

Panasonic®

Installation Manual

Pure IP-PBX



Model No.

KX-NS1000



Thank you for purchasing this Panasonic product.

Please read this manual carefully before using this product and save this manual for future use. In particular, be sure to read "1.1 For Your Safety (Page 22)" before using this product.

KX-NS1000: PCMPR Software File Version 003.20000 or later

Manuals and supporting information are provided on the Panasonic Web site at:
<http://panasonic.net/pcc/support/pbx/>

System Components

System Components for KX-NS1000

Category	Model No.	Description
Main Unit	KX-NS1000	Main Unit
Activation Key Codes¹	KX-NSE101	Activation Key for Mobile Extension for 1 User (1 Mobile User)
	KX-NSE105	Activation Key for Mobile Extension for 5 Users (5 Mobile Users)
	KX-NSE110	Activation Key for Mobile Extension for 10 Users (10 Mobile Users)
	KX-NSE120	Activation Key for Mobile Extension for 20 Users (20 Mobile Users)
	KX-NSF201	Activation Key for Call Centre Feature Enhancement (Call Centre Enhance)
	KX-NSM005	31-50 IP Phone Capacity (Up to 50 IP Phone)
	KX-NSM010	31-100 IP Phone Capacity (Up to 100 IP Phone)
	KX-NSM030	31-300 IP Phone Capacity (Up to 300 IP Phone)
	KX-NSM099	31-640 IP Phone Capacity (System MAX IP Phone)
	KX-NSX910	51-100 IP Phone Capacity (Expansion from NSM005)
	KX-NSX930	101-300 IP Phone Capacity (Expansion from NSM010)
	KX-NSX999	301-640 IP Phone Capacity (Expansion from NSM030)
	KX-NSM102	2-Channel IP Trunk Activation Key (2 IP Trunk)
	KX-NSM104	4-Channel IP Trunk Activation Key (4 IP Trunk)
	KX-NSM108	8-Channel IP Trunk Activation Key (8 IP Trunk)
	KX-NSM116	16-Channel IP Trunk Activation Key (16 IP Trunk)
	KX-NSM201	1-Channel IP Softphone/IP Proprietary Telephone Activation Key (1 IPSoftphone/IP PT)
	KX-NSM205	5-Channel IP Softphone/IP Proprietary Telephone Activation Key (5 IPSoftphone/IP PT)
	KX-NSM210	10-Channel IP Softphone/IP Proprietary Telephone Activation Key (10 IPSoftphone/IP PT)
	KX-NSM220	20-Channel IP Softphone/IP Proprietary Telephone Activation Key (20 IPSoftphone/IP PT)
	KX-NSM501	1-Channel IP Proprietary Telephone Activation Key (1 IP PT)
	KX-NSM505	5-Channel IP Proprietary Telephone Activation Key (5 IP PT)

Category	Model No.	Description
	KX-NSM510	10-Channel IP Proprietary Telephone Activation Key (10 IP PT)
	KX-NSM520	20-Channel IP Proprietary Telephone Activation Key (20 IP PT)
	KX-NSM701	1-Channel SIP Extension Activation Key (1 SIP Extension)
	KX-NSM705	5-Channel SIP Extension Activation Key (5 SIP Extension)
	KX-NSM710	10-Channel SIP Extension Activation Key (10 SIP Extension)
	KX-NSM720	20-Channel SIP Extension Activation Key (20 SIP Extension)
	KX-NSN001	Activation Key for One-look Network (One-look Network)
	KX-NSN002	Activation Key for QSIG Network (QSIG Network)
	KX-NSN101	Built-in Router (Built-in Router AK)
	KX-NSN216	16-channel IPsec Activation Key (16ch IPsec AK)
	KX-NSP001	Standard Activation Key Package (E-mail/Two-way Recording) for 1 User (Std. Pkg 1 User)
	KX-NSP005	Standard Activation Key Package (E-mail/Two-way Recording) for 5 Users (Std. Pkg 5 Users)
	KX-NSP010	Standard Activation Key Package (E-mail/Two-way Recording) for 10 Users (Std. Pkg 10 Users)
	KX-NSP020	Standard Activation Key Package (E-mail/Two-way Recording) for 20 Users (Std. Pkg 20 Users)
	KX-NSP101	Advanced Activation Key Package (E-mail/Two-way Recording/Mobile/CA Pro) for 1 User (Adv. Pkg 1 User)
	KX-NSP105	Advanced Activation Key Package (E-mail/Two-way Recording/Mobile/CA Pro) for 5 Users (Adv. Pkg 5 Users)
	KX-NSP110	Advanced Activation Key Package (E-mail/Two-way Recording/Mobile/CA Pro) for 10 Users (Adv. Pkg 10 Users)
	KX-NSP120	Advanced Activation Key Package (E-mail/Two-way Recording/Mobile/CA Pro) for 20 Users (Adv. Pkg 20 Users)
	KX-NSP201	Mobile Activation Key Package (E-mail/Mobile) for 1 User (Mobile Pkg 1 User)
	KX-NSP205	Mobile Activation Key Package (E-mail/Mobile) for 5 Users (Mobile Pkg 5 Users)

System Components

Category	Model No.	Description
	KX-NSP210	Mobile Activation Key Package (E-mail/Mobile) for 10 Users (Mobile Pkg 10 Users)
	KX-NSP220	Mobile Activation Key Package (E-mail/Mobile) for 20 Users (Mobile Pkg 20 Users)
	KX-NSU001	Activation Key for Recording Time Expansion (REC Time Expansion)
	KX-NSU002	Activation Key for Two-way Recording Control (Two-way REC Control)
	KX-NSU003	Activation Key for Message Backup (Message Backup)
	KX-NSU102	2-Channel Unified Messaging Activation Key (2 UM Port)
	KX-NSU104	4-Channel Unified Messaging Activation Key (4 UM Port)
	KX-NSU201	Activation Key for Unified Messaging E-mail Notification for 1 User (UM/E-mail 1 User)
	KX-NSU205	Activation Key for Unified Messaging E-mail Notification for 5 Users (UM/E-mail 5 Users)
	KX-NSU210	Activation Key for Unified Messaging E-mail Notification for 10 Users (UM/E-mail 10 Users)
	KX-NSU220	Activation Key for Unified Messaging E-mail Notification for 20 Users (UM/E-mail 20 Users)
	KX-NSU299	Activation Key for Unified Messaging E-mail Notification for All Users (UM/E-mail All Users)
	KX-NSU301	Activation Key for Two-way Recording for 1 User (2way REC 1 User)
	KX-NSU305	Activation Key for Two-way Recording for 5 Users (2way REC 5 Users)
	KX-NSU310	Activation Key for Two-way Recording for 10 Users (2way REC 10 Users)
	KX-NSU320	Activation Key for Two-way Recording for 20 Users (2way REC 20 Users)
	KX-NSU399	Activation Key for Two-way Recording for All Users (2way REC All Users)
	KX-NSA010	Activation Key for CA Thin Client Server Connection (CA Thin Client)
	KX-NSA020	Activation Key for Multiple CSTA Connection (CSTA Multiplexer)
	KX-NSA201	Activation Key for CA PRO for 1 User (CA Pro 1 user)
	KX-NSA205	Activation Key for CA PRO for 5 Users (CA Pro 5 users)

