 0 ~ 65535 Default is 5080			X
10-46-07	IP MLT Server Information Setup – Encryption Mode	Enable or disable encryption mode.	0 = Off 1 = On 1 = Default		X	
10-46-08	IP MLT Server Information Setup – Encryption Type	Assign the encryption type.	0 = Mode 1 Default is 0 READ ONLY		X	
10-46-09	IP MLT Server Information Setup – One-Time Password	Password used when Program 10-46-07 is set to ON. Assign a character string of 10 characters or less.	Valid Characters (0-9, *, #) Default Not assigned		X	
10-46-10	IP MLT Server Information Setup – Start Port	With Automatic logon the starting port number for automatic port allocation.	Range = (1 ~ 128) Default = 1		X	
15-05-01	IP Telephone Terminal Basic Data Setup – Terminal Type	Type of IP terminal registered with the specified extension number.	1 = H.323 2 = SIP 3 = None 4 = SIP MLT Default is 3 READ ONLY			X
15-05-02	IP Telephone Terminal Basic Data Setup – Terminal MAC Address	Allow association of a MAC Address to an extension. When the IP phone sends a register message to the CPU the CPU responds back with the extension number associated to the MAC address.	00.00.00.00.00.00~ FF.FF.FF.FF.FF.FF Default is 00.00.00.00.00.00		X	
15-05-07	IP Telephone Terminal Basic Data Setup – Using IP Address	IP address the IP Terminal is using for the specified extension number.	0.0.0.0~ 255.255.255.255. Default is 0.0.0.0 READ ONLY			X
15-05-15	IP Telephone Terminal Basic Data Setup – CODEC Type	Assign CODEC type for IP Terminal. If SIP SLT, use Program 84-19. If SIP MLT, use Program 84-24.	1 = Type 1 2 = Type 2 3 = Type 3 4 = Type 4 5 = Type 5 1 = Default is 1		X	
15-05-20	IP Telephone Terminal Basic Data Setup – Bottom Option Information	Read Only CM showing type of adapter installed on the ITH-style telephone.	0 = No Option 1 = ADA 2 = BHA Default is 0 READ ONLY			X
15-05-26	IP Telephone Terminal Basic Data Setup – IP MLT Terminal Type	Assign type of SIP MLT terminal connected.	0 = Not Set 1 = Not Used 2 = ITL Series-12/24 Button without 8LK Unit 3 = Not Used 4 = Not Used 5 = Softphone 6 = CTI 7 = Not Used 8 = Not Used 9 = IP4WW-24TIXH Default is 0 10 ~ 14 = Not Used 15 = ITZ-**LDG/ITZ-**LD 16 = ITY-6D 17 = ITY-8LDX 18 = IP7WW-8IPLD-C1			X

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
15-05-27	IP Telephone Terminal Basic Data Setup –Personal ID Index	For SIP Multiline phone using Manual/ Auto registration. Assign each phone a unique personal index. When complete go to command 84-22 and set the user name and password.	0 = Not Set 1-128 = Set Default is 0		X	
15-05-28	IP Telephone Terminal Basic Data Setup –Additional Information Setup		0 = Disable 1 = Enable Default is 0		X	
15-05-29	IP Telephone Terminal Basic Data Setup –Using Router		0.0.0.0 ~ 255.255.255.255 Default is 0.0.0.0 READ ONLY		X	
15-05-30	IP Telephone Terminal Basic Data Setup –DTMF Play During Conversation at Receive Extension		0 = Disable 1 = Enable Default is 0			X
15-05-31	IP Telephone Terminal Basic Data Setup – Alarm Tone During Conversation (RTP packet loss alarm)		0 = Disable 1 = Enable Default is 1			X
15-05-33	IP Telephone Terminal Basic Data Setup – Using IP Address		0.0.0.0~ 255.255.255.255 Default is 0.0.0.0 READ ONLY			X
15-05-35	IP Telephone Terminal Basic Data Setup – Encryption Mode On/Off		0 = Off 1 = On Default is 0 READ ONLY			X
15-05-36	IP Telephone Terminal Basic Data Setup – IP MLT Firmware Version		00.00.00.00~ FF.FF.FF.FF Default is 00.00.00.00 READ ONLY			X
15-05-38	IP Telephone Terminal Basic Data Setup – Paging Protocol Mode	Sets the protocol mode for the Paging function.	0 = Multicast 1 = Unicast 2 = Auto Default is 0			X
15-05-39	IP Telephone Terminal Basic Data Setup – CTI Override Mode		0 = Disable 1 = Enable Default is 0			X
15-05-40	IP Telephone Terminal Basic Data Setup – Calling Name Display Info via Trunk for Standard SIP		0 = Both Name and Number 1 = Name only 2 = Number only 3 = None Default is 0			X
15-05-41	IP Telephone Terminal Basic Data Setup – Time Zone (Hour)		0~24 (-12 ~ +12 hour) Default is 12			X
15-05-43	IP Telephone Terminal Basic Data Setup – Video Mode		0 = Disable 1 = Enable Default is 0			X
15-05-44	IP Telephone Terminal Basic Data Setup – Using STD-SIP Display for CPN		0 = Disable 1 = Enable Default is 0			X

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
15-05-45	IP Telephone Terminal Basic Data Setup – NAT Plug and Play	Effective when Program 10-46-14 is set to NAT Mode. Select sending RTP port number to remote router, use from negotiation result (0) or received RTP packet (1).	0 = Off 1 = On Default is 0			X
15-05-47	IP Telephone Terminal Basic Data Setup – Registration Expire Timer for NAT	On a per station basis, this setting defines the SIP registration expiry timer. If this value is set to 0, for a NAPT terminal, the value in Program 84-23-01 is applied.	0 = Disable 60 ~ 65535 (sec) Default is 180		X	
15-05-48	IP Telephone Terminal Basic Data Setup – Subscribe Expire Timer for NAT	On a per station basis, this setting defines the SIP Subscribe expiry timer. If this value is set to 0, for a NAPT terminal, the value in Program 84-23-02 is applied.	0 = Disable 60 ~ 65535 (sec) Default is 180		X	
84-10-XX	ToS Setup	Assignments deal with setting of the Layer 3 IP Header ToS field as it leaves the VoIPDB unit. Specify the protocol to assign the ToS field for, and select the populated field to conform to either IP Precedence or Differentiated Services. When setting IP Precedence, assign Priority, Delay, Throughput, and Reliability in Programs 84-10-01/02/03/04/05. When setting DiffServ, only assign the DSCP in Program 84-10-07.	Protocol Type 1 = Not Used 2 = Not Used 3 = Reserved 4 = H.323 5 = RTP/RTCP 6 = SIP 7 = Reserved 8 = SIP MLT 9 = SIP Trunk 10 = Reserved 11 = Reserved		X	
84-22-01	IP MLT Logon Information Setup – User ID	User ID for Manual or Auto registration (Program 10-46-01).	Assign up to 32 Alpha/ Numeric Characters Default is No Setting		X	
84-22-02	IP MLT Logon Information Setup – Password	Password for Manual or Auto registration (Program 10-46-01).	Assign up to 16 Alpha/ Numeric Characters Default is No Setting		X	
84-22-03	IP MLT Logon Information Setup – User ID Omission	When set to manual login mode, the user ID is omitted from the display during entry by the user.	0 = Off 1 = On Default is 0		X	
84-22-04	IP MLT Logon Information Setup – Log Off	Allow the ability to log off from the IP terminal when using manual registration mode.	0 = Off 1 = On Default is 1		X	
84-22-05	IP MLT Logon Information Setup – Nickname	Assign up to 32 Alpha/Numeric characters.	Assign up to 32 Alpha/ Numeric Characters Default is No Setting		X	
84-23-01	IP MLT Basic Information Setup – Registration Expire Timer	At half the value of this timer the IP terminal sends another registration message to the CPU.	Range: 60~65535 Sec. Default is 180		X	
84-23-02	IP MLT Basic Information Setup – Subscribe Expire Timer	At half the value of this timer the IP terminal sends another Subscribe message to the CPU.	Range: 60~65535 Sec. Default is 3600		X	
84-23-03	IP MLT Basic Information Setup – Session Expire Timer	At half the value of this timer the IP terminal sends a re-invite message.	Range: 0~65535 Sec. Default is 180		X	
84-23-04	IP MLT Basic Information Setup – Minimum Session Expire Timer	Minimum time the CPU accepts a session timer for a new call.	Range: 0~65535 Sec. Default is 180		X	

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
84-23-05	IP MLT Basic Information Setup – Invite Expire Timer	When INVITE message received from SIP MLT does not contain Expires header, the CPU uses this value for timeout of outgoing call. E.g. The SIP MLT hears RBT for duration of this timer and then is disconnected.	Range: 0~65535 Sec. Default is 180		X	
84-23-06	IP MLT Basic Information Setup – Signal Type of Service	Used for updating the IP terminals SIGNALING TOS values.	Range: 0x00 ~ 0xFF Default is 00		X	
84-23-07	IP MLT Basic Information Setup – Error Display Timer	The time that an IP terminal holds an error message in the display. Setting 0 holds the error message indefinitely.	Range: 0 ~ 65535 Sec. Default is 0		X	
84-23-08	IP MLT Basic Information Setup – Digest Authorization Registration Expire Timer	When Digest Authentication mode is ON, this value is available. After receiving Initial INVITE without authentication information, CPU will send 401 message to the SIP MLT, then waits for an INVITE message with the authentication message from SIP MLT within this timer. Additionally, after receiving Re-REGISTER message for Keep Alive purpose, the CPU sends a 401 message.	Range: 0 ~ 4294967295 Default is 0			X
84-23-10	IP MLT Basic Information Setup – Number of Password Retries	The number of times an incorrect password can be entered when the security key is pressed. If set to (1), only one attempt is allowed. When number of password retries is met an error message displays on the phone: Incorrect security code password entered, press call key to contact an administrator	Range: 0 ~ 255 Default is 0		X	
84-23-11	IP MLT Basic Information Setup – Password Lock Time	Time to leave the terminal Locked Out after entering the wrong security code.	Range; 0 ~ 120 Default: 0 Default is 0		X	
84-23-12	IP MLT Basic Information Setup – Reference Number	Assign the network admin telephone number. When the user presses the Call key to contact the network administrator, this number is dialed.	Up to 32 Digits (0~9, *, #, P, R, @) Default is No Setting		X	
84-23-13	IP MLT Basic Information Setup – Media Type of Service	Assign the IP terminals MEDIA TOS values.	Range: 0x00 ~ 0xFF (0~9, A~F) Default is 00		X	
84-23-14	IP MLT Basic Information Setup – Refer Expire Timer	The valid period of the REFER subscription.	Range: 0 ~ 65535 Sec. Default is 60			X
84-24-01	IP MLT CODEC Basic Information Setup – Number of G.711 Audio Frames	Amount of audio in each RTP packet.	Range: 1~4 1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms Default is 2		X	
84-24-02	IP MLT CODEC Basic Information Setup - G.711 Silence Detection Mode	Select whether to compress silence with G.711. When there is silence, the RTP packet is not sent. When VAD is enabled the CPU will stop sending packets but the IP Phone will continue to transmit silence packets.	0 = Disable 1 = Enable Default = 0			X

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
84-24-03	IP MLT CODEC Basic Information Setup – G.711 Type	μ-law used in N.A.	0 = A-law 1 = μ-law Default is 1		X	
84-24-04	IP MLT CODEC Basic Information Setup – G.711 Jitter Buffer Minimum	Minimum value of the dynamic jitter buffer.	Range: 0 ~ 255ms Default is 20		X	
84-24-05	IP MLT CODEC Basic Information Setup – G.711 Jitter Buffer Average	Average value of the dynamic jitter buffer.	Range: 0 ~ 255ms Default is 40		X	
84-24-06	IP MLT CODEC Basic Information Setup – G.711 Jitter Buffer Maximum	Maximum value of the dynamic jitter buffer.	Range: 0 ~ 255ms Default is 80		X	
84-24-07	IP MLT CODEC Basic Information Setup – Number of G.729 Audio Frames	Amount of audio in each RTP packet.	Range: 1~4 1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms Default is 2		X	
84-24-08	IP MLT CODEC Basic Information Setup – G.729 Voice Activity Detection	Select whether to compress silence with G.729. When there is silence, the RTP packet is not sent. When VAD is enabled the CPU will stop sending packets but the IP Phone will continue to transmit silence packets.	0 = Disable 1 = Enable Default is 0			X
84-24-09	IP MLT CODEC Basic Information Setup – G.729 Jitter Buffer Minimum	Minimum value of the dynamic jitter buffer.	0~300ms Default is 20		X	
84-24-10	IP MLT CODEC Basic Information Setup – G.729 Jitter Buffer Average	Average value of the dynamic jitter buffer.	0~300ms Default is 40		X	
84-24-11	IP MLT CODEC Basic Information Setup – G.729 Jitter Buffer Maximum	Maximum value of the dynamic jitter buffer.	0~300ms Default is 80		X	
84-24-17	IP MLT CODEC Basic Information Setup – Jitter Buffer Mode		1 = Static 2 = Not used 3 = Adaptive immediate Default is 3		X	
84-24-18	IP MLT CODEC Basic Information Setup - Voice Activity Detection Threshold		0 ~ 30 Default is 20		X	
84-24-28	IP MLT CODEC Basic Information Setup – Audio Capability Priority	This assign the CODEC to be used.	Range: 0~3 0 = G.711_PT 1 = Not Used 2 = G.729_PT 3 = G.722_PT Default is 0		X	
84-24-32	IP MLT CODEC Basic Information Setup – G.722 Audio Frame Number	Amount of audio in each RTP packet.	Range: 1~4 1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms Default is 3		X	

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
84-24-34	IP MLT CODEC Basic Information Setup – G.722 Jitter Buffer Minimum	Minimum value of the dynamic jitter buffer.	Range: 0 ~ 255ms Default is 30		X	
84-24-35	IP MLT CODEC Basic Information Setup – G.722 Jitter Buffer Average	Average value of the dynamic jitter buffer.	Range: 0 ~ 255ms Default is 60		X	
84-24-36	IP MLT CODEC Basic Information Setup – G.722 Jitter Buffer Maximum	Maximum value of the dynamic jitter buffer.	Range: 0 ~ 255ms Default is 120		X	
84-28-01	IP MLT Firmware Name Setup – Firmware Directory	Maximum 64 characters.	Default is No Setting		X	
84-28-02	IP MLT Firmware Name Setup – Firmware File Name	Maximum 30 characters.	Default is No Setting		X	

13.10 SIP MLT Quick Startup Guide

The following guides describe the setup for a SIP MLT from a default state for these modes:

- Plug and Play
- Automatic Registration
- Manual Registration

13.10.1 Plug and Play

1. Program 10-12

Assign the VoIPDB registration/signaling IP address, subnet mask, and default gateway. If no customer provided default gateway is provided, leave Gateway IP address at 0.0.0.0.

System Data
10-12 : CPU Network Setup

01 - IP Address: 0.0.0.0

02 - Subnet Mask: 255.255.255.0

03 - Default Gateway: 172.16.0.1

04 - Time Zone: (GMT -05:00) Eastern Time (US and Canada)

05 - NIC Setting: Automatic detection

07 - NAPT Router IP Address: 0.0.0.0

08 - ICMP Redirect:

09 - VOIPDB IP Address: 172.16.0.10

10 - VOIPDB Subnet Mask: 255.255.0.0

11 - VOIPDB NIC Setting: Automatic detection

Figure 9-27 System Data 10-12: CPU Network Setup

2. Program 84-26
Assign the IP addresses that the DSP is going to use. The IP address assigned must be in the same subnet as the address in Program 10-12-09.
After these commands are uploaded to the CPU, a system reset must be applied.



System Data
84-26 : VOIPDB Basic Setup (DSP)

VoIP Gateway	IP Address	RTP Port	RTCP Port
1	172.16.0.20	10020	10021

Figure 9-28 System Data 84-26: VoIPDB Basic Setup (DSP)

3. Program 11-02

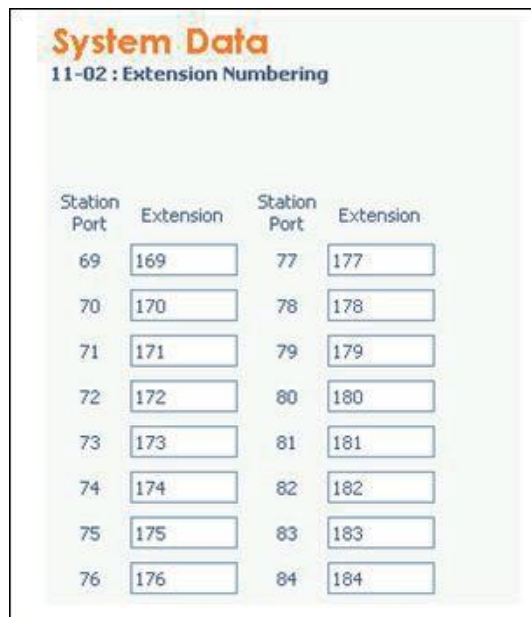
SIP MLT Stations are assigned to non-equipped hardware ports.

Physical Station ports are assigned automatically from lowest number ascending as cards are added to the system.

Because of this you should assign SIP MLT Stations starting with the higher number ports. By default all Station Ports are assigned numbers in the SL2100. These are easily changed in Program 11-02 to the required station number as long as the leading digit/digits are set in Program 11-01 as Extension.

Ports are dedicated to VoIP stations in groups of 2. E.g. In the image below if port 84 (Extension 184) is used for a SIP MLT Station that group of 2 ports (Ports 83 and 84) is now dedicated to VoIP use only.

After one port in a block of two is used by a VoIP station, the remaining port can be used only for another VoIP Extension.



System Data
11-02 : Extension Numbering

Station Port	Extension	Station Port	Extension
69	169	77	177
70	170	78	178
71	171	79	179
72	172	80	180
73	173	81	181
74	174	82	182
75	175	83	183
76	176	84	184

Figure 9-29 System Data 11-02: Extension Numbering

4. This step is optional. To enable Key data and other station feature programming (before IP Phone is brought online) the extensions must be identified as IP Phones. Once checked in the IPPhone

List in PC-Pro, the extensions are available for selection in Program 15 and other station related Programs.

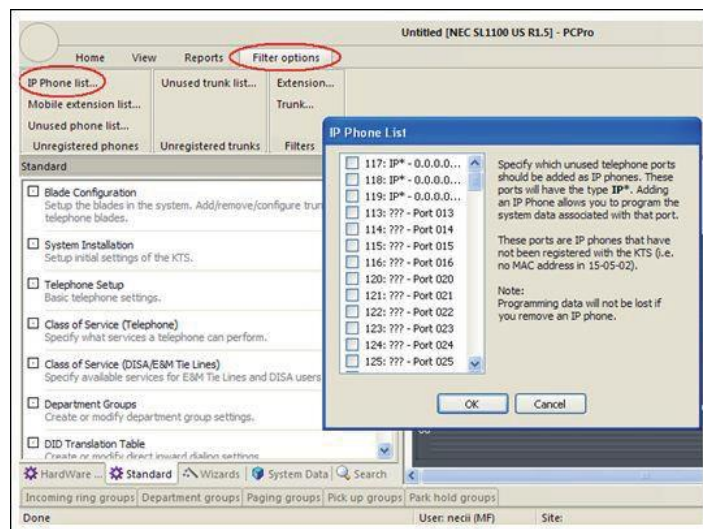



Figure 9-30 IP Phone List


- The SIP MLT Station requires assignments to be made in the phone itself. Enter the Program Mode in the station using the following steps.



 *The station does not require an Ethernet connection to enter the program mode. Only power is required. Power can be provided by POE provided by a data switch. If the data switch is providing POE it must be using the **802.3AF** standard.*

For Basic bench testing only the following assignments are required:

- At this point you are prompted with a User Name and Password. These are the defaults: User Name: **ADMIN**
Password: **6633222**

 *The user name should already be entered in the terminal.*

- Press **Set** soft key to step down to the password field.
- After you enter the password, press **OK** soft key.

Network Settings

- DHCP Mode – DHCP Disable. Click **OK**.
- IP Address – Enter the IP Address for the station, and click **OK**.
- Default Gateway – Enter the Default Gateway Address, and click **OK**. If you are testing without a router/gateway, this must be left at the default 0.0.0.0
- Subnet Mask - Enter the Subnet Mask for the station, and click **OK**.

SIP Settings

- SIP User – Intercom Number
Enter the extension number for the IP station, and click **OK**.
- Server Address & URI – 1st Server Address
Enter the IP address assigned in command 10-12-09, and click **OK**.
- SIP Server Port - 1st Server Port
Enter port 5080, and click **OK**.
- Press the **EXIT** key until you are back at the Main menu.

- Press the **SAVE** key and the phone saves the configuration to memory, reboots itself and registers with the CPU.

13.10.2 Automatic Registration

1. Steps 1~3 are the same as for Plug and Play mode. Step 4 is not optional and **MUST** be assigned when using Automatic Registration.
2. Same as Plug and Play mode.
3. Same as Plug and Play mode.
4. To enable key data and other station feature programming before IP Phone is brought online, the extensions must be identified as IP Phones. Once checked in the IP Phone List in PC-Pro (see images below), the extensions are available for selection in Program 15 and other station related Programs.

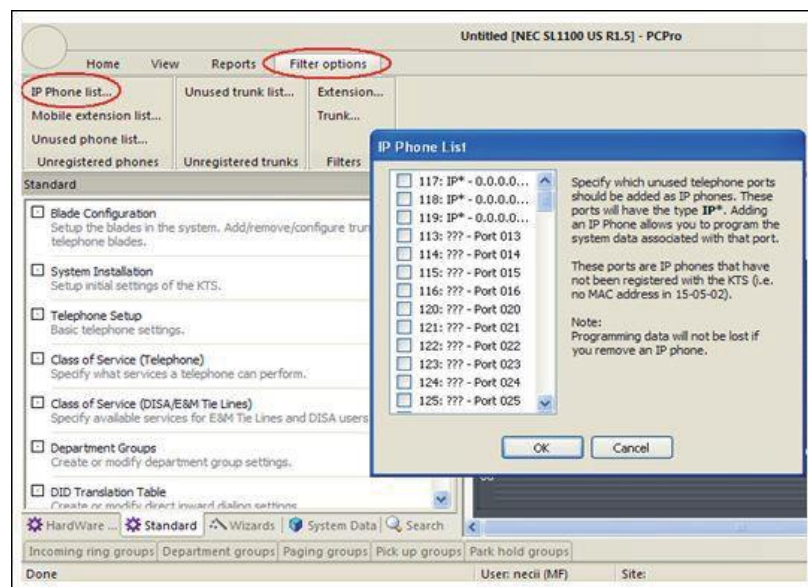


Figure 9-31 IP Phone List

5. Program 10-46
Change Program 10-46-01 to **Automatic**.



Figure 9-32 IP Multiline Terminal Server Information Setup

6. Program 15-05-27
Each IP phone requires a unique personal ID index. Valid settings are 1 ~ 512.



Figure 9-33 Automatic Registration Basic Setup



Figure 9-34 Automatic Registration Personal ID Index

7. Program 84-22-01
Assign the user ID and password to be associated with the Personal ID Index assigned in Step 6.

Personal ID Index	User Id	Password
001	1234	4321
002		
003		
004		
005		
006		
007		
008		

Figure 9-35 Automatic Registration User Name and Password Assignment

8. The SIP MLT Station requires assignments to be made in the phone itself. Enter the Program Mode in the station using the following steps.



- The station does not require an Ethernet connection to enter the program mode. Only power is required. Power can be provided by an AC adapter plugged into the phone or by POE provided by a data switch. If the data switch is providing POE it MUST be using the 802.3AF standard.
For Basic bench testing, only the following assignments are required:

- At this point, you are prompted with a User Name and Password. These are the defaults: User Name: **ADMIN**
Password: **6633222**

- The user name should already be entered in the terminal.

- Press **Set** soft key to step down to the password field.
- After you enter the password, press **OK** soft key.

Network Settings

- DHCP Mode - DHCP Disable. Click **OK**.
- IP Address - Enter the IP Address for the station, and click **OK**.
- Default Gateway - Enter the Default Gateway Address, and click **OK**. If you are testing without a router/gateway, this must be left at the default 0.0.0.0.
- Subnet Mask - Enter the Subnet Mask for the station, and click **OK**.

SIP Settings

- SIP User
 - **User ID** - Enter User ID assigned in command 84-22. Click **OK**.
 - **Password** - Enter the password assigned in command 84-22. Click **OK**.
 - **Incom Number** - Enter the extension number for the IP station. Click **OK**.
- Server Address & URI - 1st Server Address
Enter the IP address assigned in command 10-12-09, and click **OK**.
- SIP Server Port - 1st Server Port
Enter port 5080. Click **OK**.
- Press the **EXIT** key until you are back at the Main menu.
- Press the **SAVE** key, and the phone saves the configuration to memory, reboots itself and registers with the CPU.

13.10.3 Manual Registration

Steps 1~4 are the same as for Section [Automatic Registration](#).

1. Same as for Automatic Registration Mode.
2. Same as for Automatic Registration Mode.
3. Same as for Automatic Registration Mode.
4. Same as for Automatic Registration Mode.
5. Program10-46 – ChangeProgram10-46-01 to **Manual**.

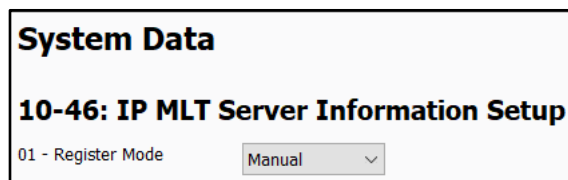



Figure 9-36 IP Multiline Terminal Server Information Setup


6. Same as for Automatic Registration Mode.
7. Same as for Automatic Registration Mode.

8. The SIP MLT Station requires assignments to be made in the phone itself. Enter the Program Mode in the station using the following steps.



 *The station does not require an Ethernet connection to enter the program mode. Only power is required. Power can be provided by an AC adapter plugged into the phone or by POE provided by a data switch. If the data switch is providing POE it must be using the **802.3AF** standard. For Basic bench testing only the following assignments are required.*

- At this point, you are prompted with a User Name and Password. These are the defaults: User Name: **ADMIN**
Password: **6633222**

 *The user name should already be entered in the terminal.*

- Press **Set** soft key to step down to the password field.
- After you enter the password, press **OK** soft key.

Network Settings

- DHCP Mode - DHCP Disable. Click **OK**.
- IP Address - Enter the IP Address for the station, and click **OK**.
- Default Gateway - Enter the Default Gateway Address, and click **OK**. If you are testing without a router/gateway, this must be left at the default 0.0.0.0
- Subnet Mask - Enter the Subnet Mask for the station, and click **OK**.

SIP Settings

- Do not enter any information in the SIP user field. When the phone boots up, it requires a user name and password. These are preassigned in the system. When entered correctly, the phone is provided an extension number.
- Server Address & URI - 1st Server Address
Enter the IP address assigned in command 10-12-09, and click **OK**.
- SIP Server Port - 1st Server Port
Enter port 5080, and click **OK**.
- Press the **EXIT** key until you are back at the Main menu.
- Press the **SAVE** key, and the phone saves the configuration to memory, reboots itself and registers with the CPU.

13.11 IP Phone Relocation

The IP Phone Relocation feature gives users access to their IP telephone from any location by using the override login function. Users have the flexibility of logging into their IP Station in the office as well as remotely at the home office.

IP Phone Relocation Override

IP Phone Relocation is a feature for overriding the registration of an IP phone from various locations. To override the registration of an IP phone, you must have the login ID and Password of that IP phone.

Conditions

- Multiple IP Phones cannot use the same user ID and the same password at the same time.
- When a user is using multiple IP Phones at the same time, the user ID and password must be different for each phone.
- When a user is using SoftPhone (CTI mode) and controlling the IP Phone by this SoftPhone, the user ID and password should be different for the SoftPhone and IP Phone.
- An IP Phone (IP Phone and Soft phone) with DSS console cannot override another IP Phone.

- An IP Phone (IP Phone and Soft phone) with DSS console cannot be overridden from another IP Phone.
- The login ID and Password are programmed in Program 15-05-27 and Program 84-22.
- IP Phone Relocation can be used only in Manual Registration Mode.
- Two ports of the same terminal type (Program 15-05-26) cannot be assigned to the same Personal ID index (Program 15-05-27).
- When using Override with an active CTI connection, Program 15-05-39 must be enabled for the extensions that will be overridden. The overriding terminal must be of the same type and number of line keys as the terminal to be overridden. If the types of terminals and number of keys are different between overriding and overridden phones, the Telephony Service Providers (1st Party and 3rd Party) may not function properly.

Table 9-4 IP Phone Relocation

Program/Item No.	Description/ Selection	Assigned Data	Comments
10-46-01	IP MLT Server Information Setup – Register Mode	0 = Plug and Play 1 = Automatic 2 = Manual Default is 0	Set up the information of the IP Multiline Terminal Server. This Program is a system-wide setting.
15-05-27	IP Telephone Terminal Basic Data Setup – Personal ID Index	0~128 0 Default is 0	Used when the SIP Multiline telephone is using manual/ auto registration. Assign each phone a unique personal index. Then go to command 84-22 to assign the user name and password.
84-22-01	IP MLT Logon Information Setup – User ID	Up to 32 characters Default not assigned	Input the User ID when using manual or auto registration (Program 10-46-01).
84-22-02	IP MLT Logon Information Setup – Password	Up to 16 characters Default not assigned	Input the Password when using manual or auto registration (Program 10-46-01).
84-22-04	IP MLT Logon Information Setup – Log Off	0 = Off 1 = On Default is 1	Input the Personal ID from terminal automatically when log on again. If set to 0, IP Phone Relocation fails.

IP Single Line Telephone (SIP)

Section 1 INTRODUCTION

Session Initiation Protocol (SIP) Station feature provides Voice over Internet Protocol (VoIP) for IP stations. This feature is defined by the Internet Engineering Task Force (IETF) RFC3261.

SIP analyzes requests from clients and retrieves responses from servers, then sets call parameters at either end of the communication, handles call transfer and terminates. Typically, Voice over IP services are available from an SIP service provider.

With the VoIPDB up to 128 TDM talk paths are supported. This total may be shared among SIP stations or SIP trunks. Registered SIP stations and/or SIP trunks require a one-to-one relation with the VoIPDB DSP Resource. This is a required component of SIP implementation in the NEC SL2100. The NEC SL2100 VoIPDB contains a regular TCP/RTP/IP stack that can handle real-time media and supports industry standard SIP (RFC3261) communication on the WAN side.

For this feature, the VoIPDB is installed and assigned. The VoIPDB supports IP signaling for up to 128 (SIP Trunks and/or SIP Stations) and reduces the maximum capacity of system stations and/or Trunks in accordance with the number of registered SIP Stations.

The NEC SL2100 supports the following CODECS that are considered to provide toll-quality equivalent speech path.

The following voice compression methods are supported for the IP Station SIP feature:

- G.729. Low bandwidth requirement used on most Wide Area Network links.
- G.711. μ Law – High bandwidth requirement usually used on Local Area Networks.
- G.722 This CODEC is useful in fixed network, Voice over IP applications, where the required bandwidth is typically not prohibitive.
- G.726 is an ITU-T ADPCM speech-coded standard covering the transmission of voice at rates of 16-, 24-, 32-, and 40Kbps.

The SIP Station feature set supports the HOLD and TRF features based on RFC draft.

- Draft-IETF-sipping-service-examples-09.txt.
- Section 2.5 Draft-ietf-sipping-service-examples- (Transfer - Attended) 15.txt
- IETF RFC is defined as: Internet Engineering Task Force (RFC) Request for Comments.
- The SIP Station feature set supports the Message Waiting Indication (MWI) based on RFC3842.
- SIP INFO works independent from other DTMF methods such as RFC2833. This means SIP Terminals should send DTMF information by a single method, otherwise the system will receive both separately causing double digits.
- When PRG 15-05-49 is set to 2: Allowed while RTP is not available, SIP INFO will be received while RTP is not established. In-band method such as RFC2833 will be used once voice path is established.
- When PRG 15-05-49 is set to 1: Allowed any time, SIP INFO will be received whenever they arrive.

NAT Mode for SIP Phone

- NAT mode for SIP Phone which can not use SIP P2P mode and standard SIP video call feature uses P2P mode cannot establish in same system.
- When PRG 10-33-05 NAT mode for SIP phone is set to 1 - Enable, P2P mode for SIP Phone becomes always Off regardless PRG 15-05-50 setting.

- The system time can be provided using NTP time server updates to standard SIP terminals.
- When connecting multiple SIP Phones via NAT, PRG 15-05-18 has to be set to admit the registration of multiple SIP Phones which are using the same IP address. For example, if you had a STD SIP Terminal that had two lines registering with the same IP Address, you would need to flag PRG 15-05-18 for both Extension numbers.
- In the router/firewall that the SL2100 resides behind port forwarding is required. Port forwarding at the SIP Terminal end is not required as long as PRG 15-05-45 (Plug and Play) is enabled, which it is by default. The ports that must be forwarded to the SL2100 are as follows:
 - UDP Port 5070 **MUST** be forwarded to the IP Address assigned in PRG 10-12-09. UDP Ports 10020 ~ 10147 **MUST** be forwarded to the IP Address assigned in PRG 84-26-01.


Section 2 PROGRAMMING

2.1 Card Setup

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
10-03-01	IPL Configuration - VoIP Type	VoIPDB Type	0 ~ 3 = Not Used 4 = Built-in VoIP 5 = VoIPDB	X		
10-03-02	IPL Configuration - Number of Channel	VoIPDB Channel	Built-in VoIP = 8 VoIPDB = 16 ~ 128	X		
10-03-03	IPL Configuration - Number of Voice Channel	Voice Channel on VoIPDB DSP Resource	0 ~ 128 (Read Only)	X		

2.2 Configure VoIPDB Networking Information

The VoIPDB DSP's (PRG 84-26-01) should be connected to the same IP Subnet as the VoIPDB signaling address (PRG 10-12-09).

 *If any IP Address or NIC setting is changed, the system must be reset for the changes to take affect.*

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
10-12-03	CPU Network Setup – Default Gateway	Assign the IP Address for the Router.	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254 Default is 0.0.0.0	X		
10-12-09	CPU Network Setup – IP Address	Assign the IP Address of the VoIPDB.	0.0.0.0 ~ 126.255.255.254 128.0.0.13~191.255.255.254 192.0.0.1~223.255.255.254 Default is 172.16.0.10	X		
10-12-10	CPU Network Setup – Subnet Mask	Assign the Subnet Mask of the VoIPDB.	255.255.0.0 Default is 255.255.0.0	X		

2.2.1 VoIPDB (DSP) Basic Setup

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
84-26-01	VoIP Basic Setup – IP Address	Assign the IP Address for the DSP resource. Note: The VoIPDB IP Addresses must be statically assigned.	Default: Slot 1 = 172.16.0.20	X		
84-26-02	VoIP Basic Setup – RTP Port Number	Assign the RTP Port Number.	0~65534 Default for DSP1 is 10020			X
84-26-03	VoIP Basic Setup – RTCP Port Number (RTP Port Number + 1)	Assign the RTCP Port Number.	0~65534 Default for DSP1 is 10021			X

2.2.2 VoIP ToS Setup

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
84-10-01	ToS Setup – ToS Mode	Use this field to define your SIP QoS marking for ToS or Diffserv. When Input Data is set to 1, Item No. 07 is invalid. When Data is set to 2, Item No. 02 ~ 06 are invalid.	0 = Disabled (Invalid) 1 = IP Precedence 2 = Diffserv Default is 0		X	

2.2.3 SIP Peer to Peer

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
15-05-50	IP Telephone Terminal Basic Data Setup – Peer to Peer Mode	Enable or disable Peer-to-Peer mode for SIP phones. When PRG 10-33-05 NAT mode is set to 1 (Enable), P2P mode for Sip phones always set to Off automatically regardless of this program setting.	0 = No (Disable) 1 = Yes (Enable) (default is 0)		X	

2.2.4 IP Extension Numbering

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
11-01-01	System Numbering	Refer to the SL2100 Programming Manual for all options and default settings.	1 = 3 Digit; Intercom Default is 3 Digit; Intercom	X		
11-02-01	Extension Numbering	Assign up to eight digits for extension numbering	Dial (Up to eight digits) Default Ports 1~84 = 101~184	X		

2.2.5 SIP Extension CODEC Information

Program Number	Program Name	Description/ Comments	Assigned Data	1	2	3
84-19-01	SIP Extension CODEC Information Basic Setup – Number of G.711 Audio Frames	Define the G.711 audio Frame Size	1–4 1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms Default is 2		X	
84-19-02	SIP Extension CODEC Information Basic Setup – G.711 Voice Activity Detection Mode	Enable/Disable Voice Activity Detection for G.711.	0 = Disable 1 = Enable Default is 0			X
84-19-03	SIP Extension CODEC Information Basic Setup – G.711 Type	Define the G.711 Type – μ -law is recommended in USA.	0 = A-law 1 = μ -law Default is 1			X
84-19-04	SIP Extension CODEC Information Basic Setup – G.711 Jitter Buffer (min)	Define G.711 Jitter Buffer minimum accepted value.	0–300ms Default is 20			X
84-19-05	SIP Extension CODEC Information Basic Setup – G.711 Jitter Buffer (Average)	Define G.711 Jitter Buffer setting.	0–300ms Default is 40			X
84-19-06	SIP Extension CODEC Information Basic Setup – G.711 Jitter Buffer (max)	Define G.711 Jitter Buffer maximum accepted value.	0–300ms Default is 80			X
84-19-07	SIP Extension CODEC Information Basic Setup – Number of G.729 Audio Frames	Define the G.729 audio Frame Size.	1–6 1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms 5 = 50ms 6 = 60ms Default is 2		X	
84-19-08	SIP Extension CODEC Information Basic Setup – G.729 Voice Activity Detection Mode	Enable/Disable Voice Activity Detection for G.729.	0 = Disable 1 = Enable Default is 0			X
84-19-09	SIP Extension CODEC Information Basic Setup – G.729 Jitter Buffer (min)	Define G.711 Jitter Buffer minimum accepted value.	0–300ms Default is 20			X
84-19-10	SIP Extension CODEC Information Basic Setup – G.729 Jitter Buffer (average)	Define G.729 Jitter Buffer setting.	0–300ms Default is 40			X
84-19-11	SIP Extension CODEC Information Basic Setup – G.729 Jitter Buffer (max)	Define G.729 Jitter Buffer maximum accepted value.	0–300ms Default is 80			X
84-19-17	SIP Extension CODEC Information Basic Setup – Jitter Buffer Mode	Define the Jitter Buffer mode – supported Static or Immediate.	1 = Static 2 = Not used 3 = Adaptive Immediately Default is 3			X
84-19-18	SIP Extension CODEC Information Basic Setup – VAD Threshold	Define the VAD Threshold.	0–30 Default is 20			X
84-19-28	SIP Extension CODEC Information Basic Setup – Audio Capability Priority	Define Audio capability priority.	0 = G.711_PT 1 = Not Used 2 = G.729_PT 3 = G.722 4 = G.726 5 = Not Used Default is 0		X	

Program Number	Program Name	Description/ Comments	Assigned Data	1	2	3
84-19-33	SIP Extension CODEC Information Basic Setup – Number of G.722 Audio Frames		1~4 1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms Default is 3		X	
84-19-35	SIP Extension CODEC Information Basic Setup – G.722 Jitter Buffer (min)		0~255ms Default is 30			X
84-19-36	SIP Extension CODEC Information Basic Setup – G.722 Jitter Buffer (Average)		0~255ms Default is 60			X
84-19-37	SIP Extension CODEC Information Basic Setup – G.722 Jitter Buffer (max)		0~255ms Default is 120			X
84-19-38	SIP Extension CODEC Information Basic Setup –Number of G.726 Audio Frames		1~4 1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms Default is 3		X	
84-19-39	SIP Extension CODEC Information Basic Setup – G.726 Voice Activity Detection Mode		0 = Disable 1 = Enable Default is 0			X
84-19-40	SIP Extension CODEC Information Basic Setup – G.726 Jitter Buffer (min)		0~255ms Default is 30			X
84-19-41	SIP Extension CODEC Information Basic Setup – G.726 Jitter Buffer (Average)		0~255ms Default is 60			X
84-19-42	SIP Extension CODEC Information Basic Setup – G.726 Jitter Buffer (max)		0~255ms Default is 120			X
84-19-49	SIP Extension CODEC Information Basic Setup – RTP Filter		0 = Disable 1 = Enable Default is 1			X
84-19-65	SIP Extension CODEC Information Basic Setup – Video Quality Mode	This setup specifies the maximum capacity of video. Refer to following ※ about the definition in each mode.	0 = mode1 1 = mode2 Default is 0			
84-19-66	SIP Extension CODEC Information Basic Setup – Video codec		0 = H.264 Default is 0			
84-19-67	SIP Extension CODEC Information Basic Setup – Jitter Buffer Mode for Video	This setup specifies the jitter buffer mode of the video stream. Jitter buffer size adjustment method decides depending on the mode setting. Please set to 2 (Self adjusting) usually.	0 = Static 1 = Self Adjusting Default is 2			
84-19-68	SIP Extension CODEC Information Basic Setup – Minimum Jitter Buffer for Video	This setup specifies the minimum value of jitter buffer for the video stream. This value must be smaller than the value of the maximum jitter buffer.	0 ~ 1000 (ms) Default is 70			

Program Number	Program Name	Description/ Comments	Assigned Data	1	2	3
84-19-69	SIP Extension CODEC Information Basic Setup – Initial Jitter Buffer for Video	This setup specifies the initial value of jitter buffer for the video stream. This value must be smaller than the value of the maximum jitter buffer and be bigger than the value of the minimum jitter buffer.	0 ~ 1000 (ms) Default is 140			
84-19-70	SIP Extension CODEC Information Basic Setup – Maximum Jitter Buffer for Video	This setup specifies the maximum value of jitter buffer for the video stream. It is used only when "67-Jitter Buffer Mode for video" is 1:Fixed. This value must be bigger than the value of the minimum jitter buffer.	0 ~ 1000 (ms) Default is 210			