Category	Model No.	Description
	KX-NSA210	Activation Key for CA PRO for 10 Users (CA Pro 10 users)
	KX-NSA240	Activation Key for CA PRO for 40 Users (CA Pro 40 users)
	KX-NSA249	Activation Key for CA PRO for 128 Users (CA Pro 128 users)
	KX-NSA301	Activation Key for CA ACD Monitor for 1 ICD Supervisor (CA Supervisor)
	KX-NSA401	Activation Key for CA Operator Console (CA Console)
	KX-NSA901	Activation Key for CA Network Plug-in for 1 User (CA Network 1 user)
	KX-NSA905	Activation Key for CA Network Plug-in for 5 Users (CA Network 5 users)
	KX-NSA910	Activation Key for CA Network Plug-in for 10 Users (CA Network 10 users)
	KX-NSA940	Activation Key for CA Network Plug-in for 40 Users (CA Network 40 users)
	KX-NSA949	Activation Key for CA Network Plug-in for 128 Users (CA Network 128 users)
	KX-NSB0001	Activation Key for Poltys C. Bridge (Poltys C. Bridge)
	KX-NSB0002	Activation Key for PSDN Option-1 (PSDN Option-1)
	KX-NSB0003	Activation Key for PSDN Option-2 (PSDN Option-2)
	KX-NSB0101	Activation Key for Poltys CA RCS-Start for 1 User (Poltys CA RCS-Start 1 user)
	KX-NSB0105	Activation Key for Poltys CA RCS-Start for 5 Users (Poltys CA RCS-Start 5 users)
	KX-NSB0110	Activation Key for Poltys CA RCS-Start for 10 Users (Poltys CA RCS-Start 10 users)
	KX-NSB0149	Activation Key for Poltys CA RCS-Start for 128 Users (Poltys CA RCS-Start 128 users)
	KX-NSB0201	Activation Key for Poltys CA RCS-Extend for 1 User (Poltys CA RCS-Extend 1 user)
	KX-NSB0205	Activation Key for Poltys CA RCS-Extend for 5 Users (Poltys CA RCS-Extend 5 users)
	KX-NSB0210	Activation Key for Poltys CA RCS-Extend for 10 Users (Poltys CA RCS-Extend 10 users)
	KX-NSB0249	Activation Key for Poltys CA RCS-Extend for 128 Users (Poltys CA RCS-Extend 128 users)
	KX-NSF101	Activation Key for CTI interface (CTI interface)
Physical Cards		

Category	Model No.	Description
FAX Card Slot	KX-NS0106	FAX Interface Card (FAX)
DSP Card Slot	KX-NS0110	VoIP DSP Card (S Type) (DSP S)
	KX-NS0111	VoIP DSP Card (M Type) (DSP M)
	KX-NS0112	VoIP DSP Card (L Type) (DSP L)
Storage Memory Card Slot	KX-NS0135	Storage Memory (S Type) (Storage Memory S)
	KX-NS0136	Storage Memory (M Type) (Storage Memory M)
	KX-NS0137	Storage Memory (L Type) (Storage Memory L)
Free Slot	KX-NS0180	2-Port Analogue Trunk / 2-Port SLT Card (SLC2/LCOT2)
	KX-NS0280	4-Port BRI / 2-Port SLT Card (SLC2/BRI4)
	KX-NS0290CE	PRI30 / 2-Port SLT Card (SLC2/PRI30)
	KX-NS0290	PRI23 / 2-Port SLT Card (SLC2/PRI23)
	KX-NS0130	Stacking Master Card (STACK-M)
Doorphone Slot	KX-NS0161	Doorphone Interface Card (DOORPHONE)

¹ Note that the types of activation keys are subject to change without notice. For CA activation keys, refer to the documentation for CA.

System Components for Legacy Gateways

For details about supported optional service cards and Power Supply Units (PSUs), refer to the Installation Manual of the corresponding PBX.

KX-NCP500/KX-NCP1000/KX-NS1020

Category	Model No.	Description
Legacy Gateways	KX-NCP500	KX-NCP500 as Legacy Gateway Unit
	KX-NCP1000	KX-NCP1000 as Legacy Gateway Unit
	KX-NS1020	KX-NS1020 Expansion Cabinet
Legacy Gateway Cards	KX-NS0131	Stacking Card for KX-NCP Series (STACK-S (NCP))
Physical Trunk Cards	KX-NCP1180	4-Port Analogue Trunk Card (LCOT4)
	KX-NCP1187	T-1 Trunk Card (T1)
	KX-NCP1188	E-1 Trunk Card (E1)
	KX-NCP1280	2-Port BRI Card (BRI2)
	KX-NCP1290	PRI Card (PRI23)
	KX-NCP1290CE	PRI Card (PRI30)
	KX-NCP1290CJ	PRI Card (PRI30)

Category	Model No.	Description
Physical Extension Cards	KX-NCP1170	4-Port Digital Hybrid Extension Card (DHLC4)
	KX-NCP1171	8-Port Digital Extension Card (DLC8)
	KX-NCP1172	16-Port Digital Extension Card (DLC16)
	KX-NCP1173	8-Port Single Line Telephone Extension Card (SLC8)
	KX-NCP1174	16-Port Single Line Telephone Extension Card (SLC16)
Other Physical Cards	KX-NCP1190	Optional 3-Slot Base Card (OPB3)
	KX-TDA0161	4-Port Doorphone Card (DPH4)
	KX-TDA0162	2-Port Doorphone Card (German Type) (DPH2)
	KX-TDA0164	4-Port External Input/Output Card (EIO4)
	KX-TDA0166	16-Channel Echo Canceller Card (ECHO16)