2.2.6 SIP Extension Basic Information Setup

Program Number	Program Name	Description/ Comments	Assigned Data	1	2	3
84-20-01	SIP Extension Basic Information Setup – Registrar/Proxy Port	Define SIP station Proxy Port.	1~65535 Default is 5070			X
84-20-02	SIP Extension Basic Information Setup – Session Timer Value	Define the periodic refresh time that allows both user agents and proxies to determine if the SIP session is still active.	0~65535 Default is 180			X
84-20-03	SIP Extension Basic Information Setup – Minimum Session Timer Value	Define to convey the minimum allowed value for the SIP session timer.	0~65535 Default is 180			X
84-20-04	SIP Extension Basic Information Setup – Called Party Info	Define the SIP Extension presented Caller ID information.	0 = Request URI 1 = To Header Default is 0			X
84-20-05	SIP Extension Basic Information Setup – Expire Value of Invite	Define the time out response value for SIP invite.	0~256 seconds Default is 180			X
84-20-06	Expire Value of Invite (send)	The expiration time is set for the Invite message.	1~3600 seconds Default is 180			X

2.2.7 IP Phone Configuration

Program Number	Program Name	Description/ Comments	Assigned Data	1	2	3
15-05-01	IP Telephone Terminal Basic Data Setup – Terminal Type	Review the type protocol support by the IP Phone. Viewing Only – No changes permitted.	0 = NGT 1 = H.323 2 = SIP 3 = MEGACO 4 = SIP-MLT READ ONLY Default = 3			X

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
15-05-02	IP Telephone Terminal Basic Data Setup – Terminal MAC Address	MAC Address of registered MLT SIP phone is stored and/or can input the MAC address of an MLT SIP phone so when it comes online it is provided with the extension in which the MAC address matches.	MAC address 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF Default is 00-00-00-00-00-00			X
15-05-07	IP Telephone Terminal Basic Data Setup – Using IP Address	Informational Only registered IP Phones	0.0.0.0~255.255.255.255 Default is 0.0.0.0			X
15-05-16	IP Telephone Terminal Basic Data Setup – Password	Assign the authentication password for SIP single line telephones. This program is valid when PRG 15-05-01 Terminal Type is set to 2. (2 = SIP)	Up to 24 characters Default not assigned		X	
15-05-18	IP Telephone Terminal Basic Data Setup – IP Duplication Allowed Group	If an adapter has one IP address coming into it but multiple extensions off of it, assign all extensions to a group so the CPU knows that the one IP address is assigned to multiple extensions.	0 = Not Used 1 = Group 1 2 = Group 2 3 = Group 3 4 = Group 4 5 = Group 5 6 = Group 6 7 = Group 7 8 = Group 8 9 = Group 9 10 = Group 10 Default is 0		X	
15-05-40	IP Telephone Terminal Basic Data Setup – Calling Name Display		0 = Both Name and Number 1 = Name only 2 = Number only 3 = None Default = 0			X
15-05-41	IP Telephone Terminal Basic Data Setup – Time Zone		0 ~ 24 (-12 ~ +12 hour) Default = 12			X
15-05-43	IP Telephone Terminal Basic Data Setup – Video Mode		0 = Disable 1 = Enable Default = 0			X
15-05-44	IP Telephone Terminal Basic Data Setup – Using STD-SIP Display for CPN		0 = Disable 1 = Enable Default = 0			X
15-05-49	IP Telephone Basic Setup - Receiving SIP INFO	Determines whether SIP INFO messages are received by the system.	0 = Disable 1 = Allowed any time 2 = Allowed while RTP is not available Default = 2			

2.2.8 NAT Mode for Standard SIP terminal

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
10-12-03	CPU Network Setup – Default Gateway	Assign the IP Address for the Router.	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254 Default is 0.0.0.0	X		
10-12-07	CPU Network Setup - NAPT Router IP Address (Default Gateway [WAN])	Define the IP Address of the WAN side of the router.	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254 Default is 0.0.0.0	X		

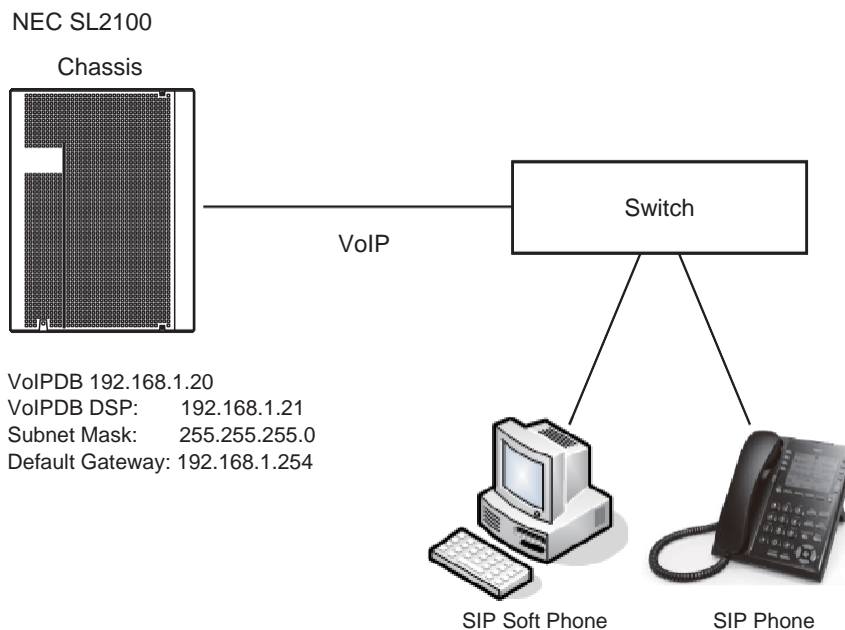
Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
10-12-08	CPU Network Setup - ICMP Redirect	When receiving ICMP redirect messages, this determines if the IP Routing Table updates automatically or not.	0 = Enable 1 = Disable Default is 0		X	
10-12-09	CPU Network Setup – IP Address	Assign the IP Address of the VoIPDB.	0.0.0.0 ~ 126.255.255.254 128.0.0.13~191.255.255.254 192.0.0.1~223.255.255.254 Default is 172.16.0.10	X		
10-12-10	CPU Network Setup – Subnet Mask	Define the Media Gateway Subnet Mask Address.	128.0.0.0 192.0.0.0 224.0.0.0 240.0.0.0 248.0.0.0 252.0.0.0 254.0.0.0 255.0.0.0 255.128.0.0 255.192.0.0 255.224.0.0 255.240.0.0 255.248.0.0 255.252.0.0 255.254.0.0 255.255.0.0 255.255.128.0 255.255.192.0 255.255.224.0 255.255.240.0 255.255.248.0 255.255.252.0 255.255.254.0 255.255.255.0 255.255.255.128 255.255.255.192 255.255.255.224 255.255.255.240 255.255.255.248 255.255.255.252 255.255.255.254 255.255.255.255 default is 255.255.0.0	X		
10-12-11	CPU Network Setup - NIC Setup	Define the LAN interface speed and mode of the VoIP application supported.	0 = Auto Detect 1 = 100Mbps, Full Duplex 2 = 10Mbps, Full Duplex 3 = 1Gbps, Full Duplex default is 0	X		
15-05-50	IP System Operation Setup – SIP Peer to Peer Mode	Enable or disable Peer-to-Peer mode for SIP phones. When PRG 10-33-05 NAT mode is set to 1 (Enable), P2P mode for SIP phones always set to Off automatically regardless of this program setting.	0 = No (Disable) 1 = Yes (Enable) default is 0		X	
10-33-02	SIP Registrar/Proxy Information Basic Setup – Authentication Mode	When connecting STD SIP Terminal via NAT, this option must be enabled to prohibit illegal SIP phone registration.	0 = No (Disable) 1 = Yes (Enable) default is 1	X		
10-33-05	SIP Registrar/Proxy Information Basic Setup NAT Mode	When system controls remote SIP phone via NAT router, set this program to 1 = Enable.	0 = No (Disable) 1 = Yes (Enable) default is 0	X		

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
10-37-01	UPnP Setup – UPnP Mode	Default Gateway (WAN), PRG 10-12-07 can be set automatically when this program is set to 1 = Enable.	0 = No (Disable) 1 = Yes (Enable) default is 0		X	
10-58-01	Network Address – Network Address	If there are other networks connected to this system that are not to be routed through NAPT translations, then these networks must be identified in PRG 10-58. Use this PRG to assign the individual IP Address (e.g. 192.168.1.100) or assign the whole network address (e.g. 192.168.1.0).	Assign a valid IP Address or assign a valid Network Address. default is 0.0.0.0		X	
10-58-02	Network Address – Subnet Mask	If there are other networks connected to system that are not to be routed through NAPT translations, then these networks must be identified in PRG 10-58. Use this PRG to assign the subnet mask for the IP Address entered in PRG 10-58-01.	Assign a valid subnet mask. default is 0.0.0.0		X	
15-05-16	IP Telephone Terminal Basic Data Setup – Password	Assign the authentication password for SIP single line telephones. This program is valid when PRG 15-05-01 Terminal Type is set to 2. (2 = SIP)	Up to 24 characters Default not assigned	X		
15-05-45	IP Telephone Terminal Basic Data Setup- NAT Plug & Play	Per IP Single line telephone, enable NAT Plug and Play so that port forwarding is NOT required in the router the IP single line telephone resides behind. Effective only when PRG 10-46-14 is set to 1 = Enable.	0 = No (Disable) 1 = Yes (Enable) default is 1	X		
15-05-47	IP Telephone Terminal Basic Data Setup – Registration Expire Timer for NAT	On a per station basis, this setting defines the SIP registration expiry timer. If this value is set to 0, for the terminal, the value in PRG 84-23-01 is applied.	0 = User Timer in Program 84-23-01 60~65535(sec) default is 180 seconds		X	
15-05-48	IP Telephone Terminal Basic Data Setup – Subscribe Expire Timer for NAT	On a per station basis, this setting defines the SIP subscribe expiry timer. If this value is set to 0, for the terminal, the value in PRG 84-23-02 is applied.	0 = User Timer in Program 84-23-01 60~65535(sec) default is 180 seconds		X	
84-26-01	VoIPDB Basic Setup – IP Address	Assign the IP Address for each DSP resource on the VoIPDB	xxx.xxx.xxx.xxx Default: Slot 1 = 172.16.0.20	X		
84-26-02	VoIPDB Basic Setup – RTP Port Number	Assign the RTP Port Number.	0~65534 Default for DSP1 is 10020			X
84-26-03	VoIPDB Basic Setup – RTCP Port Number	Assign the RTCP Port Number.	0~65535 Default for DSP1 is 10020~10147			X

2.2.9 NTP Time Server

Program Number	Program Name	Description/Comments	Assigned Data	1	2	3
10-65-01	NTP Server	Set 1 when you want to start the NTP Server.	0 = Disable (Stop) 1 = Enable (Start) default is 0 (Stop)			
10-65-02	NTP Server Port	Set the receiving port of the NTP Server.	1 ~ 65535 default is 123			

2.3 SIP Phone Example



Section 3 IP Single Line Telephone (SIP) - TLS Connection Support

3.1 Description

With Ver 2.00 or higher, TLS protocol is supported on STD SIP terminals. The SIP message encryption acts only between "SL2100 and STD SIP terminals".

By default, the TLS Registrar/Proxy Port in Program 84-20-07 is set to 0. To register a STD SIP terminal using TLS it is necessary to assign the TLS Registrar/Proxy Port.

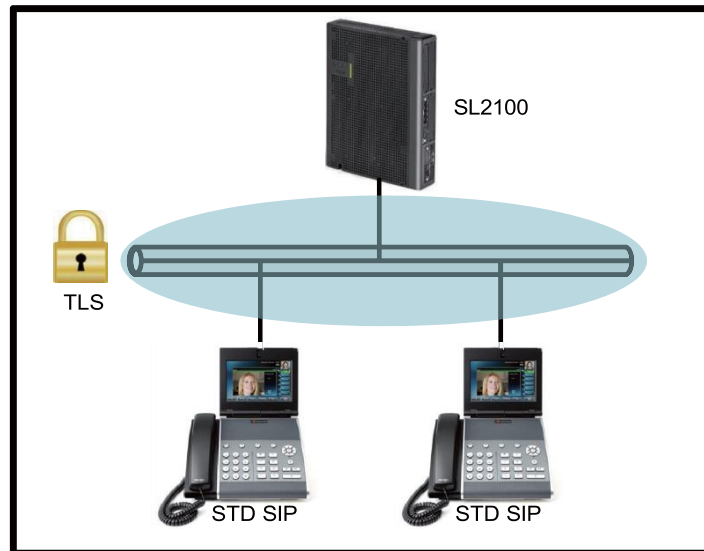


Figure 10-1 TLS Configuration

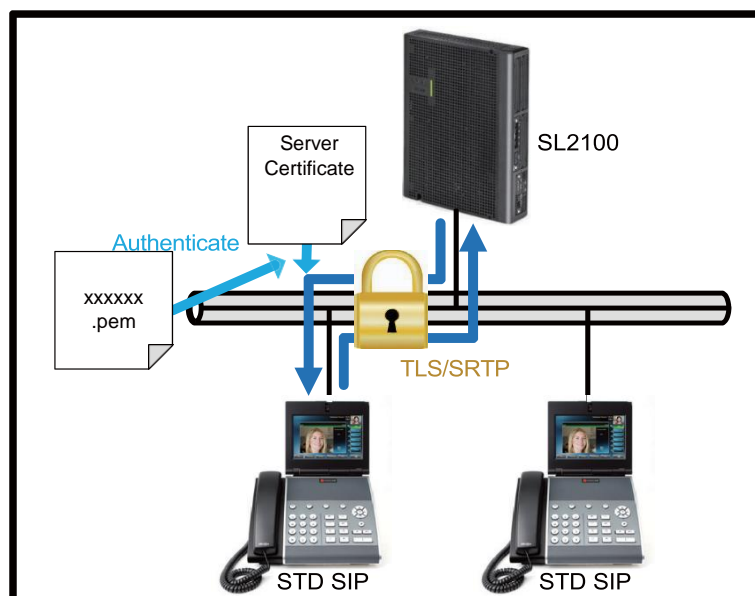


Figure 10-2 SL2100 Authentication

3.1.1 Conditions

- NAT Traversal is supported.
- The TLS STD SIP terminals do not support P2P call even if P2P settings are programmed.
- This feature does not support the terminals which do not use REGISTER method (Program 15-24-04).
- A real Encryption License (0030) is required as it is not included in Free License.
- DNS server is required for ST500, to match with the Domain when the Certificate is authenticating.

TLS Support

- The SIP signaling packets between SL2100 and TLS STD SIP terminals are encrypted.

- The TLS connection is disconnected in the following cases:
 - Reset of SL2100
 - Restart of STD SIP terminal
 - Network Disconnection

SL2100 Certificate and Private Key

- Registered certificate on SL2100 is used when SL2100 receives a request for TLS connection.
- If no certificate file name is set in Program 10-72 then SL2100 uses self-signed certificate for TLS connection.
- Only the certificate consisting of "PEM format" is supported. The extension of certificate file is ".pem" or ".PEM" and the extension of private key file is ".key" or ".KEY".
- The file name can consist of a maximum of 32 characters including the extension.
- The SL2100 system retains "certificate" and "key" files even after system restart and cold start.
- The "Certificates" and "Keys" will be saved in "CERT" folder.
- The certificates can be checked, added and deleted by Web Programming under "Certificate Registration".
- Only IN level User can use "Certificate Registration" on Web Programming.
- "Certificate Registration" is not displayed when SA level or UA level user logs in.
- If server certificate and private key file name set in Program 10-72 are not registered with SL2100, the STD SIP cannot be registered using TLS.
- If the private key file name set in Program 10-72-02 is invalid, the STD SIP cannot be registered using TLS.
- The import of CA certificate on different terminal are explained in the following table:

Table 10-1 Import CA Certificate Requirements

Terminal	Certificate Format	Certificate Import Method
Polycom	<ul style="list-style-type: none"> • Format PEM • Extension .pem or.crt 	A certificate is downloaded from a file server (FTP, TFTP and Web Server) and the certificate is imported.
ST500 (iOS)	<ul style="list-style-type: none"> • Format PEM • Extension .pem or.crt 	<ul style="list-style-type: none"> • A certificate is attached to a mail and the certificate of attached file is imported. • A link of a certificate file is chosen from a web browser and the certificate is imported. • Android only - Its possible to import a certificate from microSD.
ST500 (Android)	<ul style="list-style-type: none"> • Format PEM • Extension .crt 	
ITX-3370-1[]()TEL	<ul style="list-style-type: none"> • Format PEM 	<ul style="list-style-type: none"> • A certificate is imported via the Web GUI. • Open a certificate on your PC with text editor. • Copy CA certificate / private key / private key password, and paste it to the Web GUI.

- The conditions of a TLS connection:

Table 10-2 TLS Certificate Conditions

Terminal	CA Certificate of a Terminal	Note
Polycom/ST500/ITX-3370-1	<ul style="list-style-type: none"> • A valid and relevant CA Certificate should be used. 	If Domain Name is used for CN in a certificate then DNS server is required.

SRTP Support

- Voice Encryption acts between SL2100 and STD SIP terminals.
- To encrypt voice packets, it is necessary to enable SRTP Mode (Program 84-27-03 "enable").
- The behavior of SIP message encryption and voice packets encryption depend on both Program 15-05-51 and Program 84-27-03 shown below:

Table 10-3 SIP Message Encryption

Program 15-05-51 (Read Only) Transport Protocol	Program 84-27-03 SRTP Mode	Behavior
TLS	1: Enable	SIP messages and the voice packets are encrypted.
	0: Disable	SIP messages are encrypted, voice packets are not.
UDP/TCP	1: Enable	SIP messages and voice packets are not encrypted.
	0: Disable	

- When a TLS registered STD SIP terminal calls to a non TLS registered STD SIP terminal or SIP MLT, the call will be non-P2P even if P2P settings are programmed and SRTP is enabled.
- If SRTP mode is enabled, the VoIP resource is not decreased.
- Alarm 74 display on Multiline terminal set in program 90-50-01 are shown below:

Table 10-4 Example of Terminal Display Alarms

Error	Cause	Correction	Display
License not available	Encryption license not installed.	License check passes. (When the TLS connection is re-established or a TLS SIP call is initiated.)	TLS ALM (P:00) No License
Error in Server Certificate (Program 10-72-01)	Failed to validate Server Certificate.	When SL2100 receives offer of TLS connection, after setting correct file in Program 10-72-01.	TLS ALM (P: 00) Cert Err02
Error in Private Key (Program 10-72-02)	Failed to validate Private Key.	When SL2100 receives offer of TLS connection, after setting correct file in Program 10-72-01.	TLS ALM (P: 00) Cert Err03

- DIM command for TLS can be enabled.

DIM Command	Description
SIPTLS DEBUG 1	TLS Connection
SIPTLS DEBUG 2	Encrypted Message Dump
SIPTLS DEBUG 3	SRTP Negotiate

3.1.2 Default Settings

None

3.2 System Availability

3.2.1 Terminals

- Polycom VVX500 (v5.9.7.12459)
- ST500
- ITX-3370-1

3.2.2 Required Component(s)

- Built-In VoIP (CPU) /VoIPDB
- SL2100 Ver 2.00
- SL2100 ENCRYPTION LIC

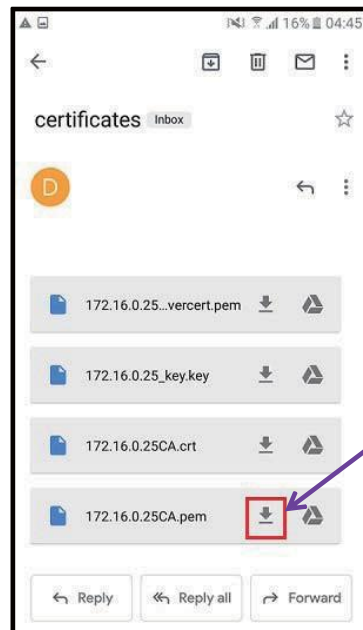
3.2.3 CA Certificate import on ST500 (Smartphone)

The CA certificate on ST500 can be imported by using:

- Mail Server
- Micro SD card
- Webserver

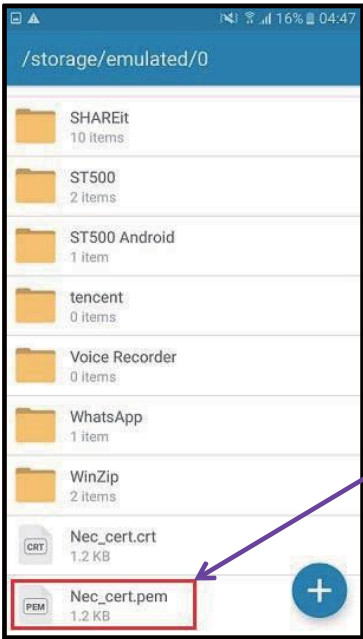
Using Mail Server

- Attach the CA certificate to a mail and send it to ST500 user's mail address.
- ST500 users access the mail account on android device where ST500 is installed, and check the mail having CA certificate.
- Now Click on the attached CA Certificate to download the CA certificate.



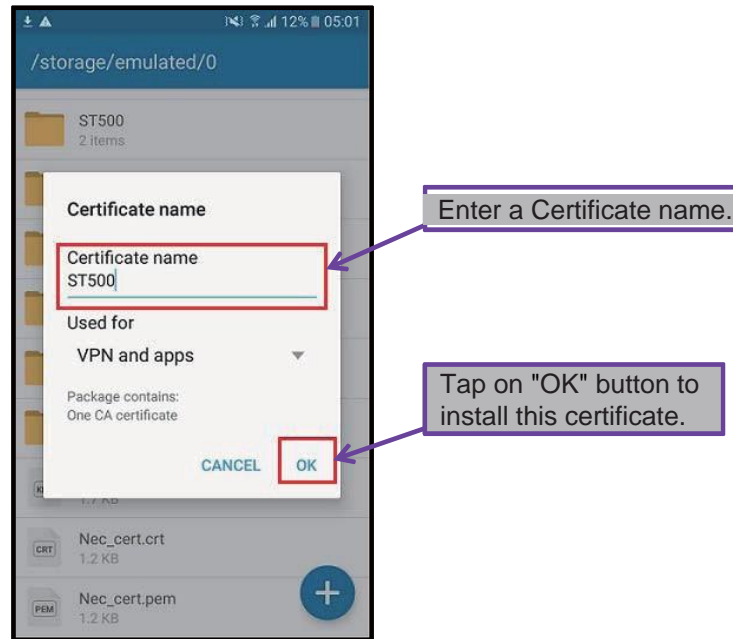
Open the Mail having CA certificate and click on "Download" button to save the certificate to Phone's local memory.

- CA certificate is downloaded in local memory space in device of ST500.

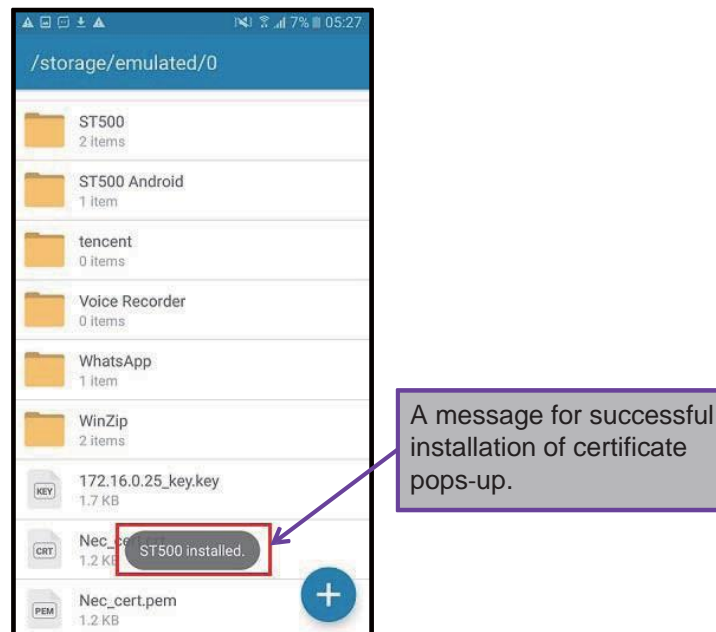



To install the certificate tap on the Saved CA certificate.

- Enter a Certificate name and click on "OK" button to install the certificate.



- After successful installation of certificate, a success message POPs-UP.

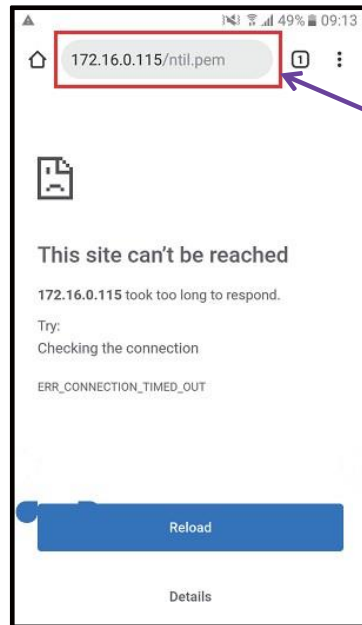


 *The installed certificates can be viewed under User of "Security Certificates".*

Using WEB-Server

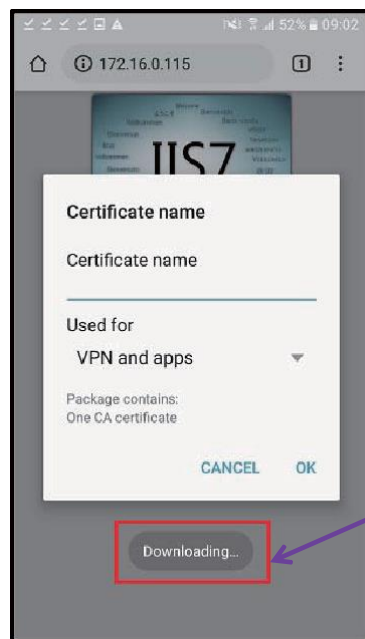
- Place the CA certificate in root directory of WEB-Server.
ST500 users access the WEB-Server on android/iOS device's browser where ST500 is installed.

- Now enter the URL to access the certificates.



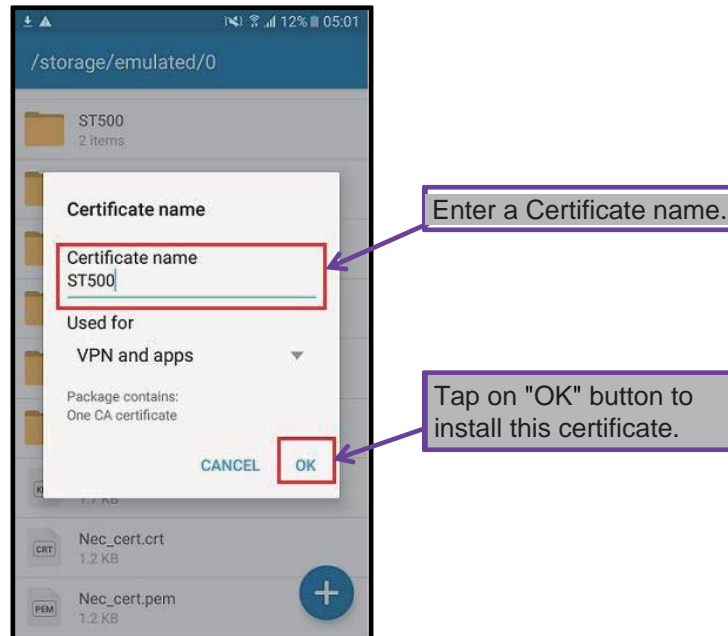
Enter the URL (http://ip/path/filename.pem) in the browser.

- CA certificate is downloaded to the device.

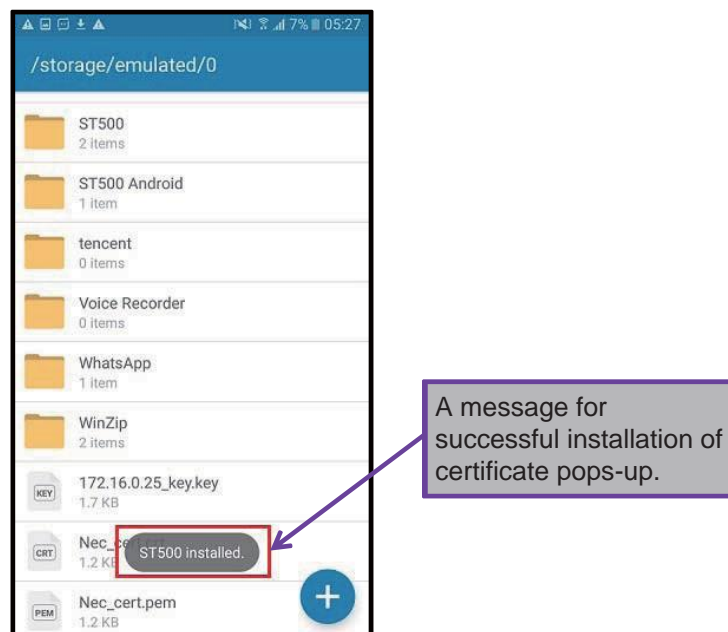



An informational POP-UP that CA certificate is downloading.

- Enter a Certificate name and click on "OK" button to install the certificate.



- After successful installation of certificate, a success message POPs-UP.

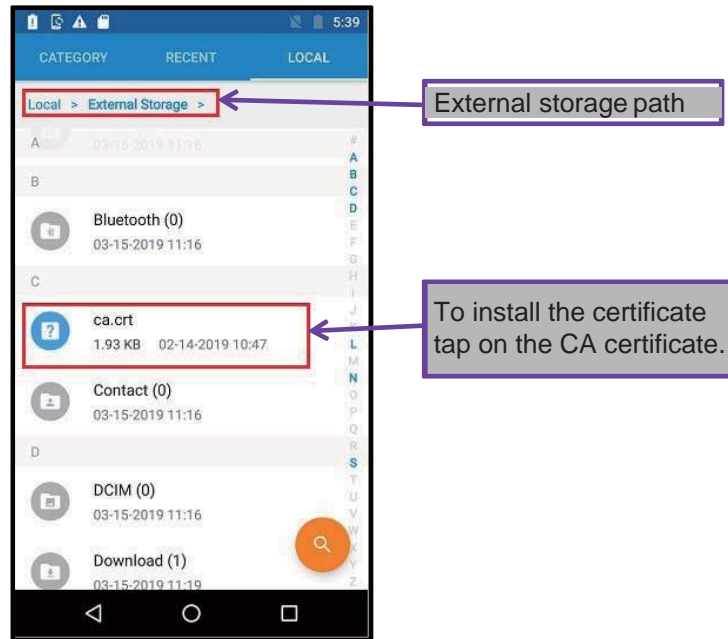


 *The installed certificates can be viewed under User of "Security Certificates (Android)".*

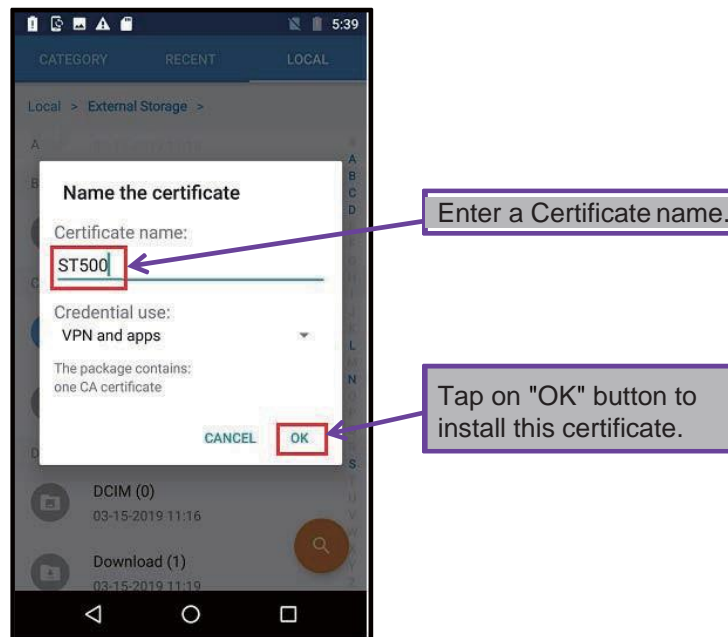
Using SD Card

- Go to the External storage path where the SD card Placed.

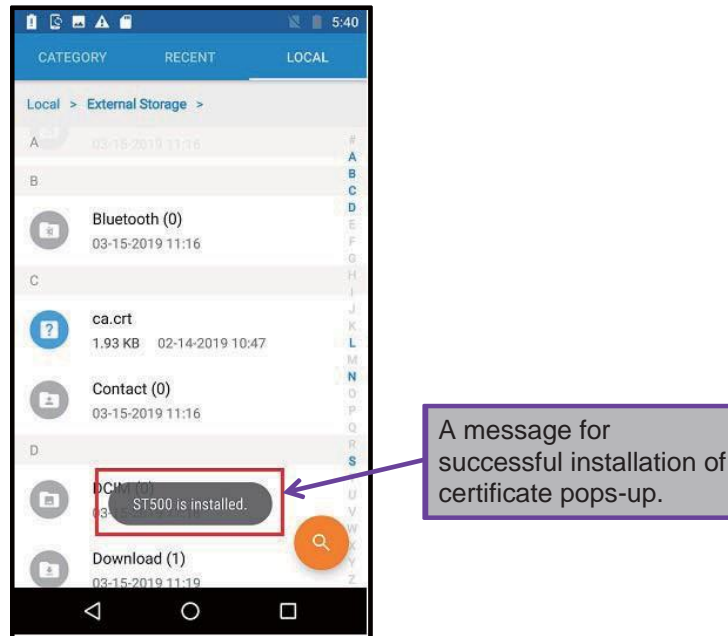
- Tap on the CA certificate to install it.




- Enter a Certificate name and click on "OK" button to install the certificate.



- After successful installation of certificate, a success message POPs-UP.



 The installed certificates can be viewed under User of "Security Certificates (Android)".

3.2.4 Import CA Certificate on Polycom VVX500

- The CA certificate on Polycom VVX500 can be imported using:
 - FTP Server
 - TFTP Server
 - Web Server
- Open the web management interface of the Polycom VVX500 and browse to the **Settings** -> **Network** -> **TLS** menu.
- Select the desired Application CA container and enter the URL to the certificate file using either FTP, TFTP or HTTP.
- The **Install** button should activate once a properly formatted URL is entered. Click **Install**, the device should report that the SSL certificate was successfully installed.

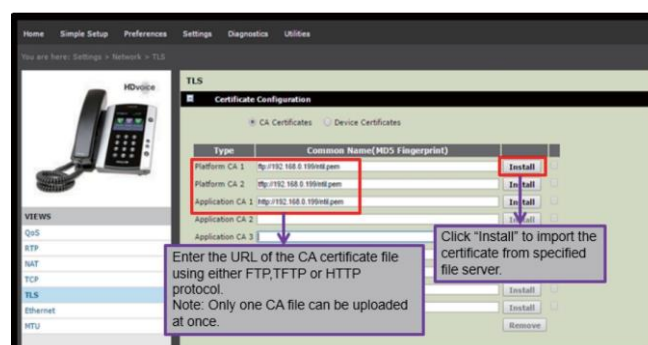


Figure 10-3 TLS Certificate Configuration Screen

After successful import of CA certificate the following screen appears:

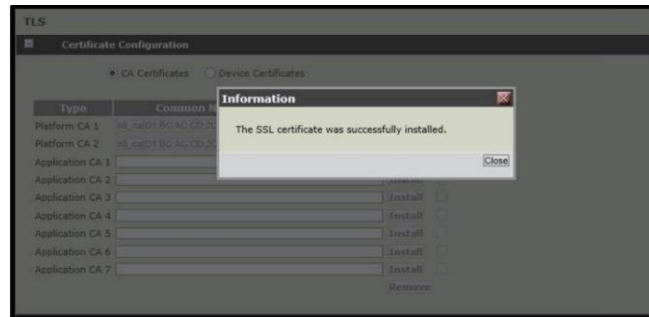


Figure 10-4 SSL Certificate Successfully Installed

The imported certificate is displayed.

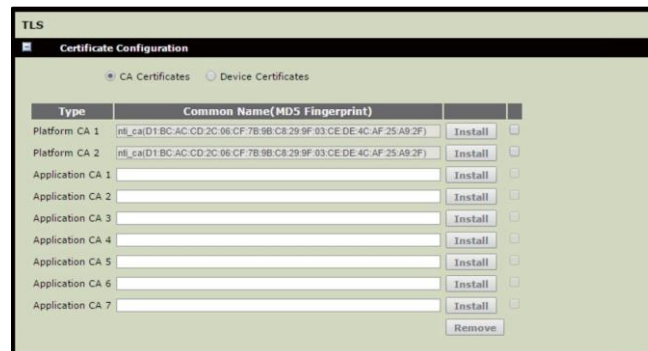


Figure 10-5 Example of Imported CA Certificates

3.2.5 Import CA Certificate on ITX-3370-1

- The CA certificate on ITX-3370-1W can be imported using the Web GUI.
- Refer to the IP Phone GT890 Administration Guide (ST500) - SIP-TLS section.

3.3 Guide to Feature Programming

Program No.	Program Name / Description	Input Data	Default
10-72-01	Network Security Setup - Server Certificate Assign the Server Certificate file's name for SL2100.	Maximum of 32 characters	No Setting
10-72-02	Network Security Setup - Private Key Assign the Private Key file's name for SL2100.	Maximum of 32 characters	No Setting
15-05-51	IP Phone Basic Setup - Transport Protocol Read only program that shows the transport protocol for selected SIP -terminal.	0 = UDP 1 = TCP 2 = TLS	0
84-27-03	VOIPDB Basic Setup - SRTP Mode Setup Enable/Disable SRTP mode to Enable/Disable voice packet encryption.	0 = Disable 1 = Enable	0
84-27-04	VOIPDB Basic Setup - SRTP Mode Select	0 = Mode1	0

Program No.	Program Name / Description	Input Data	Default
84-20-07	SIP Extension Basic Setup - TLS Registrar/Proxy Port Set the STD SIP port number (Receiving Transport for SL2100 SIP) for TLS. <i>When setting port number is 0, a port number does not open.</i>	0 ~ 65535	0
90-10-01	System Alarm Setup - Alarm Type Set the alarm type 74. Alarm 74 Set system alarm for TLS SIP error information.	0 = Not Set 1 = Major Alarm 2 = Minor Alarm	0
90-50-01	System Alarm Display Setup - System Alarm Display Telephone	Up to eight digits	No setting

3.4 Operation

3.4.1 Certificate Registration in Web Programming:

1. Login to Web Programming at IN level.

The screenshot shows the NEC SL2100 Web Programming interface. The left sidebar contains a menu with the following items: Session Management, System Initialization, Modification History, Trace Command Control, System Alarm, Data Download, Data Upload, Software Update, **Certificate Registration** (highlighted with a red box), License Upload, and InCapture. The main content area displays the 'Session Management' page with a table of active sessions:

User	Type	Access Level	Time of Login	Time of Last Activity	Logout
tech (this session)	Web	IN	28 Feb 01:21:43 2018	28 Feb 01:28:02 2019	

At the bottom of the interface, there is a status bar showing: User : tech, Access Level : IN, and Software Ver. : 01.99.06.




2. Click on **Certificate Registration**.

NEC
SL2100
Web Programming

- Session Management
- System Initialization
- Modification History
- Trace Command Control
- System Alarm
- Data Download
- Data Upload
- Software Update
- Certificate Registration
- License Upload
- InCapture

Certificate Registration

Upload file No file chosen

Certificate File	Start Date	Expiry Date	
server.key			
server.pem	Feb 5 12:17 2019 GMT	Feb 2 12:17 2029 GMT	
AmazonRootCA1.pem	Jun 29 17:39 204 GMT	Jun 29 17:39 2034 GMT	

"Delete" button is used to delete the registered certificate files.

User : tech Access Level : IN Software Ver. : 01.99.06

- Browse or Select the certificate file and click on **Upload** button.
If no file is selected or invalid extension is selected the error is displayed.
- A maximum of ten files can be registered and if registered files are 10 or more, an error message "There is no available space in the storage" is displayed.
- There is a list of the Certificate and Private Key files registered with SL2100 on the Certificate Registration page. "Start Date" and "Expiry Date" columns of Private Key file are displayed as blank.
- The page is reloaded if the certificate has been uploaded and the certificate file's name is displayed in the list.
- To delete, find the certificate file and select the **Delete** button located on the same line.

NAPT

Section 1 NAPT

1.1 Introduction

NAPT, or Network Address Port Translation, is a method by which a private address (or addresses) and their TCP/UDP ports are translated into a single public address and its TCP/UDP ports. In the case of IP phones with the SL2100 it allows their connection to a public (Internet) IP address which is then converted back to the private (non-Internet) IP address on the customer's network. The translation is available at the SL2100 end as well as at the remote IP Phone end of the connection if required.