KX-TDE100/KX-TDE200/KX-TDA100/KX-TDA200/KX-TDA100D

Category	Model No.	Description
Legacy Gateways	KX-TDE100	KX-TDE100 as Legacy Gateway Unit
	KX-TDE200	KX-TDE200 as Legacy Gateway Unit
	KX-TDA100	KX-TDA100 as Legacy Gateway Unit
	KX-TDA200	KX-TDA200 as Legacy Gateway Unit
	KX-TDA100D	KX-TDA100D as Legacy Gateway Unit
Legacy Gateway Cards	KX-NS0132	Stacking Card for KX-TDE Series (STACK-S (TDE))
Physical Trunk Cards	KX-TDA0180	8-Port Analogue Trunk Card (LCOT8)
	KX-TDA0181	16-Port Analogue Trunk Card (LCOT16)
	KX-TDA0182	8-Port DID Card (DID8)
	KX-TDA0183	4-Port Analogue Trunk Card (LCOT4)
	KX-TDA0184	8-Port E & M Trunk Card (E&M8)
	KX-TDA0187	T-1 Trunk Card (T1)
	KX-TDA0188	E-1 Trunk Card (E1)
	KX-TDA0284	4-Port BRI Card (BRI4)
	KX-TDA0288	8-Port BRI Card (BRI8)
	KX-TDA0290CE	PRI Card (PRI30)
	KX-TDA0290CJ	PRI Card (PRI30)
	KX-TDA0290	PRI Card (PRI23)
	KX-TDA1180	8-Port Analogue Trunk Card with CID (CLCOT8) ¹

Category	Model No.	Description
Physical Extension Cards	KX-TDA0143	4 Cell Station Interface Card (CSIF4)
	KX-TDA0144	8 Cell Station Interface Card (CSIF8)
	KX-TDA0170	8-Port Digital Hybrid Extension Card (DHLC8) ²
	KX-TDA0171	8-Port Digital Extension Card (DLC8)
	KX-TDA0172	16-Port Digital Extension Card (DLC16)
	KX-TDA0173	8-Port Single Line Telephone Extension Card (SLC8) ²
	KX-TDA0174	16-Port Single Line Telephone Extension Card (SLC16) ²
	KX-TDA0175	16-Port Single Line Telephone Extension with Message Lamp Card (MSLC16) ²
	KX-TDA0177	16-Port Single Line Telephone Extension Card with Caller ID (CSLC16) ²
	KX-TDA1176	16-Port Single Line Telephone Extension with Caller ID and Message Lamp Card (MCSLC16) ³
	KX-TDA1178	24-Port Single Line Telephone Extension with Caller ID and Message Lamp Card (MCSLC24) ³
Other Physical Cards	KX-TDA0161	4-Port Doorphone Card (DPH4)
	KX-TDA0162	2-Port Doorphone Card (German Type) (DPH2)
	KX-TDA0164	4-Port External Input/Output Card (EIO4)
	KX-TDA0166	16-Channel Echo Canceller Card (ECHO16)
	KX-TDA0168	Extension Caller ID Card (EXT-CID)
	KX-TDA0189	8-Port Caller ID/Pay Tone Card (CID/PAY8)
	KX-TDA0190	Optional 3-Slot Base Card (OPB3)
	KX-TDA0193	8-Port Caller ID Card (CID8)
	KX-TDA1186	8-Port Analogue Trunk Card with CID Daughter Card (CLCOT8E) ¹
PSUs⁴	KX-TDA0103	L-Type Power Supply Unit (PSU-L)
	KX-TDA0104	M-Type Power Supply Unit (PSU-M)
	KX-TDA0108	S-Type Power Supply Unit (PSU-S)

¹ KX-TDA100D only.² Except KX-TDA100D.³ Except KX-TDA100/KX-TDA200.⁴ Some PSUs are only supported by certain PBXs. For more details, refer to the Installation Manual of the corresponding PBX.

KX-TDE600/KX-TDE620/KX-TDA600/KX-TDA620

Category	Model No.	Description
Legacy Gateways	KX-TDE600 KX-TDE620 KX-TDA600 KX-TDA620	KX-TDE600 as Legacy Gateway Unit KX-TDE620 as Legacy Gateway Unit KX-TDA600 as Legacy Gateway Unit KX-TDA620 as Legacy Gateway Unit
Legacy Gateway Cards	KX-NS0132	Stacking Card for KX-TDE Series (STACK-S (TDE))
Physical Trunk Cards	KX-TDA0182 KX-TDA0184 KX-TDA0187 KX-TDA0188 KX-TDA0284 KX-TDA0288 KX-TDA0290CE KX-TDA0290CJ KX-TDA0290	8-Port DID Card (DID8) 8-Port E & M Trunk Card (E&M8) T-1 Trunk Card (T1) E-1 Trunk Card (E1) 4-Port BRI Card (BRI4) 8-Port BRI Card (BRI8) PRI Card (PRI30) PRI Card (PRI30) PRI Card (PRI23)
Physical Extension Cards	KX-TDA0143 KX-TDA0144 KX-TDA0170 KX-TDA0171 KX-TDA0172 KX-TDA0173 KX-TDA0177 KX-TDA6174 KX-TDA6175 KX-TDA6178 KX-TDA6179 KX-TDA6381 KX-TDA6382	4 Cell Station Interface Card (CSIF4) 8 Cell Station Interface Card (CSIF8) 8-Port Digital Hybrid Extension Card (DHLC8) 8-Port Digital Extension Card (DLC8) 16-Port Digital Extension Card (DLC16) 8-Port Single Line Telephone Extension Card (SLC8) 16-Port Single Line Telephone Extension Card with Caller ID (CSLC16) 16-Port Single Line Telephone Extension Card (ESLC16) 16-Port Single Line Telephone Extension with Message Lamp Card (EMSLC16) 24-Port Single Line Telephone Extension Card with Caller ID (ECSLC24) 24-Port Single Line Telephone Extension with Caller ID and Message Lamp Card (EMSLC24) 16-Port Analogue Trunk Card w/o CID (ELCOT16) 16-Port Analogue Trunk Card with CID16 (ELCOT16)
Other Physical Cards	KX-TDA0161 KX-TDA0162	4-Port Doorphone Card (DPH4) 2-Port Doorphone Card (German Type) (DPH2)

System Components

Category	Model No.	Description
	KX-TDA0164	4-Port External Input/Output Card (EIO4)
	KX-TDA0168	Extension Caller ID Card (EXT-CID)
	KX-TDA0189	8-Port Caller ID/Pay Tone Card (CID/PAY8)
	KX-TDA0190	Optional 3-Slot Base Card (OPB3)
	KX-TDA0193	8-Port Caller ID Card (CID8)
	KX-TDA6166	16-Channel Echo Canceller Card (EECHO16)
PSUs	KX-TDA0103	L-Type Power Supply Unit (PSU-L)
	KX-TDA0104	M-Type Power Supply Unit (PSU-M)

Unsupported System Components for Legacy Gateways

The following components are not supported for legacy gateways.