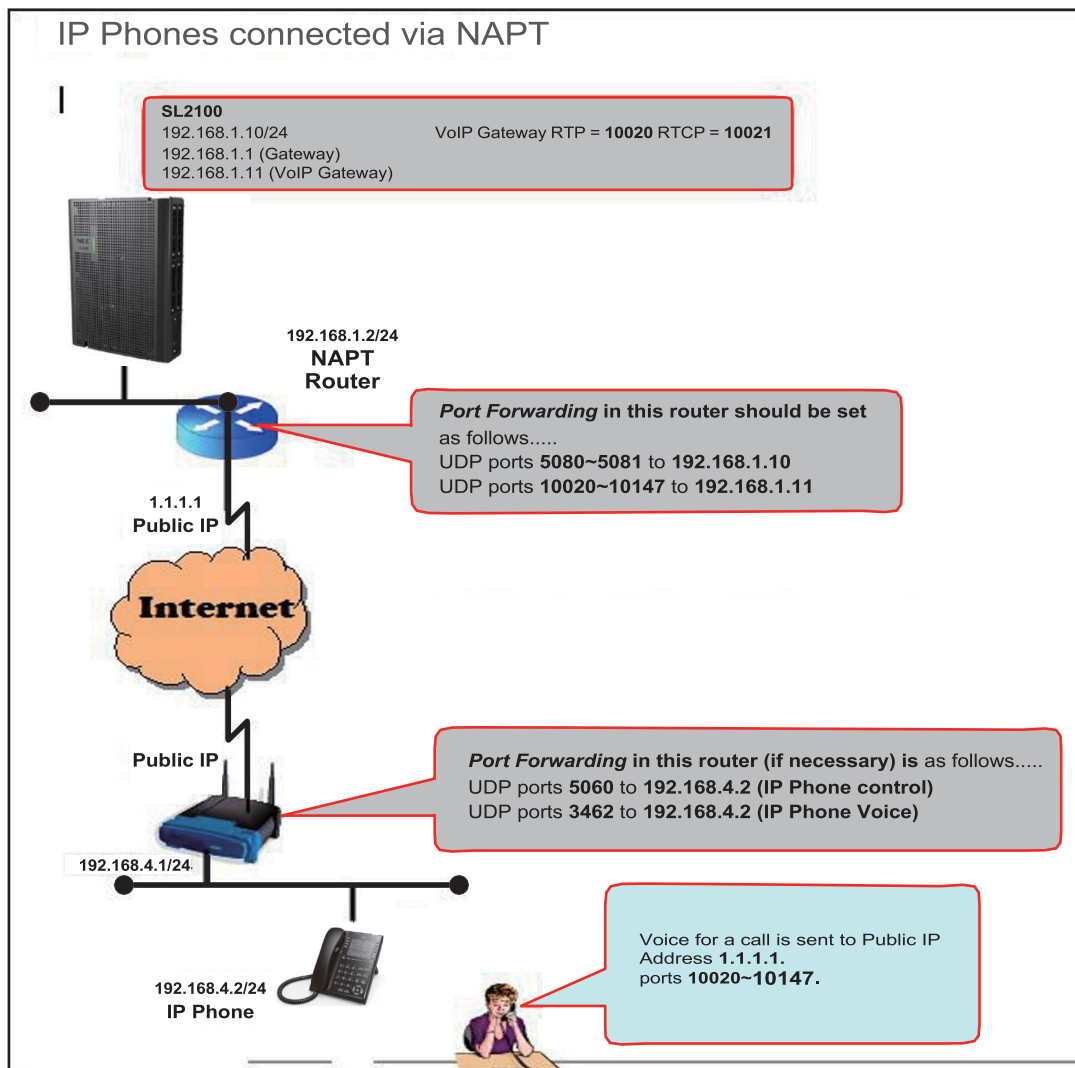


Figure 11-1 NAPT Configuration Example

1.2 SL2100 Requirements

The following information provides requirements for NAPT.

Main Software

NAPT is supported with the V1.00 or higher release of the SL2100.

Hardware

The SL2100 requires the following hardware:


- CPU (V1.00 or higher)
- VoIP Daughter Board

Capacity

A maximum of 112 IP phones can be connected.

1.3 Installation

The following settings have been added for NAT traversal in the IP Multiline Terminal.

 To enter IP phone programming at the terminal, press **HOLD, TRANSFER, *, #**. User name is **ADMIN** and password is **6633222 (NEC)**.

1.3.1 Settings for terminals

Setting location: 0. Config/ 2. SIP Settings/ 8. NAT Traversal

Number and Name of Setting	Setting Value	Default Value	Factory Value	Auto Config	Description
1. NAT Traversal Mode	1. Disable 2. Dynamic 3. Static	1. Disable	Available	Available	Settings for NAT Traversal: Disable: Disables NAT Traversal Dynamic: Performs NAT Traversal using a dynamic conversion table. Static: Performs NAT Traversal using a static conversion table and requires the WAN IP Address to be entered into the IP Terminal.
2. Network Area Name	A character string	No value	Available	Available	The name of the network area to which terminals belong. Specify up to 32 alphanumeric characters. Step is optional.
3. WAN Settings					See table below.

Setting location: 0. Config/ 2. SIP Settings/ 8. NAT Traversal/ 3. WAN Settings

Number and Name of Setting	Setting Value	Default Value	Factory Value	Auto Config	Description
1. WAN Mate IP Address	IP Address	0.0.0.0	Available	Available	WAN Address of the router that the SL2100 resides behind. This setting must match what is programmed in PRG 10-12-07.
2. WAN SIP Mate Port	1024~65535	5060	Available	Available	Port number the SL2100 uses for SIP registration in PRG 10-46-06.
3. WAN Self IP Address	IP Address	0.0.0.0	Available	Available	Only used when Static NAT is enabled. This setting is the WAN address of the router that the NAPT Terminal resides behind.

Setting location: 0. Config/ 1. Network Settings/ 6. Advanced Settings/ 5. Self Port Settings

Number and Name of Setting	Setting Value	Default Value	Factory Value	Auto Config	Description
1. RTP Self Port	1024-65528 (Even numbers only)	3462	Available	Not available	The number of the port receiving RTP data. At default this is assigned to port 3462. The First IP phone on this local LAN can use this port. The second IP phone would need to be changed to port 5062.
2. SIP Self Port	1024-65535	5060	Available	Not available	The number of the port receiving SIP data. At default this is assigned to port 5060. The first IP phone on this local LAN can use this port. The second IP phone would need to be changed to port 3464.

Section 2 CONDITIONS

- The NAPT feature supports CPU software V1.00 or higher.
- Terminals using NAPT must be at firmware V1.0.0.0 or higher.
- IP terminals can be connected via NAT router or WAN (direct connection).
- The NAT router on the SL2100 side must have a static WAN IP address.
- The software change Programs 15-05-47 and 15-05-48 to a shorter interval. These programs are changed on a per station basis. Non NAPT phones will still use Programs 84-23-01 and 84-23-02 while only NAPT phones will use Programs 15-05-47 and 15-05-48.
- It is necessary to set Program 10-46-14 to **OFF** when the VoIPDB is assigned a global (public) IP address.
- When Program 10-46-14 is set to **ON**, it references programs 10-58-01 and 10-58-02. These programs are used to define any destination networks that do not get sent through the NAPT translations.
- UDP ports in the remote routers may be required to be forwarded to the IP Terminals.
- NAPT can be used for SIP trunks and terminals on the same system.

Section 3 RESTRICTIONS

- With static NAT, the terminal needs a static IP Address assigned to it, or entries in the DHCP must be made to provide the same IP Address to the terminal.
- The NAT router on the terminal side must have the function for setting up static NAT.
- A conversion table must be manually set up for the NAT router on the terminal side.
- If installing multiple terminals in the domain of the NAT router on the terminal side, the RTP Self port and SIP Self port for each terminal must be specified so as to avoid overlapping.
- The SIP server cannot be switched. (Only one address can be registered as the SIP server.)

Dynamic NAT

- The NAT router on the terminal side must have the function for setting up dynamic NAT.
- It is assumed that port numbers are not changed by the NAT router on the terminal side. If a port number is changed by NAT router, NEC does not guarantee proper operation.
- If installing multiple terminals in the domain of the NAT router on the terminal side, the RTP Self port and SIP Self port for each terminal must be specified so as to avoid overlapping.
- The SIP server cannot be switched. (Only one address can be registered as the SIP server.)

Section 4 MINIMUM REQUIRED PROGRAMMING

The **Level 1**, **Level 2** and **Level 3** columns indicate the programs that are assigned when programming this feature in the order they are most commonly used. These levels are used with PCPro and WebPro wizards for feature programming.

- Level 1 – these are the most commonly assigned programs for this feature.
- Level 2 – these are the next most commonly assigned programs for this feature.
- Level 3 – these programs are not often assigned and require an expert level working knowledge of the system to be properly assigned.

Program Number	Program Name	Description/Comments	Assigned Data	Level		
				1	2	3
10-12-01	CPU Network Setup - IP Address	Assign the IP Address for the CPU's NIC card. If a VoIPDB is installed in the system it is recommended to set this to 0.0.0.0 and all connections to the system will be made through the VoIPDB.	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254 (default =192.168.0.10)	✓		
10-12-03	CPU Network Setup – Default Gateway	Assign the default gateway IP address for the CPU.	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254 (default = 0.0.0.0)	✓		
10-12-07	CPU Network Setup – NAPT Router IP Address (Default Gateway [WAN])	Define the IP Address of the WAN side of the router.	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254 (default = 0.0.0.0)	✓		
10-12-09	CPU Network Setup – IP Address	Assign the IP Address for the VoIPDB. If a VoIPDB is installed in the system it is recommended to set PRG 10-12-01 to 0.0.0.0 and all connections to the system will be made through the VoIPDB.	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 191.255.255.254 192.0.0.1 ~ 223.255.255.254 (default = 172.16.0.10)	✓		

Program Number	Program Name	Description/Comments	Assigned Data	Level		
				1	2	3
10-12-10	CPU Network Setup – Subnet Mask	Define the Media Gateway Subnet Mask Address.	128.0.0.0 192.0.0.0 224.0.0.0 240.0.0.0 248.0.0.0 252.0.0.0 254.0.0.0 255.0.0.0 255.128.0.0 255.192.0.0 255.224.0.0 255.240.0.0 255.248.0.0 255.252.0.0 255.254.0.0 255.255.0.0 255.255.128.0 255.255.192.0 255.255.224.0 255.255.240.0 255.255.248.0 255.255.252.0 255.255.254.0 255.255.255.0 255.255.255.128 255.255.255.192 255.255.255.224 255.255.255.240 255.255.255.248 255.255.255.252 255.255.255.254 255.255.255.255 (default = 255.255.0.0)	✓		
10-46-06	Register Port Assign the port number to which the SIP messages are sent to on the VoIPDB. This same port number must be assigned in the SIP Multiline terminals. If this command is changed, it requires a CPU reset.	0~65535	5080		✓	
10-46-13	Subscribe Session Port	0~65535	5081		✓	
10-46-14	NAT Mode	Turns On/Off the NAT mode of the system.	0 = Off 1 = On Default = Off	✓		
15-05-45	NAT Plug&Play	Effective when PRG 10-46-14 is set to NAT Mode. Select sending RTP port number to remote router, use from negotiation result (0) or received RTP packet (1).	0 = Off 1 = On Default = Off		✓	
15-05-47	IP Telephone Terminal Basic Data Setup - Registration Expire Timer for NAT	On a per station basis, this setting defines the SIP registration expiry timer. This setting only applies to IP Multiline Terminals connected via NAPT. If this value is set to 0, for a NAPT terminal, the value in PRG 84-23-01 is applied.	0 = Disable 60 ~ 65535 (sec) Default = 180		✓	
15-05-48	IP Telephone Terminal Basic Data Setup - Subscriber Expire Timer for NAPT	On a per station basis, this setting defines the SIP subscribe expiry timer. This setting only applies to IP Multiline Terminals connected via NAPT. If this value is set to 0, for a NAPT terminal, the value in PRG 84-23-02 is applied.	0 = Disable 60 ~ 65535 (sec) Default = 180		✓	

Program Number	Program Name	Description/Comments	Assigned Data	Level		
				1	2	3
84-26-01	VoIPDB Basic Setup (DSP)– IP Address	Assign the IP address for the VoIP Gateway.	Default = 172.16.0.20	✓		
84-26-02	VoIPDB Basic Setup (DSP)– RTP Port Number	Assign the RTP port number to be used for the DSP on the VoIPDB.	VoIP GW = 10020~10147	✓		
84-26-03	VoIPDB Basic Setup (DSP)– RTCP Port Number (RTP Port Number + 1)	Define the port number for RTCP to use for each DSP.	VoIP GW = 10021		✓	

All DSP Busy Indication

Section 1 INTRODUCTION

The All DSP Busy feature is used to alert users via telephone displays and/or Alarm reports when all DSP (VoIP) resources in the system are being used. This can be used to trouble shoot issues or to alert when the current hardware might need to be upgraded to a higher capacity.

Alarm Message Format:

The Alarm message for will vary depending on what type of resource is unavailable, and will be displayed on display telephones and included in reports.

Table 12-1 Alarm Types

Parameters	Description
STA	DSP for IP Station Calls Were All Busy.
TRK	DSP for Trunk Calls Were All Busy, includes SIP.

Alarm Report Example:

The report example below shows an alarm for all busy Station and Trunk DSPs.

```
<< ALARM REPORT >>                                01/22/2009 23:37
```

LVL	NO	STAT	DATE	TIME	ITEM	UNIT	SLT	PRT	PARAMETER
MAJ	0068	ERR	01/22/09	09:30	VoIP All DSP Busy	VoIPDB	01	00	STA
MAJ	0068	ERR	01/22/09	09:31	VoIP All DSP Busy	VoIPDB	01	00	TRK
MIN	0002	REC	01/22/09	09:32	PKG Installation	PRIU	02	00	

LCD Display

LCD Display Indication	Note
Clock/Calendar	XX = Slot number of CPU with VoIPDB.
VoIP All Busy XX	
Soft Key	

Section 2 SERVICE CONDITIONS

- When using IP Phones, the alarm is shown on both terminals involved in that call if they are both on the same system.
- The alarm cannot be displayed on Standard SIP Phones or Single Line phones.
- If a call from a Standard SIP telephone to a Multiline telephone cannot be established due to an All DSP Busy condition, the Multiline telephone will not display the "All DSP" busy message.
- If a SIP trunk call is sent to the SL2100 when all DSP resources are busy, the call is rejected but the alarm is not displayed on any system telephone.

- The default alarm setting is Minor.

Section 3 RELATED FEATURES

- IP Multiline Station (SIP)
- IP Trunk – (SIP) Session Initiation Protocol

Section 4 GUIDE TO FEATURE PROGRAMMING

Program Number	Program Name	Description/Comments	Assigned Data	Level		
				1	2	3
20-13-52	VoIP All DSP Busy Display	Set on a per station class of service basis, whether the "All DSP Busy" alarm displays on the LCD when the caller makes an IP call and there is no VoIP DSP resource.	0 = Off 1 = On (default = 1)	✓		
90-10-01	System Alarm Setup	Alarm Number 68 is used for All DSP Busy.	0 = Not set 1 = Major 2 = Minor (default = 2)		✓	

SL Net

The software provides a maximum of 256 ports in the entire network.

This SL Net feature is only supported when networked with another SL2100 or SL1100; no other system types are available.

Section 1 INTRODUCTION

SL Net allows networking between multiple SL2100's and SL1100's to act as a single "virtual" SL2100 system. Interconnected with VoIP, each phone system becomes a node on the network that can communicate with any other phone system node. Systems can be installed separately in the same building, or in Remote Offices connected via a qualified network.

A few benefits of SL Net are:

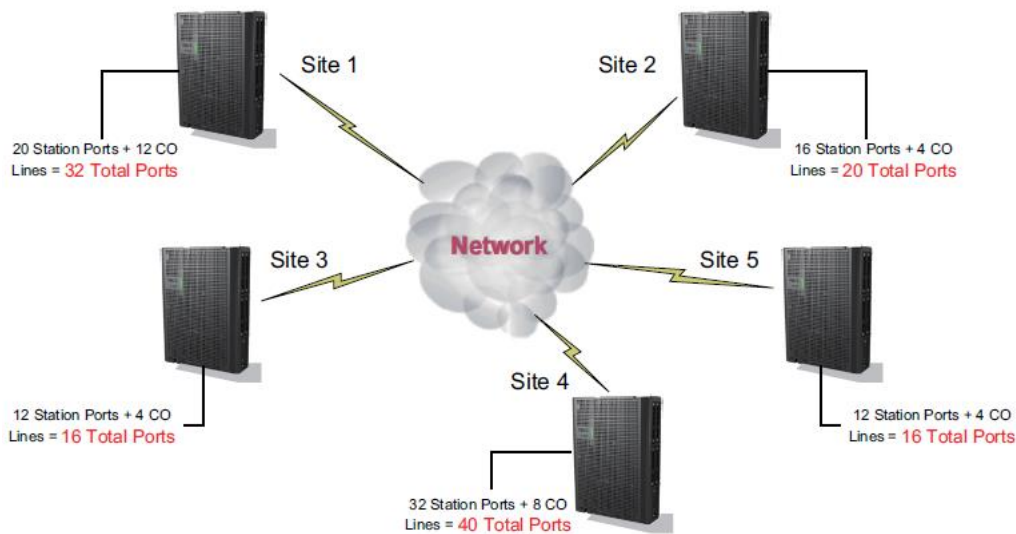
- **Centralized Network Attendant**
Centralized Network Attendant allows multiple networked systems to share a single centralized attendant. The centralized attendant can receive calls from and transfer calls to any destination throughout the whole network. This allows calls to route as if they were part of a single, much larger system.
- **Centralized Voice Mail**
Centralized Voice Mail allows one voice mail system to be installed in a single node. Centralized Voice Mail does not have to be used in an SL Net network. Each system can still have its own independent voice mail.
- **ICM calling between all sites**
Users may place an intercom call or transfer a call to any location by simply dialing an extension number.
- **Sharing Trunk Lines between all sites**
Users may access trunks at any site and make calls as if they were calling from their own local system. Inbound calls can come into one central location and then be routed to any destination extension number in the network. At the same time each site can still have their own independent trunks. It is recommended that each site have at least one analog trunk to dial 911 in the case of an emergency.
- **Network BLF Indication/Centralized Call Park Orbits**
Users can see the status of other extensions throughout the network as if they were all in the same system. Park orbits can also be shared and viewed by all users in the network.

SL Net requires a system license per node, the license is: SL2100 SL NET-08 LIC. This license is a Channel license. License would be required per channels which are used for SL Net in each system.


Section 2 System Capacity

SL Net allows a maximum of 51 systems to be networked together without exceeding a maximum of 256 ports in the entire network. The 256 port capacity is a sum of station and trunk ports in all nodes. When the capacity is exceeded, all systems will enter a standalone mode and will not be able to communicate with each other. At this point the systems can only utilize resources within their own

location. Below is an example showing a network that exceeds the 256 port maximum capacity when site 5 is added to the network.



When the capacity is exceeded, an alarm report is generated and the message "NW port limit exceeded" is displayed on an Alarm indication telephone. To restore the network, so all systems can communicate with each other, the system totals need to be brought below the 256 port maximum. After the necessary ports (station or trunk) are removed from a system, a restart of the SL2100 is not required. Every time a system in an SL Net network is reset, a port count is performed. If the network port count is below 256, all systems are allowed to communicate.

 *InMail ports are not counted against the 256 port maximum capacity.*


Each system will require a CPU-C1 and VoIPDB, which by default will provide 8 channels (by CPU-C1 only) and 16 channels (by CPU-C1 + VoIPDB) to be shared for all IP related devices (e.g. IP Phones, IP Trunks, SL Net). If more than 16 channels are required at any site, the system must have the following license: **SL2100 IP CHANNEL-16 LIC** (5103). With this license installed, the system will now have 32 channels to share for all IP devices. Every system that requires 32 ports must purchase and install this license. Up to 256 channels can be set per system.

Section 3 Network Requirements

The voice quality of VoIP depends on variables such as available bandwidth, network latency, and quality of service initiatives (QoS), all of which are controlled by the network and internet service providers. Because these variables are not within NEC's control, the performance of the users IP-based voice solution cannot be guaranteed. Therefore, NEC recommends connecting the VoIP equipment through a fully managed data network with Quality of Service (QOS) implemented.

For a network to be suitable for VoIP it must pass specific requirements. The requirements are:

- One way delay must not exceed 150 ms
- Round trip delay must not exceed 300 ms
- Packet loss must not exceed 1 %
- Data switches must be manageable
- No half-duplex equipment may be present in the network
- Routers must provide QOS

 *Depending upon how the QOS policies are built in the network, assignments may be needed in the CPU (PRG 84-10).*

- Adequate bandwidth for the estimated VoIP traffic must be available



See below chart for bandwidth calculations.

Below is a chart that shows the average bandwidth per VoIP call over Ethernet.

Codec	Packet Size	Bandwidth Used	Codec	Packet Size	Bandwidth Used
G.711	10 ms	110.4 kbps	G.729	10 ms	54.4 kbps
G.711	20 ms	87.2 kbps	G.729	20 ms	31.2 kbps
G.711	30 ms	79.5 kbps	G.729	30 ms	23.5 kbps
G.711	40 ms	75.6 kbps	G.729	40 ms	19.6 kbps
G.722	10 ms	110.4 kbps	G.729	50 ms	17.3 kbps
G.722	20 ms	87.2 kbps	G.729	60 ms	15.7 kbps
G.722	30 ms	79.5 kbps			
G.722	40 ms	75.6 kbps			

For example, if one site plans on making a maximum of 16 calls across the network using G.729 with a 30 ms packet size, there must be a minimum of 376 kbps available for voice traffic. The QOS policy for this network should allow for 376 kbps to be set aside for voice prioritization.