Model No.	Description
KX-NCP1104	4-Channel VoIP DSP Card (DSP4)
KX-TDA0105	Memory Expansion Card (MEC)
KX-TDA0191	4-Channel Message Card (MSG4)
KX-TDA0192	2-Channel Simplified Voice Message Card (ESVM2)
KX-TDA0194	4-Channel Simplified Voice Message Card (ESVM4)
KX-TDA0196	Remote Card (RMT)
KX-TDA0410	CTI Link Card (CTI-LINK)
KX-TDA0470	16-Channel VoIP Extension Card (IP-EXT16)
KX-TDA0480	4-Channel VoIP Gateway Card (IP-GW4)
KX-TDA0484	4-Channel VoIP Gateway Card (IP-GW4E)
KX-TDA0490	16-Channel VoIP Gateway Card (IP-GW16)
KX-TDE0105	Memory Expansion Card (IPCMEC)
KX-TDE0110	16-Channel VoIP DSP Card (DSP16)
KX-TDE0111	64-Channel VoIP DSP Card (DSP64)

Equipment Compatibility for KX-NS1000

The PBX supports the following equipment:

Cell Stations

DECT

- DECT 8-Channel IP Cell Station Unit Using a V-IPCS4 Card for DECT Portable Station (KX-NCP0158CE)

DECT 6.0

- DECT 6.0 8-Channel IP Cell Station Unit Using a V-IPCS4 Card for DECT 6.0 Portable Station (KX-NCP0158)

SIP based DECT

- DECT Cell Station Unit (SIP) Using a V-UTEXT32 Card for DECT Portable Station (SIP) (KX-UDS124)

Doorphones

- Doorphone (KX-T30865, KX-T7765)

Telephones**Panasonic Proprietary Telephones**

- IP proprietary telephones (e.g., KX-NT300 series, KX-NT500 series)
- IP softphones (e.g., KX-NCS8100)
- Portable stations (e.g., KX-TCA364, KX-WT115)

SIP Phones

- KX-UT series SIP phones (e.g., KX-UT133, KX-UT248, KX-UT670)
- KX-UDT series portable stations (e.g., KX-UDT111)
- IP conferencing phones (e.g., KX-NT700)
- Third party SIP phones (SIP hardphones/SIP softphones)

Other

- Single line telephones

Note

- For the equipment (e.g., Add-on Key Module, USB Module, Headset) that can be connected to a particular telephone, refer to the telephone's manual.
- For other equipment that can be connected to the PBX, refer to "2.1.2 System Connection Diagram".
- The PBX does not support the following Panasonic proprietary telephones:
 - Analogue proprietary telephones
 - Digital proprietary telephones
 - KX-NT136 IP proprietary telephone
 - KX-NT400 IP proprietary telephone
 - KX-HGT100 SIP telephone

Trunk Adaptors

- E1 Trunk Adaptor (KX-NS8188)
- PRI Adaptor (KX-NS8290)

Equipment Compatibility for Legacy Gateways

You can connect the following PBXs to a KX-NS1000 as legacy gateways.

- KX-NS1020
- KX-NCP series PBX
- KX-TDE series PBX
- KX-TDA series PBX
- KX-TDA100D

Connecting legacy gateways expands the usage of legacy terminals and trunks.

If a legacy gateway is connected to a KX-NS1000, the following equipment is also supported.

Note

In this manual, KX-TDA100D is not included in KX-TDA series.

Cell Stations**DECT**

- 2-Channel Cell Station Unit Using a DHLC/DLC Card (PT-interface CS) for DECT Portable Station (KX-TDA0141CE)

- 4-Channel Cell Station Unit Using a CSIF Card for DECT Portable Station (KX-TDA0142CE)
- 2-Channel Cell Station Unit Using a DHLC/DLC Card (PT-interface CS) for DECT Portable Station (KX-TDA0155CE)
- 2-Channel Cell Station Unit Using a DHLC/DLC Card (PT-interface CS) for DECT Portable Station (KX-TDA0155LA)
- 4-Channel Cell Station Unit Using a CSIF Card for DECT Portable Station (KX-TDA0156CE)
- 8-Channel High-density Cell Station Unit Using a DHLC/DLC Card (PT-interface CS) for DECT Portable Station (KX-TDA0158CE)

DECT 6.0

- DECT 6.0 2-Channel Cell Station Unit Using a DHLC/DLC Card (PT-interface CS) for DECT 6.0 Portable Station (KX-TDA0155)
- DECT 6.0 4-Channel Cell Station Unit Using a CSIF Card for DECT 6.0 Portable Station (KX-TDA0156)
- DECT 6.0 8-Channel Cell Station Unit Using a DHLC/DLC Card (PT-interface CS) for DECT 6.0 Portable Station (KX-TDA0158)

2.4 GHz CS

- 2-Channel Cell Station Unit Using a DHLC/DLC Card (PT-interface CS) for 2.4 GHz Portable Station (KX-TDA0141)
- 3-Channel Cell Station Unit Using a CSIF Card for 2.4 GHz Portable Station (KX-TDA0142)
- 2-Channel Cell Station Unit Using a DHLC/DLC Card (PT-interface CS) for 2.4 GHz Portable Station (KX-TDA0151)
- 3-Channel Cell Station Unit Using a CSIF Card for 2.4 GHz Portable Station (KX-TDA0152)

Telephones

Panasonic Proprietary Telephones

- Digital Proprietary Telephone (e.g., KX-DT300 series, KX-DT500 series, KX-T7400 series, KX-T7500 series, and KX-T7600 series)
- Portable Station (e.g., KX-TD7600 series)
- DSS Console (e.g., KX-DT390, KX-DT590)
- Analogue Proprietary Telephone (e.g., KX-T7700 series)

Note

The following Panasonic proprietary telephones are not available even if a legacy gateway is connected:

- KX-NT136 IP proprietary telephone
- KX-HGT100 SIP telephone
- KX-NT400 IP proprietary telephone
- KX-TDA0300 PC Console
- KX-T7000 series proprietary telephone
- KX-T7200 series proprietary telephone
- KX-T7300 series proprietary telephone

Voice Processing System

Voice Processing System (e.g., KX-TVM series)

Notice

- This PBX supports SIP extensions. However, some PBX features may not be available depending on the type of telephone.
- Under power failure conditions, the connected telephones may not operate. Please ensure that a separate telephone, not dependent on local power, is available for emergency use.
- Prior to connection of this product, please verify that the intended operating environment is supported. Satisfactory performance cannot be guaranteed for the following:
 - interoperability and compatibility with all devices and systems connected to this product

- proper operation and compatibility with services provided by telecommunications companies over connected networks

Note

- Some optional hardware, software, and features are not available in some countries/areas. Please consult your certified Panasonic dealer for more information.
- In this manual, the suffix of each model number (e.g., KX-NS1000**NE**) is omitted unless necessary.

List of Abbreviations

- CA → Communication Assistant
- IP-PT → IP Proprietary Telephone
- PS → Portable Station
- SIP Extension → Extensions of the PBX which use Session Initiation Protocol for communication.
- SLT → Single Line Telephone
- S-PS → SIP-CS compatible Portable Station
- APT → Analogue Proprietary Telephone
- DPT → Digital Proprietary Telephone
- SIP-CS → SIP based DECT Cell Station unit

Introduction

This Installation Manual is designed to serve as an overall technical reference for the Panasonic Pure IP-PBX, KX-NS1000. It provides instructions for installing the hardware, and programming the PBX using Web Maintenance Console.

The Structure of this Manual

This manual contains the following sections:

Section 1 Safety Precautions

Provides important information intended to prevent personal injury and property damage.

Section 2 System Outline

Provides general information on the PBX, including the system capacity and specifications.

Section 3 Information about the Activation Keys

Provides information on activation keys, including how to obtain activation keys.

Section 4 Installation

Describes the procedures to install the PBX. Detailed instructions for planning the installation site, optional service cards, and cabling of peripheral equipment are provided. Further information on system expansion and peripheral equipment installation is included.

Section 5 Programming Information

Describes the installation procedure, structure, and functions of the Web Maintenance Console for programming IP telephones and the PBX. Further information on programming the PBX for use with SIP trunks and a VoIP network is included.

Section 6 Information about Stacking PBXs

Provides information about stacking PBXs as legacy gateways.

Section 7 Troubleshooting

Provides information on the PBX and telephone troubleshooting.

Section 8 Networking Information

Provides information about topics such as using the PBX in a VoIP network, and the TCP ports used by the PBX.

Section 9 Appendix

Provides information about PBX Region Suffix Codes and Areas, System Prompt Languages, and the revision history.

About the Other Manuals

Along with this Installation Manual, the following manuals are available:

Feature Guide

Describes all basic, optional and programmable features of the PBX.

PC Programming Manual

Provides step-by-step instructions for performing system programming using a PC.

User Manual

Provides operating instructions for end users using IP-PTs, SIP phones, SLTs, PSs, or DSS Consoles.

About the software version of your PBX

The contents of this manual apply to PBXs with a certain software version, as indicated on the cover of this manual. To confirm the software version of your PBX, see "How do I confirm the software version of the PBX or installed cards?" in "2.3 Frequently Asked Questions (FAQ)" of the PC Programming Manual.

Trademarks

- The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc., and any use of such marks by Panasonic Corporation is under licence.

- Microsoft, Outlook, Internet Explorer, Windows and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Mozilla and Firefox are registered trademarks of the Mozilla Foundation.
- All other trademarks identified herein are the property of their respective owners.
- Microsoft product screen shot(s) reprinted with permission from Microsoft Corporation.

Table of Contents

1 Safety Precautions	21
1.1 For Your Safety	22
1.2 Important Safety Instructions	29
1.3 Precautions	30
1.4 Data Security	33
2 System Outline	35
2.1 Basic System Construction	36
2.1.1 System Configurations	36
2.1.2 System Connection Diagram	39
2.2 Optional Equipment	41
2.2.1 Optional Equipment	41
2.3 Specifications	43
2.3.1 General Description	43
2.3.2 Characteristics	44
2.3.3 System Capacity	45
3 Information about the Activation Keys	67
3.1 Information about the Activation Keys	68
3.1.1 Type and Maximum Number of Activation Keys	68
3.1.2 Activation Key Code and Key Management System	88
3.1.3 Using CTI Applications	89
4 Installation	91
4.1 Before Installation	92
4.1.1 Before Installation	92
4.2 Installation of the PBX	94
4.2.1 Unpacking	94
4.2.2 Names and Locations	95
4.2.3 Opening/Closing the Top Cover	96
4.2.4 Frame Earth Connection	99
4.2.5 Installing/Removing the Optional Service Cards	100
4.2.6 Installing/Removing the Storage Memory Card	113
4.2.7 Types of Connectors	117
4.2.8 Attaching a Ferrite Core	118
4.2.9 19-inch Rack Mounting	119
4.2.10 Placing the PBX on a Desktop	120
4.2.11 Wall Mounting	121
4.2.12 Surge Protector Installation	125
4.3 The Mother Board and Expansion Cards	128
4.3.1 Mother Board	128
4.3.2 Storage Memory Card (installed by default), Storage Memory S Card (KX-NS0135), Storage Memory M Card (KX-NS0136), Storage Memory L Card (KX-NS0137)	132
4.3.3 DSP S Card (KX-NS0110), DSP M Card (KX-NS0111), DSP L Card (KX-NS0112)	133
4.3.4 FAX Card (KX-NS0106)	135
4.4 Virtual Cards	136
4.5 Physical Trunk and Extension Cards	138
4.5.1 SLC2/LCOT2 Card (KX-NS0180)	138
4.5.2 SLC2/BRI4 Card (KX-NS0280)	140
4.5.3 SLC2/PRI30 Card (KX-NS0290CE)	144
4.5.4 SLC2/PRI23 Card (KX-NS0290)	147