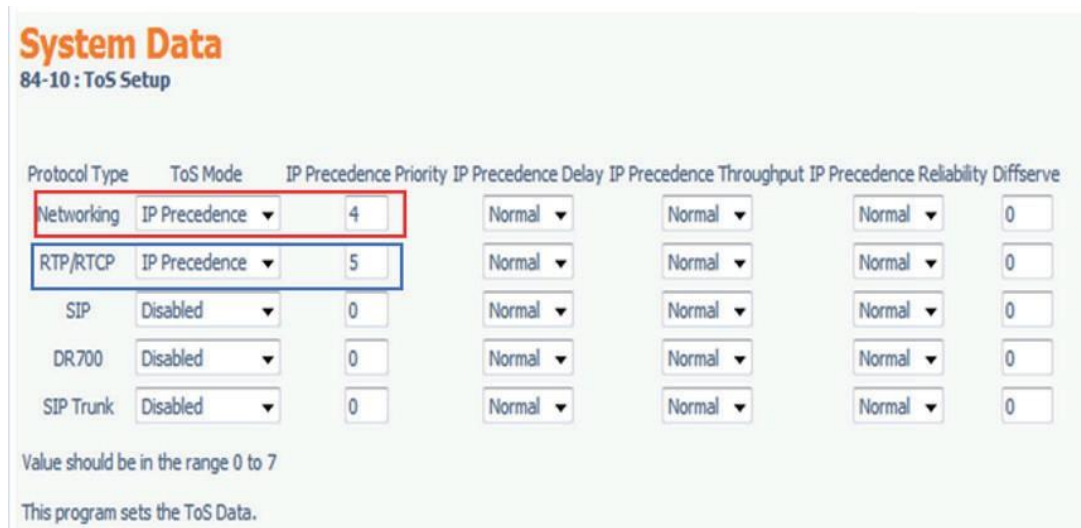
Section 4 QUALITY OF SERVICE SETTINGS (QOS)

Quality of Service (QOS) is one of the most important factors for VoIP. QOS is used to prioritize voice packets over data packets during times of network congestion. There are many ways that QOS can be implemented in the network and one of the most common ways QOS is implemented is by using IP Precedence or Diffserv. If the networks QOS policy is based on IP Precedence or Diffserv then there are settings required in the SL2100.

Program 84-10 is used to assign the IP Precedence or Diffserv Values per Protocol Type. For SL Net only two protocol types will be selected. All signaling packets will be marked with the values assigned for protocol type "H.323". All voice packets will be marked with the values assigned for protocol type "RTP/RTCP".

Section 5 IP PRECEDENCE

IP Precedence uses the first 3 bits of the TOS field to give eight possible precedence values (0 ~ 7). Under normal circumstances the higher the number the higher the priority. However this is left to the network administrator for setup. When assigning IP Precedence values (for SL Net) go to program 84-10-01 and change the type from Disabled to IP Precedence. Then in program 84-10-02 assign the value for the signaling (H.323) and voice (RTP/RTCP) packets. Below is an example where the signaling packets are to be tagged with an IP Precedence of 4 and the voice packets are to be tagged with an IP Precedence of 5.




Protocol Type	ToS Mode	IP Precedence Priority	IP Precedence Delay	IP Precedence Throughput	IP Precedence Reliability	Diffserve
Networking	IP Precedence	4	Normal	Normal	Normal	0
RTP/RTCP	IP Precedence	5	Normal	Normal	Normal	0
SIP	Disabled	0	Normal	Normal	Normal	0
DR700	Disabled	0	Normal	Normal	Normal	0
SIP Trunk	Disabled	0	Normal	Normal	Normal	0

Value should be in the range 0 to 7

This program sets the ToS Data.

Figure 13-1 IP Precedence

 After changes are made to Program 84-10 the system will need to be reset before the proper values are inserted into the IP packets.

Section 6 DIFFSERV

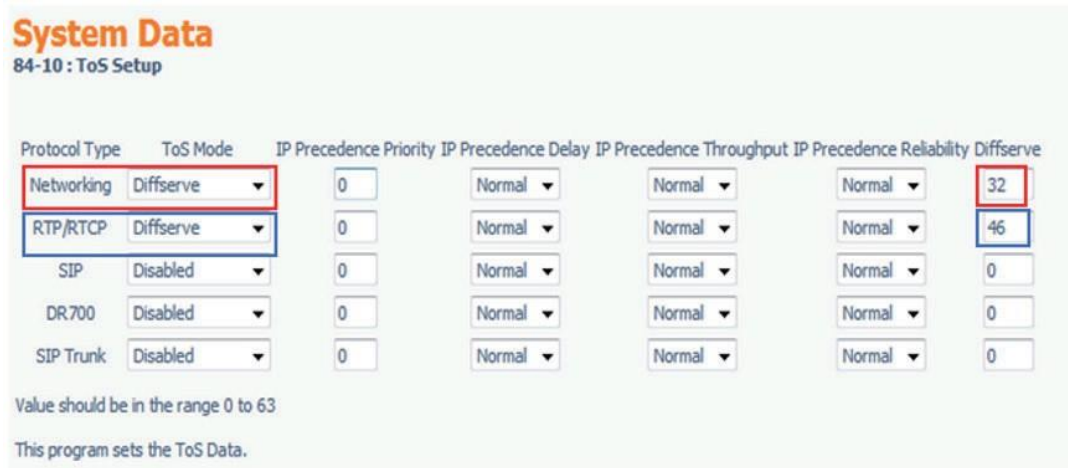
Diffserv is also known as Differential Services Code Point (or DSCP for short). It uses the first 6 bits of the TOS field, therefore giving 64 possible values. The following list shows the most common Diffserv/ DSCP Code Points and their names along with the proper setting in the SL2100.

Table 13-1 Diffserv Parameters

SL2100 Setting (DSCP Code Point)	Name
0	Best Effort (BE)
8	Class Selector 1 (CS1)
10	Assured Forwarding 11 (AF11)
12	Assured Forwarding 12 (AF12)
14	Assured Forwarding 13 (AF13)
16	Class Selector 2 (CS2)
18	Assured Forwarding 21 (AF21)
20	Assured Forwarding 22 (AF22)
22	Assured Forwarding 23 (AF23)
24	Class Selector 3 (CS3)
26	Assured Forwarding 31 (AF31)
28	Assured Forwarding 32 (AF32)
30	Assured Forwarding 33 (AF33)
32	Class Selector 4 (CS4)
34	Assured Forwarding 41 (AF41)
36	Assured Forwarding 42 (AF42)
38	Assured Forwarding 43 (AF43)
46	Expedited Forwarding (EF)

SL2100 Setting (DSCP Code Point)	Name
48	Class Selector 6 (CS6)
56	Class Selector 7 (CS7)


When assigning Diffserv values (for SL Net) go to program 84-10-01 and change the type from Disabled to Diffserve. Then in program 84-10-07 assign the value for the signaling (H.323) and voice (RTP/RTCP) packets. The next table shows an example where the signaling packets are to be tagged as Class Selector 4 and the voice packets are to be tagged as Expedited Forwarding.



Protocol Type	ToS Mode	IP Precedence Priority	IP Precedence Delay	IP Precedence Throughput	IP Precedence Reliability	Diffserve
Networking	Diffserve	0	Normal	Normal	Normal	32
RTP/RTCP	Diffserve	0	Normal	Normal	Normal	46
SIP	Disabled	0	Normal	Normal	Normal	0
DR700	Disabled	0	Normal	Normal	Normal	0
SIP Trunk	Disabled	0	Normal	Normal	Normal	0


Value should be in the range 0 to 63
This program sets the ToS Data.

Figure 13-2 Setup Example

 After changes are made to Program 84-10 the system will need to be reset before the proper values are inserted into the IP packets.

6.1 Conditions

- A maximum of 50 nodes and a total of 256 ports throughout the network.

 InMail ports do not count against the 256 port capacity.

- This feature is only supported when networked with another SL1100 or SL2100; no other system types are available.
- Each system must be individually licensed for this feature with the following license: SL2100 SL NET-08 LIC.
- The system requires a VoIPDB daughter board on the CPU-C1 when more than nine VoIP channels are used in the system. The CPU-C1 is initially available a maximum of eight VoIP channels.
- Each site must have different extension numbers assigned. The same extension number cannot exist at multiple sites.
- Call redirect is not supported with SL Net networking.
- Dual Hold across the network is not supported.
- If calls across SL Net are to follow the local ARS routing, all sites must use ARS routing.
- SL Net is not supported through NAT.
- A Trunk Access via Networking key (*06) will not light up when all trunks in the Remote site trunk group are busy. If a user tries to access a trunk, when they are all busy, the word "Busy" will be in the display and the user will hear Busy Tone but the key will not light up.
- Camp On across SL Net is only supported to a Busy extension.

- When using Barge-In across SL Net the following conditions apply:
 - Barge-In can only be initiated using a soft-key, dial access codes are not supported.
 - The destination extension must be set to have a true busy and not busy ring busy. To receive true busy disable (Set to 0) the following programs for the Class of Service of the destination phones you want to receive Barge-In:
 1. PRG 20-09-01 Second Call For DID/DISA/DIL/E&M
 2. PRG 20-09-07 Call Queuing
 3. PRG 20-13-05 Intercom Off Hook Signal
 4. PRG 20-13-06 Automatic Off Hook
 - Barge-In across SL Net to Operator Extensions is not supported.
- Hold, Transfer, and Park recall timers will follow the timer of the system where the call is on hold (Trunk and Station). For example, a user in Site A calls a user in Site B. Site B answers the call and places the call on hold. The hold recall time is based on Site A because the call on hold is in Site A and not site B.
- The allowing or denying of Class of Service features in an SL Network must be performed network wide. For example, if users in Class of Service 1 at site 1 want to block the Camp On feature a change will have to be made in Class of Service 1 of all systems in the network.
- Paging to a networked system can only be activated by dialing a service code and the target network's system ID.
- When a terminal or trunk is placed on hold, the Music on Hold comes from the system where the terminal or trunk resides.
- When the Hold recall times out, the call will recall to the operator in the system where the CO trunk resides. Hold recall timeout to the operator is controlled in Class of Service program 20-11-13.
- Forced Account Codes are not applied to calls across SL Net.
- When Multiple Voice Mails are installed in the network, each site must have a unique Voice Mail pilot number. The pilot number assigned must be within the routable extension number range in all sites throughout the network.
- When each site has its own Voice Mail system, a user in one location cannot call the Voice Mail pilot number that resides in another system.
- When each site has its own Voice Mail system, a Voice Mail Message Line key (PRG 15-07 key 77) cannot be programmed for an extension in a Remote system.
- When using centralized voice mail in a network that has both SL2100 and SL1100 systems the voice mail department group must be 32 or lower in order to work with the SL1100.
- Virtual Loopback trunks are not supported across SL Net.
- Code Restriction is not applied for CO trunks accessed across the SL Net network.
- When a network has both SL2100 and SL1100 systems PRG 84-34-02, Profile 1, Type 2 (DTMF Payload Number - Networking) must be set to 96 for all SL2100 systems.
- When using centralized voice mail it is strongly recommended that the main SL2100 containing the central voice mail be populated with a IP7WW-EXIFB-C1 and IP7WW-SDVMS-C1 (1G) or IP7WW-SDVML-C1 (4G) SD Drive.
- Network ports (extension or trunk) cannot land on a virtual extension key. When PRG 15-18 is set to "land on key" the virtual extension will still ring. When the call is answered the virtual key will go back to an idle state.
- SMDR information is collected in the system where the trunk resides. If a user in Site A accesses a CO trunk out of Site B, this call is reported in Site B's SMDR and not in Site A's SMDR.
- When a networked ICM call forwards to Voice Mail (Centralized or Individual Voice Mail) the user will not be able to perform any dialing options to dial out of the mailbox. The associated dial action table cannot be accessed unless the call originates from a CO trunk.
- If you use the Make Call feature while listening to a Voice Mail message, the first few seconds of the call may be silent if the call is routed across the SL Net network.
- When using Loop Keys to make outgoing CO calls via the network, the loop key will not light. If ARS is enabled, and an outgoing CO call via the network is placed, the loop key will light for the first few seconds until the system determines which trunk to seize.

- When a CO call via the network is put on hold, the call is placed onto the users Hold key. To retrieve this call the user must press the Hold key. If one call is already on Hold the user cannot place a second call on hold, the second call must be placed into a park orbit or transferred to another station.
- Built-in Automated Attendant and Centralized Voice Mail cannot be used in the same system.
- Calls (Intercom or Trunk) routed across the SL Net network cannot be answered by the Built-In Automated Attendant.
- Caller ID Flexible Ringing does not work for incoming calls via the SL Net network. For the calls to route based on caller ID, the programming must be performed in the system that contains the CO trunks. Routing to other system's extensions is available; however the ringing patterns will not be followed.
- Directory Dialing will not list extension numbers in remote SL Net systems.
- Distinctive Ringing patterns will only work in the system where the trunk resides.
- A Drop Key (PRG 15-07 key 84) or the Flash Key will not function for calls routed across the SL Net network.
- Long conversation cutoff will not disconnect a trunk call if a user accesses a trunk out of a networked system.
- An operator extension (PRG 20-17) cannot be assigned to an extension in a Remote SL Net system. The operator for each site must reside in their own local system.
- Calls routed across the SL Net network cannot use the Repeat Redial function
- A Reverse Voice Over key (PRG 15-07 key 47) cannot be programmed for an extension in a Remote SL Net system.
- Room Monitor cannot be used to monitor an extension in a Remote SL Net system.
- A Saved Number Dialed key (PRG 15-07 key 30) cannot be used to save a number if the call is routed across the SL Net network.
- A Secondary Incoming Extension cannot be programmed for a station in a Remote SL Net system.
- A Secretary Call Buzzer and Secretary Call Pickup key (PRG 15-07 key 41 and key 42) cannot be programmed for a station in a Remote SL Net system.
- A Serial Call cannot be performed to a station in a Remote SL Net system.
- Tandem Ringing (Call Forward Both Ring) cannot be set to an extension in a Remote SL Net system.
- If an extension is using a CO trunk in a Remote SL Net system, the Tone Override feature is not supported. In this scenario the busy station will receive the Tone Override but will not be able to answer the caller.
- Trunk Queuing/Camp-On cannot be performed to a busy CO trunk in a Remote SL Net system.
- Voice Over to a busy extension is not supported across the SL Net network.
- Personal Park (PRG 15-07 key *07 or Service Code 757) is not supported for calls across the SL Net network.
- Mobile Extension is not supported for calls across the SL Net network.
- When a call is transferred to a Department Group with All Ring, there is a difference in operation. In a single system, an extension within the same system can transfer a call to a Department Group. The call will ring an extension within the Department Group once the transferring user hangs up. In a networked system, the transfer will not go through and the call will recall the extension performing the transfer.
- Live Monitor is not supported for users in remote systems.

6.1.1 Default Settings

None

6.2 System Availability

6.2.1 Terminals

All Terminal types are supported

6.2.2 Required Component(s)

IP7[]-4KSU-C1

IP7[]-CPU-C1

IP7WW-VOIPDB-

C1

Each active SL Net call requires one of the following licenses in both end point systems:

- SL2100 SL NET-08 LIC (5091)
- SL2100 IP CHANNEL-16 LIC (5103)

6.3 Related Features

None

Section 7 GUIDE TO FEATURE PROGRAMMING

The programs listed below indicate the most commonly used programs required for this feature. The programs are listed in the order that the installer should follow. Refer to the PCPro wizards for further detailed programming.

When a * is listed next to the Program Number it indicates a program that **MUST** be set (from a default state) for this feature to be enabled.

7.1 Basic Setup

Program Number	Program Name/Description	Assigned Data
10-12-09	VoIPDB IP Address Assign the IP Address for the VoIPDB. If a VoIPDB is installed in the system, NEC recommends setting program 10-12-01 to 0.0.0.0. All connections to the system will be made through the VoIPDB.	0.0.0.0~126.255.255.254 128.0.0.1~191.255.255.254 192.0.0.1~223.255.255.254 (default =172.16.0.10)
10-12-10	VoIPDB Subnet Mask Assign the subnet mask for the VoIPDB card.	Refer to the programming manual for all the possible valid subnet mask entries. (default =255.255.255.0)
10-12-03	Default Gateway Assign the SL2100's default gateway IP address.	0.0.0.0~126.255.255.254 128.0.0.1~191.255.255.254 192.0.0.1~223.255.255.254 (default =0.0.0.0)
84-26-01	VoIP Basic Setup (DSP) Assign the IP address that is used for Voice Communications across the network. The IP address assigned here MUST be within the same network as the IP address assigned in PRG 10-12-09.	0.0.0.0~126.255.255.254 128.0.0.1~191.255.255.254 192.0.0.1~223.255.255.254 (default =172.16.0.20)

Program Number	Program Name/Description	Assigned Data
11-01-01 *	<p>System Numbering Assign the leading digit/digits of the remote SL Net systems as: (8) Networked System Access. Example 1: The Remote SL Net system is going to use extensions 200 ~ 299 then the digit 2 would be assigned as: (8) Networked System Access. Example 2: The Remote SL Net system is going to use extensions 1200 ~ 1299 then the digits 12 would be assigned as: (8) Networked System Access.</p>	0 = Not Used 1 = Service Code 2 = Extension Number 3 = Trunk Access Code 4 = Individual Trunk Access Code 5 = Operator Access 6 = F-Route 8 = Networked System Access 9 = Dial Extension Analyze (Refer to the SL2100 programming manual for the default values.)
11-01-01*	<p>System Numbering Once the leading digits/digits are assigned as network access, you must then assign them to a valid Network ID (1-4). Note: the 1st remote system would be network ID 1, the second would be network ID 2, the 3rd would be network ID 3, and the 4th would be network ID 5. The network ID's at each remote location do not have to match; they are system dependent. For example, if the Remote SL Net system uses extensions 200 ~ 299, then digit 2 would be assigned as: (8) Networked System Access and digit 2 would be assigned as network ID 1.</p>	0 = No Remote Network 1 = Remote Network 1 2 = Remote Network 2 3 = Remote Network 3 4 = Remote Network 4 (default = 0)
10-27-01*	<p>Network System ID Assignment Define the IP Address of the Remote SL Net system where the call is routed for the system ID assigned in PRG 11-01-01.</p>	0.0.0.0 ~ 126.255.255.254 128.0.0.1 ~ 192.255.255.254 192.0.0.1 ~ 223.255.255.254 (default = 0.0.0.0)
20-01-04	<p>Network BLF Indication Assign how often the SL2100 updates the DSS key BLF indications for remote SL Net systems (expressed in seconds). To provide BLF lamping indications across the network, this timer must be adjusted. NEC recommends a value of 3 seconds.</p>	0 ~ 64800 seconds (default = 0)
10-19-01	<p>VoIPDB DSP Resource Selection This program is used to assign the 16 or 32 resources of the VoIPDB. NEC recommends leaving the default settings as system default.</p>	0 = Commonly used for IP extensions, trunks, and networking 1 = Use for IP extensions 2 = Use for SIP trunks 3 = Use for networking (SL Net) 5 = Blocked 6 = Common without unicast paging 7 = Multicast paging 8 = Unicast paging (defaults: resource1 = Use for IP extensions, resource 2 ~ 128 = Common)
10-20-01	<p>External Equipment LAN setup Device type 4 (networking system) must be assigned to the same port number in ALL SL Net systems.</p>	1 = CTI Server (default = 8181) 2 = ACD MIS (default = 4000) 4 = Networking System (default = 30000) 5 = SMDR Output (default = 0) 6 = DIM Output (default = 0) 8 = UC Web Application 9 = 1st Party CTI (default = 8282) 11 = O&M Server (default = 8010) 12 = Traffic Report Output (default = 0) 13 = Room Data Output for Hotel Service (default = 0) 14 = IP-DECT Directory Access (default = 0) 15 = Presence (default = 0) Available values are: 0 ~ 65535
90-10-01	<p>System Alarm Setup Two Alarms were added for SL Net and they are: Alarm 15 – Networking keep alive error Alarm 59 – Networking port limit exceeded</p>	0 = No Setting 1 = Major Alarm 2 = Minor Alarm (Refer to the SL2100 programming manual for the default values.)

Program Number	Program Name/Description	Assigned Data
90-10-02	Report This program is used to assign if the alarm is displayed on a key telephone if the alarm information is reported to the pre-defined destination.	0 = No (<i>alarm disabled</i>) 1 = Yes (<i>alarm enabled</i>) (Refer to the SL2100 programming manual for the default values.)