4.6	Stacking Cards	150
4.6.1	STACK-M Card (KX-NS0130)	150
4.6.2	STACK-S (NCP) Card (KX-NS0131)	152
4.6.3	STACK-S (TDE) Card (KX-NS0132)	154
4.7	The Doorphone Card	158
4.7.1	DOORPHONE Card (KX-NS0161)	158
4.8	Connection of SLTs	160
4.8.1	Maximum Cabling Distances of the Extension Wiring (Twisted Cable)	160
4.9	Connecting to a Doorphone, Door Opener, and/or External Sensor	161
4.10	Connection of Peripherals	164
4.11	LAN Connection	169
4.11.1	LAN Connection for the Main Unit	169
4.11.2	LAN Connections for IP Telephones	171
4.12	Power Failure Ports	174
4.13	Starting the KX-NS1000	175
5	Programming Information	179
5.1	Overview of Web Maintenance Console	180
5.2	PC Connection	181
5.3	Starting Web Maintenance Console	183
5.4	Programming the PBX	196
5.4.1	Easy Setup Wizard	196
5.4.2	Enabling the DHCP Server Feature	202
5.4.3	Installing the Virtual IP Cards to the PBX	203
5.4.4	Installing Additional Activation Keys	203
5.4.5	Configuration of the Activation Keys	204
5.5	Programming a One-look Network	205
5.6	Programming an H.323 QSIG Network	207
5.6.1	Assigning the Hunt Pattern	207
5.6.2	Programming the Address Translation Table	208
5.6.3	Programming the Network Settings	210
5.7	Programming SIP Trunks	214
5.8	Assigning Networking Information to IP Telephones	216
5.8.1	Assigning IP Addressing Information	216
5.8.2	Setting VLAN Parameters	236
5.8.3	Setting LLDP Parameters	239
5.8.4	Setting Diffserv Parameters	243
5.8.5	Configuration of IP Ports	246
5.8.6	ECO mode (KX-NT500 series only)	252
5.9	Registering IP Telephones	254
5.9.1	Registering IP Telephones	254
5.9.2	De-registering IP Telephones	260
5.9.3	Installing SIP Phones at a Remote Site	263
5.9.4	Installing IP Phones at a Remote Site with a Built-in Media Relay Gateway	269
5.10	Configuration of Users	277
5.11	Programming E-mail Integration for UM Voice/Fax Messages	279
5.12	Automatic Configuration of Mailboxes	283
6	Information about Stacking PBXs	285
6.1	Information about Stacking PBXs	286
6.2	Methods of Stacking PBXs	287
7	Troubleshooting	291
7.1	Troubleshooting	292
7.1.1	Installation	292

Table of Contents

7.1.2	Connection	295
7.1.3	Operation	296
7.1.4	Error Messages	298
7.1.5	Restarting the KX-NS1000	300
7.1.6	Troubleshooting by Error Log	302

8 Networking Information 305

8.1	Information about Using an IP Network	306
8.1.1	Using a VoIP Network with the PBX	306
8.1.2	DHCP (Dynamic Host Configuration Protocol) Server	309
8.1.3	VLAN (Virtual LAN)	310
8.1.4	Jitter Buffer	311
8.1.5	Voice Activity Detection (VAD)	311
8.1.6	Network Configuration	312
8.1.7	Network Devices	316
8.1.8	QoS (Quality of Service)	317
8.1.9	Network Time Protocol (NTP)	318
8.2	H.323 Trunks	319
8.2.1	Avoid Multiple IP Networks	319
8.2.2	Gatekeeper	320
8.2.3	Bandwidth Assessment	320
8.2.4	Virtual VoIP Gateway Card Specifications	323
8.3	SIP Trunks	324
8.3.1	IP Telephony Service	324
8.3.2	SIP Requirements	327
8.3.3	Router Requirements	327
8.3.4	Bandwidth Requirements	327
8.3.5	Virtual SIP Trunk Card Specifications	329
8.4	Types of PBX Networks	330
8.4.1	One-look Network	330
8.4.2	One-look Networking Survivability	333
8.4.3	H.323 QSIG Network	340
8.4.4	Working with Multiple PBX Networks	341
8.5	Port Security	342
8.6	Built-in Router	346
8.6.1	Built-in Router Overview	346
8.6.2	WAN Connection	348
8.6.3	DHCP Relay Agent	349
8.6.4	Dynamic DNS	350
8.6.5	DNS Client	351
8.6.6	Protocol Bridge—IPv6 Bridge	352
8.6.7	Protocol Bridge—PPPoE Bridge	352
8.6.8	MAC Address Clone	353
8.6.9	Routing	354
8.6.10	Firewall	354
8.6.11	Firewall—Packet Filtering	355
8.6.12	Firewall—Stateful Packet Inspection	356
8.6.13	Firewall—DoS Protection	356
8.6.14	Firewall—Other Security Settings	357
8.6.15	Dynamic NAPT (IP masquerade)	358
8.6.16	Static NAPT (Port Forwarding)	358
8.6.17	DMZ Host	359
8.6.18	VoIP Port Dynamic Setting	359
8.6.19	IPsec Pass-through	360
8.6.20	PPTP Pass-through	361

8.6.21	L2TP Pass-through	361
8.6.22	Quality of Service (QoS)	362
8.6.23	VPN—IPsec	363
8.6.24	VPN—VPSS Setting	366
8.6.25	Router Command	368
8.6.26	WAN Port Mirroring	368
9	Appendix	369
9.1	PBX Region Suffix Codes and Areas	370
9.2	System Prompt Languages	372
9.3	Revision History	374
9.3.1	PCMPR Software File Version 002.0xxxx	374
9.3.2	PCMPR Software File Version 002.1xxxx	375
9.3.3	PCMPR Software File Version 003.0xxxx	376
9.3.4	PCMPR Software File Version 003.2xxxx	378

Table of Contents

Section 1

Safety Precautions

This section provides important information intended to prevent personal injury and property damage.

1.1 For Your Safety

To prevent personal injury and/or damage to property, be sure to observe the following safety precautions.

The following symbols classify and describe the level of hazard and injury caused when this unit is operated or handled improperly.



WARNING

This notice means that misuse could result in death or serious injury.



CAUTION

This notice means that misuse could result in injury or damage to property.

The following types of symbols are used to classify and describe the type of instructions to be observed.



This symbol is used to alert users to a specific operating procedure that must not be performed.



This symbol is used to alert users to a specific operating procedure that must be followed in order to operate the unit safely.



WARNING

For All Telephone Equipment



- Do not install the product in any other way than described in relevant manuals.
- Do not install the product in a place exposed to rain or moisture, or a place where water, oil, or other liquids can drip or splash onto on the product. Such conditions can lead to fire or electric shock, and may impair the performance of the product.
- Do not install the system in the following locations:
 - a. Areas where shocks or vibrations are frequent or strong. Such activity may lead to the product falling over and causing injury, or may impair the product's performance.
 - b. Areas with high amounts of dust. High amounts of dust can lead to fire or electric shock, and impair the performance of the product.
- Do not place the product on an unstable or uneven surface. If the product were to fall over, it may cause injury or damage to the product.
- Do not supply power to a combination of devices that exceeds the total rated capacity of the wall outlets or extension cables used. If outlets, power strips, extension cords, etc. are used in a manner that exceeds their rated capacity, they emit large amounts of heat, which could cause a fire.



- The product must only be installed and serviced by qualified service personnel. The product should be used as-is from the time of purchase; it should not be disassembled or modified. Disassembly or modification can cause a fire, electric shock, or damage to the product.
- Follow all warnings and instructions marked on the product.
- The hook clip poses a choking hazard. Keep the hook clip out of reach of children.
- Products that require a power source should only be connected to the type of electrical power supply specified on the product label. If you are not sure of the type of power supply to your home, consult your dealer or local power company.
- For safety purposes some products are equipped with an earthed plug. If you do not have an earthed outlet, please have one installed. Do not bypass this safety feature by tampering with the plug.
- When installing telephone wiring, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:
 - a. Never install telephone wiring during a lightning storm.
 - b. Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
 - c. Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
 - d. Use caution when installing or modifying telephone lines.
 - e. Anti-static precautions should be taken during installation.
- Unplug the product from the wall outlet and have it serviced by qualified service personnel in the following cases:
 - a. When the power supply cord or plug is damaged or frayed.
 - b. If liquid has been spilled into the product.
 - c. If the product has been exposed to rain or water.

1.1 For Your Safety

- d. If the product does not operate according to the operating instructions. Adjust only the controls that are explained in the operating instructions. Improper adjustment of other controls may result in damage and may require service by a qualified technician to restore the product to normal operation.
- e. If the product has been dropped or the cabinet has been damaged.
- f. If product performance deteriorates.

For the PBX



- Do not insert foreign objects of any kind into this product, as they may touch dangerous voltage points or short out parts that could result in a fire or electric shock.
- Do not pull, bend, rest objects on, or chafe the power cord and plug. Damage to the power cord or plug can cause fire or electric shock.
- Do not attempt to repair the power cord or plug. If the power cord or plug is damaged or frayed, contact an authorised Panasonic Factory Service Centre for a replacement.



- When mounting the PBX on a 19-inch rack, only use the 19-inch rack mounting equipment (attachment bracket, screws) included with the PBX.
- If damage to the unit exposes any internal parts, disconnect the power supply cord immediately and return the unit to your dealer.
- To prevent fires, electric shock, injury, or damage to the product, be sure to follow these guidelines when performing any wiring or cabling:
 - a. Before performing any wiring or cabling, unplug the product's power cord from the outlet. After completing all wiring and cabling, plug the power cord back into the outlet.
 - b. When laying cables, do not bundle the product's power cord with the power cords of other devices.
 - c. Do not place any objects on top of the cables connected to the PBX.
 - d. When running cables along the floor, use protectors to prevent the cables from being stepped on.
 - e. Do not run any cables under carpeting.
- Unplug this unit from the AC outlet if it emits smoke, an abnormal smell or makes unusual noise. These conditions can cause fire or electric shock. Confirm that smoke has stopped and contact an authorised Panasonic Factory Service Centre.
- Make sure that the wall that the unit will be attached to is strong enough to support the unit (approx. 35 kg). If not, it is necessary for the wall to be reinforced.
- Only use the wall-mounting equipment (anchor plugs, screws, metal brackets) included with the PBX and the wall mounting kit. Make sure that the wall is made of concrete.
- The earthing wire of the AC cable has an effect against external noise and lightning strikes, but it may not be enough to protect the PBX and to ensure electromagnetic compatibility. A permanent connection between earth and the earth terminal of the PBX must be made.
- Proper earthing (connection to earth) is very important to reduce the risk to the user of electrocution or to protect the PBX from the bad effects of external noise in the case of a lightning strike. (See "4.2.4 Frame Earth Connection".)
- Plug the power cord firmly into an AC outlet. Otherwise, it can cause fire or electric shock.
- Be careful not to drop any components. Dropping components may damage them or cause an injury.
- Make sure that the AC outlet is properly earthed, then securely connect the 3-pin AC plug including the earthed pin.

- A lithium battery is used in the mother board, STACK-S (NCP) card, and STACK-S (TDE) card. There is a risk of explosion if the battery is replaced with an incorrect type. Dispose of used batteries according to the manufacturer's instructions.



CAUTION

For All Telephone Equipment



- The product should be kept free of dust, moisture, high temperature (more than 40 °C) and vibration, and should not be exposed to direct sunlight.
- Unplug the product from the wall outlet before cleaning. Wipe the product with a soft cloth. Do not clean with abrasive powders or with chemical agents such as benzine or thinner. Do not use liquid cleaners or aerosol cleaners.

For the PBX



- Do not install the system in the following locations:
 - a. In direct sunlight and hot, cold, or humid places. (Temperature range: 0 °C to 40 °C)
 - b. Areas where sulphuric gases may be present, such as near thermal springs.
 - c. Near devices that generate high frequencies, such as sewing machines or electric welders.
 - d. Locations where other objects will obstruct the area around the PBX. Be especially careful to leave at least 5 cm to the sides of the PBX for ventilation.
 - e. Locations where condensation can occur.
- Do not block the openings of the PBX. Allow space of at least 20 cm above and 10 cm at the sides of the PBX.
- When the PBX is mounted on a 19-inch rack, do not block the openings of the PBX. Allow space of at least 10 cm around the PBX's fan.
- When installing or removing the Storage Memory Card, do not put pressure on any parts of the mother board. Doing so may result in damage to the PBX.
- When installing or removing the optional service cards, do not put pressure on any parts of the mother board. Doing so may result in damage to the PBX.
- The Storage Memory Card contains software for all the processes of the PBX and all the customer data. Therefore, do not allow unauthorised access to prevent data leakage.
- Once you have started the PBX, if you unplug the PBX, do not initialise it again as described in "System Initialisation Procedure". Otherwise, your programmed data will be cleared. To restart the PBX, refer to "7.1.5 Restarting the KX-NS1000".



- Before touching the product (PBX, cards, etc.), discharge static electricity by touching ground or wearing an earthing strap. Failure to do so may cause the PBX to malfunction due to static electricity.