7.2 Codec Assignment

Program Number	Program Name/Description	Assigned Data
84-12-28	Audio Capability Priority This program assigns the Codec that is used when calling across the SL Net network. Refer to the above bandwidth chart when making the Codec selection.	0 = G.711 1 = Not Used 2 = G.729 3 = G.722 (default = 0)
84-12-01	G.711 Audio Frame Size Assign the G.711 Audio Frame Size. The smaller the packet sizes the more bandwidth that is consumed. However when a smaller packet is lost in a network a smaller amount of the voice is lost with it.	1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms (default = 3)
84-12-02	G.711 Voice Activity Detection This program is used to enable or disable the G.711 Codec to use silence detection. When silence detection is enabled the SL2100 can detect the absence of audio and conserve bandwidth by preventing the transmission of "silent packets" over the network. When this program is enabled, it can save on bandwidth. However, it can also affect the quality of the call. VAD may have trouble detecting the start and end of silence and therefore may cut off the beginning and/or the end of a word.	0 = Disable 1 = Enable (default = 0)
84-12-03	G.711 Audio Type In North America do not change this setting, only u-law is supported.	0 = A-law 1 = U-law (default = 1)
84-12-04	G.711 Minimum Jitter Buffer size This program assigns the minimum size that the jitter buffer will use.	0 ~ 255ms (default = 30ms)
84-12-05	G.711 Average Jitter Buffer size This program assigns the average size that the jitter buffer will use.	0 ~ 255ms (default = 60ms)
84-12-06	G.711 Maximum Jitter Buffer size This program assigns the maximum size that the jitter buffer will use.	0 ~ 255ms (default = 120ms)
84-12-07	G.729 Audio Frame Size Assign the G.729 Audio Frame Size The smaller the packet sizes the more bandwidth that is consumed. However when a smaller packet is lost in a network a smaller amount of the voice is lost with it.	1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms 5 = 50ms 6 = 60ms (default = 3)
84-12-08	G.729 Voice Activity Detection This program is used to enable or disable the G.729 CO-DEC to use silence detection. When silence detection is enabled, the SL2100 can detect the absence of audio and conserve bandwidth by preventing the transmission of "silent packets" over the network. When this program is enabled, it can save on bandwidth however it can also affect the quality of the call. VAD may have trouble detecting the start and end of silence and therefore may cut off the beginning and/or the end of a word.	0 = Disable 1 = Enable (default = 0)

Program Number	Program Name/Description	Assigned Data
84-12-09	G.729 Minimum Jitter Buffer size This program assigns the minimum size that the jitter buffer will use.	0 ~ 255ms (default = 30ms)
84-12-10	G.729 Average Jitter Buffer size This program assigns the average size that the jitter buffer will use.	0 ~ 255ms (default = 60ms)
84-12-11	G.729 Maximum Jitter Buffer size This program assigns the maximum size that the jitter buffer will use.	0 ~ 255ms (default = 120ms)
84-12-17	Jitter Buffer Mode If the jitter buffer is set to adaptive, the buffer is adjusted (larger/smaller), depending upon network conditions. If the jitter buffer is set to static, it will never adjust and always have the same size buffer.	1 = Static 3 = Adaptive Immediately (default = 3)
84-12-18	Voice Activity Detection Threshold This program is used to set the threshold of the db level that the system uses to determine silence. If VAD is enabled and this threshold is reached, the system will stop transmitting "silence packets" across the network.	0~30 = -19dB~+10dB 0 = Adaptec Threshold 1 = -19dB(-49dBm) : 20 = 0dB (-30dBm) : 29 = 9dBm(-21dBm) 30 = 10dBm(-20dBm) (default = 20)
84-12-33	G.722 Audio Frame Size Assign the G.722 Audio Frame Size The smaller the packet sizes the more bandwidth that is consumed. However when a smaller packet is lost in a network a smaller amount of the voice is lost with it.	1 = 10ms 2 = 20ms 3 = 30ms 4 = 40ms (default = 3)
84-12-35	G.722 Minimum Jitter Buffer size This program assigns the minimum size that the jitter buffer will use.	0 ~ 255ms (default = 30ms)
84-12-36	G.722 Average Jitter Buffer size This program assigns the average size that the jitter buffer will use.	0 ~ 255ms (default = 60ms)
84-12-37	G.722 Maximum Jitter Buffer size This program assigns the maximum size that the jitter buffer will use.	0 ~ 255ms (default = 120ms)
84-12-38	RTP Filter This program is used to avoid audio path problems in times of heavy RTP traffic. When enabled, the system will check the sender's IP address that is sending RTP packets. If it does not match with the IP address of the actual caller, the system will ignore it.	0 = Disable 1 = Enable (default = 1)
84-34-01	VoIPDB Setup DTMG Relay Mode (02-Networking) Select DTMF Relay Mode.	0 = Disable 1 = RFC2833 2 = H.245 Profile (1 ~ 6) (default = 0)
84-34-02	This program assigns the way the system handles DTMF across the SL Net network. For profile 1, Type 2 (Networking) this value should match in all SL Net systems.	96 ~ 127 (default = 110)

7.3 Call Routing - Outbound

Program Number	Program Name/Description	Assigned Data
11-01-01	<p>System Numbering This program is used to assign the Trunk Access code (9 by default) and the special trunk access code (unassigned at default). The trunk access code used to make alternate calls must be set to a type 4 (special trunk access code).</p>	<p>0 = Not Used 1 = Service Code 2 = Extension Number 3 = Trunk Access Code 4 = Individual Trunk Access 5 = Operator Access 6 = F-Route Access 8 = Networking System Access 9 = Dial Extension Analyze (Refer to the SL2100 programming manual for the default values of all tables)</p>
11-09-01	<p>Trunk Access Code Use this program to assign the trunk access code defined in program 11-01-01. This is the access code that users will dial to make outbound calls.</p>	<p>Maximum of 4 digits (0~9, *, #,) (default =9)</p>
11-09-02	<p>2nd Trunk Route Access Code Use this program to assign the special trunk access code defined in program 11-01-01. Users dial this access code to make outbound calls from a different trunk group rather than using the primary trunk group access code.</p>	<p>Maximum of 4 digits (0~9, *, #,) (default =not assigned)</p>
21-02-01	<p>Trunk Group Routing for Extensions This assigns extensions per day/night mode to a route table (program 14-06-01). This program follows the trunk access code in PRG 11-01-01 and 11-09-01.</p>	<p>0 = No Setting (Calls will not route) 1~50 = Route Table 1~50 (default =1)</p>
21-15-01	<p>Individual Trunk Group Routing for Extensions This assigns extensions per day/night mode to a route table (program 14-06-01). This program follows the "special trunk" access code from PRG 11-01-01 and 11-09-02.</p>	<p>0 = No Setting (Calls will not route) 1~50 = Route Table 1~50 (default =0)</p>
14-06-01	<p>Trunk Group Routing With SL Net, four new trunk group routing options have been added and they are 101 ~ 150. These options allow the caller to access and make calls using one of the Remote Systems Trunks. 101 will access trunks from Remote system 1 that is programmed in 10-27-01. 102 will access trunks from Remote system 2 that is programmed in 10-27-01. 103 will access trunks from Remote system 3 that is programmed in 10-27-01. 104 will access trunks from Remote system 4 that is programmed in 10-27-01. : 150 will access trunks from Remote system 50 that is programmed in 10-27-01.</p>	<p>0 = No Setting (Calls will not route) 001 ~ 050 = Trunk Group 1~50 101 ~ 150 = 100+Networking System No. 1001 ~ 1050 = 1000+Route Table No. (default =1)</p>
21-16-01	<p>Trunk Group Routing for Networks If a call comes in from across the network, this program determines the route table (PRG 14-06-01) that will be accessed in the local system.</p>	<p>0 = No routing (Calls will not route) 1 ~ 50 = Route table 1 ~ 50 (PRG 14-06-01) (default =1)</p>
15-07-01	<p>Programmable Function Keys This program is used on a per-station basis to assign different function keys to the multiline terminals. Function key (*06) is used to assign a key on a phone that will allow a user to access trunks out of a remote system just by pressing the key. When this key is assigned, an additional data of 1~50 is required. The additional data specifies which Remote system you will access trunks from. When this key is used to access trunks out of a Remote System, it will look at PRG 21-16-01 of the system where the CO Line resides.</p>	<p>*06 = Trunk Access via Networking Secondary Settings: 1 = Remote System 1 from PRG 10-27 2 = Remote System 2 from PRG 10-27 3 = Remote System 3 from PRG 10-27 4 = Remote System 4 from PRG 10-27 : 50 = Remote System 50 from PRG 10-27 (Refer to the SL2100 programming manual for the default values and for all other available options in this program.)</p>

Program Number	Program Name/Description	Assigned Data
11-12-16	Trunk Access via Networking This code allows the user to dial the access code (default 726), then the two-digit remote system number (01 ~ 04 from PRG 10-27), and then the telephone number to complete a call from a destination systems trunk. An example of dialing this code and calling out of Remote system 1 would be: User goes off hook and dials access code 726 .	Default Access Code = 726
26-02-03	ARS/LCR additional data If using ARS for the trunk group routing, four new items have been added to the additional data field. The options are 101 ~ 150 and these options allow the caller to access and make calls out of one of the Remote Systems Trunks. 101 will access trunks from Remote system 1 that is programmed in 10-27-01. 102 will access trunks from Remote system 2 that is programmed in 10-27-01. 103 will access trunks from Remote system 3 that is programmed in 10-27-01. 104 will access trunks from Remote system 4 that is programmed in 10-27-01. : 150 will access trunks from Remote system 50 that is programmed in 10-27-01.	If 26-02-02 is set to Trunk Group 0 = No Routing (Calls will not route) 1 ~ 50 = Trunk Groups 1 ~ 50 101 ~ 150 = Remote Systems 1 ~ 50 If 26-02-02 is set to F-Route 0 = No Routing (Calls will not route) 1 ~ 100 = F-route tables 1 ~ 100 101 ~ 150 = Remote Systems 1 ~ 50 (default =0)
44-05-01	F-Route trunk group number If using F-Route for the trunk group routing, four new items have been added to the trunk group field. The options are 101 ~ 150 and these options allow the caller to access and make calls from a Remote System Trunk. 101 will access trunks from Remote system 1 that is programmed in 10-27-01. 102 will access trunks from Remote system 2 that is programmed in 10-27-01. 103 will access trunks from Remote system 3 that is programmed in 10-27-01. 104 will access trunks from Remote system 4 that is programmed in 10-27-01. : 150 will access trunks from Remote system 50 that is programmed in 10-27-01.	0 = No Setting (Calls will not route) 1 ~ 50 = Trunk Group 1 ~ 50 101 ~ 150 = Remote Systems 1 ~ 50 255 = Intercom (default =0)

7.4 Call Routing - Inbound Analog Trunk

Program Number	Program Name/Description	Assigned Data
22-02-01	Incoming Call Trunk Setup Analog trunks at any location can be set to DIL to any extension number in the SL Net network. For an analog trunk to be DIL it must be set as a type (4) DIL. Once the trunk type is set to DIL the destination can be assigned in program 22-07-01. Analog trunks can also be set as Normal (type 0) to be routed following the ring group settings in PRG 22-05-01.	0 = Normal 1 = VRS 2 = DISA 3 = DID 4 = DIL 5 = Tie Line 6 = Delay VRS 7 = ANI/DNIS 8 = DID (DDI) Mode Switching (default =0)
22-07-01	DIL Assignment For each trunk and day/night mode assignment, designate the destination extension or pilot number where the trunk is routed. Trunks can be routed to any valid extension number in all SL Net systems.	Maximum of 8 digits (0-9, *, #,) (default =Not Assigned)

Program Number	Program Name/Description	Assigned Data
22-05-01	Incoming Trunk Ring Group Assignment SL Net calls can be routed to a Centralized Voice Mail from any location using a setting data of 103. When 103 is assigned, calls will be routed to the pilot number defined in PRG 45-01-07.	1~50 = Ring Group 1~50 102 = Voice Mail (Call goes to the VM pilot assigned in program 45-01-01) 103 = Centralized Voice Mail (if centralized VM is enabled this setting is used to route calls to the VM) (default =1)
22-08-01	DIL/IRG No Answer Destination After the timer in program 22-01-04 expires the call will overflow to the pre-defined location defined in this program. SL Net calls can overflow to a Centralized Voice Mail from any location using a setting data of 103. When 103 is assigned, calls will overflow to the pilot number defined in PRG 45-01-07.	0 = No Setting 1~50 = Ring Group 1~50 102 = Voice Mail (Call goes to the VM pilot assigned in program 45-01-01) 103 = Centralized Voice Mail (if centralized VM is enabled this setting is used to route calls to the VM) (default =1)
22-01-04	DIL/IRG No Answer Destination Timer A call will ring the DIL or Ring Group destination for the specified amount of time programmed. Once the timer expires, and the call was not answered, the call will now overflow to the destination set in program 22-08-01.	0 = No Overflow 1~64800 = 1~64800 seconds (default =0)

7.5 Call Routing - Inbound (DID)

Program Number	Program Name/Description	Assigned Data
22-02-01*	Incoming Call Trunk Setup ISDN PRI or SIP trunks at any location can send a DID directly to any extension number in the SL Net network. Trunks must be set to type (3) DID to follow the digit conversion tables.	0 = Normal 1 = VRS 2 = DISA 3 = DID 4 = DIL 5 = Tie Line 6 = Delay VRS 7 = ANI/DNIS 8 = DID (DDI) Mode Switching (default =0)
22-11-01*	Received Number Enter the digits received from the Telco that are going to be translated. The amount of digits entered should be equal to the setting assigned in program 22-09-01.	Maximum of 8 digits (0~9, *, #, #) (default =Not Assigned)
22-11-02*	Target Number Enter the destination number where the DID is sent. The destination can be any valid extension number in the SL Net network.	Maximum of 8 digits (0~9, *, #, @) (default =Not Assigned)
22-11-04	Transfer Operation Mode The transfer operation mode allows DID calls to have more routing options than just the target number. If the transfer operation mode is set to "No Transfer", calls will only be delivered to the Target Number specified in program 22-11-02. If set to one of the three other modes, it will follow that mode through all assigned transfer destinations.	0 = No Transfer 1 = Busy 2 = No Answer 3 = Busy/No Answer (default =0)

Program Number	Program Name/Description	Assigned Data
22-11-05	<p>Transfer Destination Number 1</p> <p>SL Net allows calls to overflow to a Centralized Voice Mail from any location using a setting data of 103. When 103 is assigned, calls will overflow to the pilot number defined in PRG 45-01-07.</p> <p>If the transfer operation mode is set (PRG 22-11-04), and one of the conditions is met, calls will overflow from the target number to the destination in this program. If this was a No Answer condition, calls would overflow to this program after the timer in 22-01-06 expires.</p>	<p>0 = No Setting</p> <p>1~50 = Ring Group 1~50</p> <p>102 = Voice Mail (Call goes to the VM pilot assigned in program 45-01-01)</p> <p>103 Centralized Voice Mail (if centralized VM is enabled this setting is used to route calls to the VM)</p> <p>201~250 = Department Group 1~50</p> <p>400 = VRS</p> <p>401 = DISA</p> <p>501~599 = DISA/VRS Message (VRS message number 1~99)</p> <p>1000~1999 = Speed Dial Bins 000~999 (default =0)</p>
22-11-06	<p>Transfer Destination Number 2</p> <p>SL Net allows calls to overflow to a Centralized Voice Mail from any location using a setting data of 103. When 103 is assigned, calls will overflow to the pilot number defined in PRG 45-01-07.</p> <p>If the transfer operation mode is set (PRG 22-11-04), and one of the conditions is met, calls will overflow from the target number to the destination in this program. If this was a No Answer condition, calls would overflow to this program after the timer in 22-01-06 expires.</p>	<p>0 = No Setting</p> <p>1~50 = Ring Group 1~50</p> <p>102 = Voice Mail (Call goes to the VM pilot assigned in program 45-01-01)</p> <p>103 Centralized Voice Mail (if centralized VM is enabled this setting is used to route calls to the VM)</p> <p>201~250 = Department Group 1~50</p> <p>400 = VRS</p> <p>401 = DISA</p> <p>501~599 = DISA/VRS Message (VRS message number 1~99)</p> <p>1000~1999 = Speed Dial Bins 000~999 (default =0)</p>
22-12-01	<p>DID Intercept Ring Group</p> <p>If the transfer operation mode is set (PRG 22-11-04), and the call has overflowed through Transfer Destination Number 1 and 2, and Incoming Ring Group Transfer is enabled, calls will be routed to the destination in this program.</p> <p>SL Net allows calls to overflow to a Centralized Voice Mail from any location using a setting data of 103. When 103 is assigned, calls will overflow to the pilot number defined in PRG 45-01-07.</p>	<p>0 = Not Set</p> <p>1~50 = Ring Group 1~50</p> <p>102 = Voice Mail (Call goes to the VM pilot assigned in program 45-01-01)</p> <p>103 Centralized Voice Mail (if centralized VM is enabled this setting is used to route calls to the VM)</p> <p>(default =1)</p>
22-01-06	<p>DID Ring-No-Answer Time</p> <p>Use this program to assign the amount of time that a call will ring the DID Transfer Target before overflowing to Transfer Destination Number 1.</p>	<p>0~64800 seconds</p> <p>(default =20 seconds)</p>
22-01-07	<p>DID Incoming Ring Group No Answer Time</p> <p>Use this program to assign the amount of time that a call will ring the Transfer Destination Number 1 before overflowing to Transfer Destination Number 2.</p> <p>This timer also controls the amount of time that a call will ring the Transfer Destination Number 2 before overflowing to the DID Intercept Ring Group.</p>	<p>0~64800 seconds</p> <p>(default =20 seconds)</p>

7.6 Centralized Voice Mail

Program Number	Program Name/Description	Assigned Data
11-07-01*	<p>Department Group Pilot Number</p> <p>Assign the Voice Mail pilot number to the group that is to be used. A pilot number must fall within the valid numbering plan assigned in program 11- 01-01.</p> <p>NEC recommends that you do not use department group 01 because by default all extensions are assigned to this group.</p> <p>This program is only assigned in the system that has the Voice Mail.</p>	<p>Maximum of 8 digits (0~9, *, #,)</p> <p>Default:</p> <p>Department Group No. 1~49: No Setting</p> <p>Department Group No. 50: 5999</p>

Program Number	Program Name/Description	Assigned Data
16-01-02	<p>Department Group Calling Cycle</p> <p>This program is used to define what happens when the department group pilot number is called.</p> <p>If this is set to priority, every new call to the pilot number will search an idle phone in order of the extensions priority (set in program 16-02-02). The lower the number the higher the priority for that extension. For example, if two phones are idle and one phone has a priority of a 1 and the other phone has a priority of a 2, the phone with the priority 1 will receive the call.</p> <p>If this is set to circular, every new call to the pilot number will cycle to an idle extension in a circular order. The priority of the extension is not used.</p> <p>When using a department group for Voice Mail, this program must be set to (0) priority.</p>	<p>0 = Normal Routing (Priority) 1 = Easy UCD routing (Circular) (default = 0)</p>
16-01-04	<p>Department Group Hunting Mode</p> <p>This program sets what happens when an unanswered call to a department group pilot number reaches the last member of the group.</p> <p>If this is set to (0), once the last extension is called the hunting will stop.</p> <p>If this is set to (1), once the last extension is called the hunting will continue to look for an idle member to receive the call.</p> <p>NEC recommends setting this to (1) Circular when using a department group for Voice Mail.</p>	<p>0 = Last extension is called and hunting stops 1 = Circular (Hunting will continue) (default = 0)</p>
16-01-10	<p>Department Group Enhanced Hunting</p> <p>This program defines the conditions by which calls to the pilot number will hunt to the available extensions in the group.</p> <p>For a description on all the hunting types, see the Department Group feature.</p> <p>NEC recommends setting the Voice Mail department group as (3) Busy/No Answer.</p>	<p>0 = No Hunting 1 = Hunting when Busy 2 = Hunting when Not Answered 3 = Hunting when Busy/No Answer (default = 0)</p>
16-02-01*	<p>Department Group Assignment for Extensions</p> <p>This program is used to assign the extensions to the department group.</p> <p>When using a department group for Voice Mail, you must have licenses to cover every extension assigned.</p>	<p>1~50 Default: Department Group No. 1: Extension No. 101~199, 200~271, 3100~3112 Department Group No. 50: Extension No. 3113~3128</p>
16-02-02	<p>Department Group Priority Assignment</p> <p>This program sets the extensions priority within the department group. The lower the number that is assigned the higher the priority.</p> <p>When using a department group for Voice Mail, the lowest voice mail port must have the lowest priority number in the group.</p> <p>For example if the VM had system ports 65~68 and used extensions 165~168 the following would be the assignment.</p> <p>Ext 165 = Priority 1 Ext 166 = Priority 2 Ext 167 = Priority 3 Ext 168 = Priority 4</p>	<p>1~200 Extension 101~199 = Priority 1~99 Extension 200~271 = Priority 1~16 Extension 3100~3112 = Priority 100~112 Extension 3113~3128 = Priority 129~200 (Refer to the SL2100 programming manual for the default values of all extensions)</p>
45-01-01	<p>Voice Mail Department Group Number</p> <p>When using Centralized Voice Mail in an AspireNet network, this program MUST be left unassigned in all sites that will access the VM.</p>	<p>0 = No Voice Mail Assigned 1~50 = Department Group 1~50 (default = 50)</p>
45-01-10*	<p>NSL Protocol</p> <p>All sites using the Centralized Voice Mail must enable this program for proper integration.</p>	<p>0 = Off (Disable) 1 = On (Enable) (default = 0)</p>
14-01-22	<p>Caller ID to Voice Mail</p> <p>This command enables or disables the ability for the system to send the caller ID information to the Voice Mail. This command is for ALL trunk types (analog, digital, and IP).</p>	<p>0 = Disable (Caller ID not sent to VM) 1 = Enable (Caller ID is sent to VM) (default = 0)</p>

Program Number	Program Name/Description	Assigned Data
84-34-01*	DTMF Relay Mode This program assigns the way the system handles DTMF across the network. When Centralized VM is required this program must be set to (1) RFC2833 in all systems.	0 = Disable 1 = RFC 2833 2 = H.245 Profile (1 ~ 6) (default = 0)
84-34-02	DTMF Payload Number This program assigns the way the system handles DTMF across the AspireNet network. For profile 1, Type 2 (Networking) this value should match in all AspireNet systems.	96 ~ 127 (default = 110)

7.7 Alarm Setup

Program Number	Program Name/Description	Assigned Data
90-10-01*	Alarm Type Per Alarm Number (1 ~ 100) specify an alarm type. If an alarm is set to "Not Set" then NO alarm information will be generated. If an alarm is set to "Major Alarm" or "Minor Alarm" then alarm data will be presented when an error occurs. The alarm report will be labeled with the "Major Alarm" or "Minor Alarm" tag in the report. The following Alarms are suggested when troubleshooting an SL Net network: Alarm 15 – Network Keep Alive Alarm 17 – Denial of Service Attack Alarm 57 – IP Address Collision (Duplicate IP Assignment) Alarm 59 – SL Net port count exceeded Alarm 64 – VoIPDB LAN link error Alarm 65 – VoIPDB trouble information Alarm 68 - VoIPDB DSP all Busy	0 = Not Set (No Alarm Generated) 1 = Major Alarm 2 = Minor Alarm Default Alarm Settings Alarm 15 = 0 Alarm 17 = 1 Alarm 57 = 2 Alarm 59 = 2 Alarm 64 = 1 Alarm 65 = 0 Alarm 68 = 2 (Refer to the SL2100 programming manual for the default values of all Alarms)
10-31-01	Keep Alive Interval This PRG is used to set the Interval in which the system will send a Keep Alive message to Remote SL Net systems. When set to 0 a Keep Alive will not be sent across the network and Alarm 15 will not be reported on. When set to (1 ~ 65535 seconds) the system will send a Keep Alive to the Remote SL Net systems at this interval. When the system does not receive a response to one of these Keep Alive messages an Alarm 15 will be generated and labeled as a Warning. An example of this alarm is: MIN 0015 WAR 11/07/11 14:07 NW KeepAlive -none- ID:02-004 MIN = Minor Alarm, this is because the Alarm was flagged as minor. 0015 = Alarm number 15. WAR = Warning, indicating the network is still up but a keep alive was missed. 11/07/11 = Date the Warning was generated 14:07 = Time in 24 hour format that the Warning was generated NW KeepAlive = Alarm Name None = Field not used ID:02-004 = System ID 02 (from PRG 10-27) did not respond to 4 Keep Alive messages.	0 = Disabled 1~65535 = 1~65535 seconds (default =0)

Program Number	Program Name/Description	Assigned Data
10-31-02	<p>Keep Alive Retry Timer</p> <p>This program is used to set the amount of times the system will resend a Keep Alive message when there is no response from the other side.</p> <p>If the response is not received within the specified number of retries, the networking link will be taken out of service. When the link is taken out of service an Alarm 15 will be generated and labeled as an Error.</p> <p>An example of this alarm is: MAJ 0015 ERR 11/07/11 14:10 NW KeepAlive -none- ID:02</p> <p>MAJ = Major Alarm, this is because the Alarm was flagged as major.</p> <p>0015 = Alarm number 15.</p> <p>ERR = Error, indicating the network link was taken out of service.</p> <p>11/07/11 = Date the Error was generated.</p> <p>14:10 = Time in 24 hour format that the Error was generated.</p> <p>NW KeepAlive = Alarm Name.</p> <p>None = Field not used.</p> <p>ID:02 = System ID 02 (from PRG 10-27) was taken out of service.</p>	1 ~ 255 = How many retries are transmitted before the link is taken out of service (default =5)

Section 8 PROGRAMMING EXAMPLES

The following examples will all be based off of two sites connected together with SL Net. Site A will have extension numbers in the 1XX range and site B will have extension numbers in the 2XX range. The diagram below shows the IP Addressing information for each site.

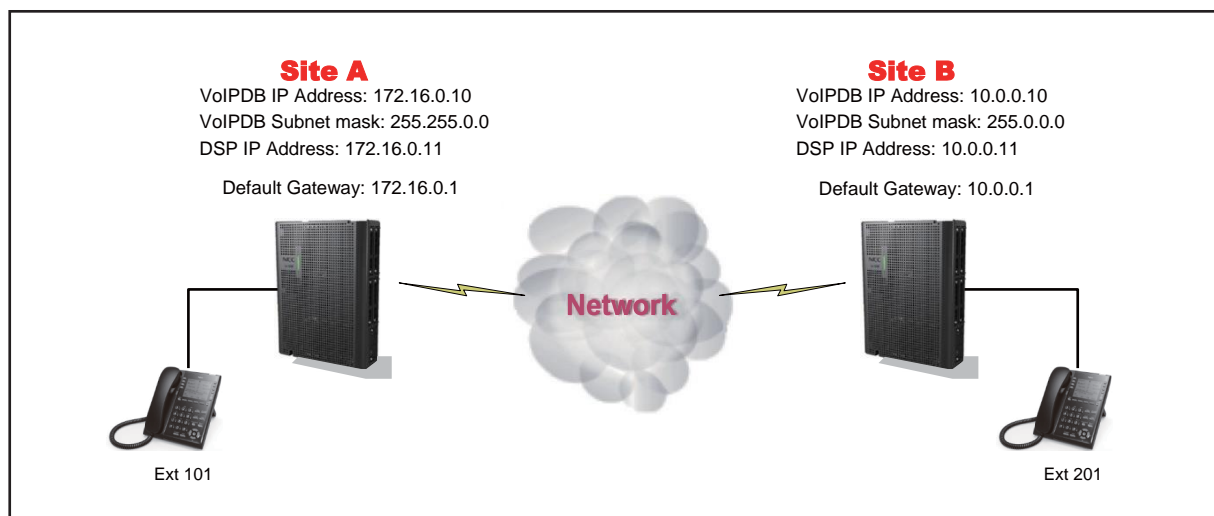


Figure 13-3 Programming Example

8.1 Basic SL Net Setup

Program	Site A	Site B	Notes
10-12-09	172.16.0.10	10.0.0.10	IP address of VoIPDB
10-12-10	255.255.0.0	255.0.0.0	Subnet Mask of VoIPDB
10-12-03	172.16.0.1	10.0.0.1	Default Gateway
84-26-01	172.16.0.11	10.0.0.11	DSP IP Address

Program	Site A	Site B	Notes
11-02-01	Default	Change extensions to 201 ~ 284	Extension numbering
11-01-01	Digit (2X) set to 3 digit length	Digit (1X) set to 3 digit length	Define the digit length for the remote destination extension numbers.
11-01-01	Digit (2X) set to Network System Access	Digit (1X) set to Network System Access	Set the leading digits of the remote destination as Network System Access.
11-01-01	Digit (2X) set to Network ID 1	Digit (1X) set to Network ID 1	Set the leading digits of the remote destination as the first available network ID.
10-27-01	Set system ID 1 = 10.0.0.10	Set System ID 1 = 172.16.0.10	Define the IP Address of the destination system. System ID 1 was used because this was the ID assigned in PRG 11-01-03.
20-01-04	3	3	Allows the sites to see BLF status of extensions across the network.
10-20-01	Device Type 4 = Default	Device Type 4 = Default	Verify that both sites still have the default value of 30000 assigned. Port numbers other than default can be used but all sites must use the same port number.

8.1.1 Centralized VM

In the example below site A will be using an InMail with 16 ports as the Centralized VM. The InMail will use station ports 69 ~ 84 and have a pilot number of 100.

Program	Site A	Site B	Notes
11-02-01	Default		Verify the InMail extension numbers are 169 ~ 184
11-07-01	Group 32 = 100	NA	Assign the VM pilot Number to group 32
15-03-01	Ext's 169 ~ 184 = DP	NA	Change ALL VM extensions to DP
15-03-03	Ext's 169 ~ 184 = Special	NA	Change ALL VM extensions to special
16-01-02	Group 32 = Priority	NA	Change VM groups calling cycle
16-01-04	Group 32 = Circular	NA	Change VM groups hunting mode
16-01-10	Group 32 = BNA	NA	Change VM groups enhanced hunting
16-02-01	Ext's 169 ~ 184 = Group 32	NA	Assign ALL VM extensions to the VM group
16-02-02	Change the 1st VM ext (169) to Priority 1, 2nd to Priority 2, etc.	NA	Assign the priority to ALL VM extensions.
45-01-01	DO NOT ASSIGN	DO NOT ASSIGN	Leave this Unassigned when using Centralized VM
45-01-07	100	100	Assign the VM pilot number to ALL sites
45-01-08	32	NA	Assign the VM department group only in the site with the VM
45-01-10	ON	ON	Enable NSL protocol on ALL sites
84-34-01	RFC2833	RFC2833	Set all sites in the network to RFC2833.

8.1.2 Network BLF Indication

In the following example ext 101 will have a DSS/BLF of extension 201 on the phone. When ext 201 is Busy, the user at extension 101 will see the DSS/BLF key is lit indicating that ext 201 is in use.

Extension 102 will have a DSS console and the first two keys on the DSS console will provide Network BLF indication for extension 201 and 202.

Extension 201 will have a DSS/BLF of extension 101 on the phone. When ext 101 is Busy, the user at extension 201 will see the DSS/BLF key is lit indicating that ext 101 is in use.

Program	Site A	Site B	Notes
10-20-01	Device Type 4 = Default	Device Type 4 = Default	Verify that both sites still have the default value of 30000 assigned. Port numbers other than default can be used but all sites must use the same port number. If the port numbers at each location do not match or are unassigned calls will still be completed across the network however BLF indication will not function properly.
20-01-04	3	3	Allows the sites to see BLF status (on line keys or DSS consoles) across the network.
15-07-01	On ext 101 assign key 1 as: 01- DSS/One-Touch 201	On ext 201 assign key 1 as: 01- DSS/One-Touch 101	PRG 15-07-01 is assigned per phone. All phones wanting to see network BLF indication will have to be assigned individually.
30-02-01	DSS console 01 = 102	NA	This associated ext 102 with the first DSS console in the system.
30-03-01	DSS Console 1 DSS Key 001 = 01 – DSS/ One-Touch 201 DSS Key 002 = 01-DSS/ One-Touch 202	NA	Keys 1 & 2 of the DSS console now will display Network BLF indication for ext 201 and 202.

8.1.3 Network Call Park

In the following example extension 101 and 201 will have Call Park orbit 01 on line key 1 of their phones. When a call is parked in this orbit (Park 01) both of these line keys will indicate that a caller is parked. The call can be picked up from these two stations by pressing the key or the call can be retrieved from any user in the network using an access code.

-Note- By default Call Park bins are shared with every phone throughout the network. This can be changed so that each site has their own call park locations and will not be shared throughout the network.

Program	Site A	Site B	Notes
10-20-01	Device Type 4 = Default	Device Type 4 = Default	Verify that both sites still have the default value of 30000 assigned. Port numbers other than default can be used but all sites must use the same port number. If the port numbers at each location do not match or are unassigned calls will still be completed across the network however Call Park indication and retrieval will not function properly.
20-01-04	3	3	Allows the sites to see Park status (on line keys or DSS consoles) across the network.
15-07-01	On ext 101 assign key 1 as: *04- Park Key 01	On ext 201 assign key 1 as: *04- Park Key 01	PRG 15-07-01 is assigned per phone. All phones wanting to see network CallPark indication will have to be assigned individually.
11-12-31	NA	NA	Default Service Code = #6. By default any user in the network can park a call using this service code.

Program	Site A	Site B	Notes
11-12-32	NA	NA	Default Service Code = *6. By default any user in the network can retrieve a parked call from anywhere in the network using this service code.
24-03-01	NA	NA	This program is used to change the extensions Park Group. By default all users in the network are in group 1. If the users do not want to share the Park bins throughout the network move them to another group (valid options 1~64).

8.1.4 Call Routing - Outbound

In the following example users in Site B will access the trunks from site A by dialing an access code of 8. When a user in site B dials 8 and a phone number the call will be processed across the network and out the trunk in site 1. Users in Site B will still be able to dial 9 and make calls out their own local trunks.

Program	Site A	Site B	Notes
11-01-01	NA	Digit (8X) set to 1 digit length	Define the digit length for the special trunk access code.
11-01-01	NA	Digit (8X) set to Individual Trunk (Special Trunk Access)	Set the leading digit as special trunk access.
11-09-02	NA	8	This assigns the special trunk access code defined in PRG 11-01-01.
21-15-01	NA	All Stations = 2	Assign all stations in all modes to Route Table 2.
14-06-01	NA	Route Table 2 = 101	101 will access trunks from Remote system 1 that is programmed in 10-27-01.
21-16-01	NA	NA	When a call comes in from across the network, this program determines the route table (PRG 14-06-01) that will be accessed in the local system. In Site A, by default, all networked systems are set to route table 1. Route table 1, by default, is assigned to trunk group 1 (PRG 14-06-01).

8.1.5 Paging across the network - Internal and External

A user can perform and Internal, External, or Combined page to any system in the SL Net network. To page a remote SL Net system, follow the operation below.

Internal Page – Dial internal paging access code (701 at default) + # + two digit system ID code (01~04) + two digit Page Zone (00~32). The following is an example of paging internal zone 1 in remote system 1. User goes off hook and dials 701 + # + 01 + 01 and begins paging. When the user is finished paging, go back on hook to end the page.

External Page – Dial the external paging access code (703 at default) + # + two digit system ID code (01~04) + single digit external zone (0~3). The following is an example of paging external zone 1 in remote system 1. User goes off hook and dials 703 + # + 01 + 1 and begins paging. When the user is finished paging, go back on hook to end the page.

Combined Page – Dial the combined paging access code (*1 at default) + # + two digit system ID code (00~04) + single digit external zone number (0~3).

Program	Site A	Site B	Notes
11-12-19	NA	NA	Default internal page code is 701
11-12-20	NA	NA	Default external page code is 703
11-12-24	NA	NA	Default combined page code is *1
31-02-01	NA	NA	Per site assign phones to an Internal Paging group. By default the first 16 ports are in group1.
31-04-01	NA	NA	Per site assign each External Pagingzone to an external paging group. By default Zone 1 = Group 1, Zone 2 =Group 2, and Zone 3 = Group 3.
31-07-01	NA	NA	Per site assign External Paging group (0~3) to an Internal Paging group (0~50) to be used for combined paging. By default all External Groups are set to Internal Page group 1.

Section 9 LIST OF SUPPORTED FEATURES IN A NETWORKED SYSTEM

Feature Name	Supported in Networked System	Comment
Abbreviated Dialing/Speed dial	No	
Account Code Forced/Verified/Unverified	No	
Account Code Entry	No	
ACD	No	
Alarm/Alarm Reports	No	
Answer Hold/Automatic Hold	No	
Attendant Call Queuing	Yes	
Automatic Release	Yes	
Automatic Route Selection (ARS)	Yes	
Background Music	No	
Barge In	Yes	<ul style="list-style-type: none"> • Barge-In can only be initiated using a soft-key, dial access codes are not supported. • The destination extension must be set to have a true busy and not busy-ring-busy. • Barge-In across SL Net to Operator Extensions is not supported.
Built In Automated Attendant	No	
Call Arrival Keys	Yes	
Call Duration Timer	Yes	
Call Forwarding	Yes	
Call Forwarding with Follow Me	Yes	
Call Forwarding Off Premise	Yes	
Call Forwarding/DND Override	Yes	
Call Monitoring	Yes	
Call Redirect	No	

Feature Name	Supported in Networked System	Comment
Call Waiting/Camp-On	* Yes	Camp On across SL Net is only supported to a Busy extension
Callback	* Yes	Callback across SL Net is only supported to a Busy extension
Caller ID Call Return	Yes	
Caller ID	Yes	
Caller ID Flexible Ringing	No	
Caller ID Shared Logging	No	
Central Office Calls, Answering	Yes	
Central Office Calls, Placing	Yes	
Class of Service	Yes	
Clock/Calendar Display/Time and Date	No	
Code Restriction	No	
Conference	Yes	
Continued Dialing	Yes	
Delayed Ringing	Yes	
Department Calling	Yes	
Department Step Calling	Yes	
DHCP Client	No	It is recommended to disable this feature when using networking.
Dial Pad Confirmation Tone	Yes	
Dial Tone Detection	Yes	
Dial Number Preview	Yes	
Direct Inward Dialing (DID)	Yes	
Direct Inward Line (DIL)	Yes	
Direct Inward System Access (DISA)	Yes	
DSS Console	Yes	
Directed Call Pickup	No	
Directory Dialing	No	
Distinctive Ringing	No	
Do Not Disturb (DND)	Yes	
Door Box	No	
Drop Key	No	
Ecology	No	
E911 Compatibility	No	Each site must have at least one local central office trunk for 911 dialing.
Flash	No	
Flexible System Numbering	Yes	
Flexible Timeouts	Yes	
Forced Trunk Disconnect	No	
Group call Pickup	No	
Group Listen	Yes	
Handset Mute/Handset Cutoff	Yes	
Hands free and Monitor	Yes	

Feature Name	Supported in Networked System	Comment
Hands free Answerback/Forced ICM Ringing	Yes	
Headset Operation	Yes	
Hold	* Yes	Dual Hold is not supported across thenetwork.
Hotel/Motel	No	
Hot Key-Pad	Yes	
Hotline	Yes	
Howler Tone Service	Yes	
InMail	* Yes	Each site can have its own VM or one Centralized VM can be used.
Intercom	Yes	
IP Multiline Station	Yes	
IP Single Line Station	Yes	
IP Trunk – SIP	Yes	
ISDN Compatibility	Yes	
Last Number Redial	Yes	
Licensing	Yes	
Line Preference	Yes	
Long Conversation Cutoff	No	
Loop Keys	* Yes	When using loop keys to make outgoing calls via the network, the loop key will not light.
Meet Me Conference	Yes	
Meet Me Paging	Yes	
Memo Dial	Yes	
Message Waiting	Yes	
Microphone Cutoff	Yes	
Mobile Extension	No	
Multiple Trunk Types	Yes	
Music on Hold	No	Each site would require its own music source. When a trunk call is placed on hold it will hear the MOH of the system that the trunk resides in.
Name Storing	Yes	
Navigation Key	Yes	
Night Service	No	
Off Hook Signaling	Yes	
One Touch Calling	Yes	
Operator	No	
Paging, External	* Yes	Paging to a networked system can only be activated by dialing a service code and the target network's system ID.
Paging, Internal	* Yes	Paging to a networked system can only be activated by dialing a service code and the target network's system ID.
Park	* Yes	Personal Park (PRG 15-07 key *07 or Service Code 757) is not supported for calls across the SL Net network.
PBX Compatibility/behind PBX	Yes	

Feature Name	Supported in Networked System	Comment
PC Programming	Yes	
Power Failure Transfer	No	
Prime Line Selection	Yes	
Private Line	No	
Programmable Function Keys	Yes	
Redial	Yes	
Remote System Upgrade	Yes	
Repeat Dial	No	
Reverse Voice Over	No	
Ring Group	Yes	
Ring Down Extension	Yes	
Room Monitor	No	
Saved Number Dialed	No	
Secondary Incoming Extension	No	
Secretary Call (Buzzer)	No	
Secretary Call Pickup	No	
Security	No	
Selectable Display Messaging	Yes	
Selectable Ring Tones	Yes	
Serial Call	No	
Single Line Terminals	Yes	
SL Desktop Suite	Yes	
Soft keys	Yes	
Station Hunt	Yes	
Station Message Detail Recording (SMDR)	No	
Station name Assignment – UserProgrammable	No	
Station Relocation	No	
T1 Trunking	Yes	
Tandem Ringing (Call Forward Both Ring)	No	
Tandem Trunking (Unsupervised Conference)	Yes	
Tone Override	No	
Traffic Reports	No	Each site requires its own SMDR
Transfer	Yes	
Trunk Group Routing	Yes	
Trunk Queuing/Camp On	No	
Unicast/Multicast Paging	* Yes	Only Unicast paging is supported across the network
Uniform Call Distribution (UCD)	No	
User Programming Ability	Yes	
Virtual Extensions	* Yes	Network ports (ICM or Trunk) cannot land on the Virtual extension key.
Virtual Loopback Trunk	No	
Voice Mail Integration (Analog)	No	Only InMail issupported as a centralized VM.

Feature Name	Supported in Networked System	Comment
Voice Mail Indication on Line Keys	Yes	
Voice Over	No	
VRS	No	
Volume Controls	Yes	
Warning Tone for Long Conversation	Yes	

MEMO

SL2100

Networking Manual

NEC Platforms, Ltd.

ISSUE 3.0