1.1 For Your Safety

- When relocating the equipment, first disconnect the telecom connection before disconnecting the power connection. When the unit is installed in the new location, reconnect the power first, and then reconnect the telecom connection.
- The power supply cord is used as the main disconnect device. Ensure that the AC outlet is located near the equipment and is easily accessible.
- Slots and openings in the front, back and bottom of the cabinet are provided for ventilation; to protect it from overheating, these openings must not be blocked or covered. The openings should never be blocked by placing the product on a bed, sofa, rug, or other similar surface while in use. The product should never be placed near or over a radiator or other heat source. This product should not be placed in a sealed environment unless proper ventilation is provided.
- Make sure that the surface behind the PBX is flat and free of obstacles, so that the openings on the back of the PBX will not be blocked.
- Make sure that the surface behind the PBX is not made of wood.
- When this product is no longer in use, make sure to detach it from the rack or wall.
- Use only the AC power cord included with the PBX.
- A certified power supply cord has to be used with this equipment. The relevant national installation and/or equipment regulations shall be considered. A certified power supply cord not lighter than ordinary polyvinyl chloride flexible cord according to IEC 60227 (designation H05VV-F 3G 0.75 mm²) shall be used.
- When the PBX is mounted on a 19-inch rack, make sure that the installation of the unit does not cause the temperature of the rack to exceed its limit.
- Make sure to install all necessary optional service cards in the PBX before performing the wall mounting procedure. If it is necessary to install or remove a card, make sure to detach the PBX from the wall before installing or removing the card.
- When driving the screws into the wall, be careful to avoid touching any metal laths, wire laths or plates in the wall.
- When placing the PBX onto the wall, make sure that the arrows on the metal brackets are pointing upward. If the arrows are not pointing upward, the PBX may fall, resulting in injury.
- When opening the top cover, the power switch must be turned off.
- For safety reasons, close the top cover and tighten the screws before operating the PBX.
- If the PBX is not installed properly using the securing correct methods, the PBX may fall causing serious damage.
- When the PBX is placed on a desktop, make sure that the PBX is placed as indicated in "4.2.10 Placing the PBX on a Desktop". Do not place it on its side or upside down.
- Performing surge protection is essential. Make sure to follow the instructions in "4.2.12 Surge Protector Installation".
- It is strongly recommended to use SSL encrypted communication when the PC is accessing the PBX via the Internet. To use SSL encryption, routers must have a port set up for https communication.
- To prevent data leakage, render the Storage Memory Card physically unusable before disposal.
- Avoid using the same AC outlet for computers and other office equipment, as noise generated by such equipment may hamper system performance or interrupt the system.
- Unplug the system from its power source when wiring, and plug the system back in only after all wiring is completed.
- Trunks should be installed with surge protectors. For details, refer to "4.2.12 Surge Protector Installation".
- When installing or removing the Storage Memory Card, the power switch must be turned off.
- When installing or removing the optional service cards, the power switch must be turned off.
- For earthing wire, green-and-yellow insulation is required, and the cross-sectional area of the conductor must be more than 0.75 mm² or 18 AWG.
- When connecting a SLC2/BRI4, SLC2/PRI30 or SLC2/PRI23 card to the trunk, connect through an NT1; do not connect to the U interface of the trunk directly.
- PRI ports of SLC2/PRI30 and SLC2/PRI23 cards are SELV ports and should only be connected to SELV services.

- The MOH port and Pager port are SELV ports and should only be connected to approved SELV devices, or in Australia, via a Line Isolation Unit with a Telecommunications Compliance Label.
- To protect the system, keep the following in mind:
 - a. Make sure that both connector cases (frame ground) of the RS-232C cross cable (shielded cable) are conductive. If they are not conductive, make sure that both connector cases of the cable are firmly connected.
 - b. If this is not possible, connect the frame of the PBX to the frame of the PC/Printer using an earthing wire in order to prevent difference in the electrical potentials.

Notice

For All Telephone Equipment

- Read and understand all instructions.

For the PBX

- Keep the unit away from heating appliances and devices that generate electrical noise such as fluorescent lamps, motors and televisions. These noise sources can interfere with the performance of the PBX.
- If you are having problems making calls to outside destinations, follow this procedure to test the trunks:
 - a. Disconnect the PBX from all trunks.
 - b. Connect known working SLTs to those trunks.
 - c. Make a call to an external destination using those SLTs.If a call cannot be carried out correctly, there may be a problem with the trunk that the SLT is connected to. Contact your telephone company.
- If all SLTs operate properly, there may be a problem with your PBX. Do not reconnect the PBX to the trunks until it has been serviced by an authorised Panasonic Factory Service Centre.

1.2 Important Safety Instructions

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Do not use the product near water, for example, near a bathtub, wash bowl, kitchen sink, or laundry tub, in a wet basement, or near a swimming pool.
- Avoid using wired telephones during an electrical storm. There is a remote risk of electric shock from lightning.
- Do not use a telephone in the vicinity of a gas leak to report the leak.
- Rack Mount Instructions—The following or similar rack-mount instructions are included with the installation instructions:
 - a. Elevated Operating Ambient—If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
 - b. Reliable Earthing—Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips).

SAVE THESE INSTRUCTIONS

1.3 Precautions

For users in the United Kingdom

FOR YOUR SAFETY, PLEASE READ THE FOLLOWING TEXT CAREFULLY.

This appliance is supplied with a moulded three-pin mains plug for your safety and convenience. Should the fuse need to be replaced, please ensure that the replacement fuse is of the same rating and that it is approved by ASTA or BSI to BS1362.

Check for the ASTA mark  or the BSI mark  on the body of the fuse.

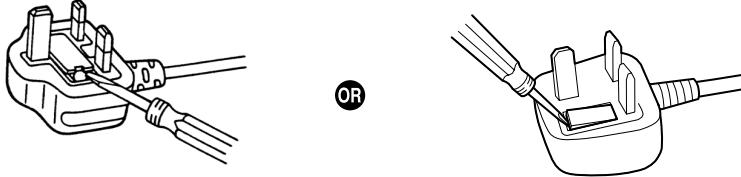
If the plug contains a removable fuse cover, you must ensure that it is refitted when the fuse is replaced. If you lose the fuse cover, the plug must not be used until a replacement cover is obtained. A replacement fuse cover can be purchased from your local Panasonic dealer.

IF THE FITTED MOULDED PLUG IS UNSUITABLE FOR THE AC OUTLET IN YOUR PREMISES, THEN THE FUSE SHOULD BE REMOVED AND THE PLUG CUT OFF AND DISPOSED OF SAFELY. THERE IS A DANGER OF SEVERE ELECTRICAL SHOCK IF THE CUT-OFF PLUG IS INSERTED INTO ANY 13 AMP SOCKET.

WARNING

This appliance must be earthed.

How to replace the fuse: Open the fuse compartment with a screwdriver and replace the fuse and fuse cover.



The equipment must be connected to direct extension lines, and a payphone should not be connected as an extension.

999 and 112 can be dialled on the apparatus after accessing the Exchange line for the purpose of making outgoing calls to the BT emergency services.

During dialling, this apparatus may tinkle the bells of other telephones using the same line. This is not a fault and we advise you not to call the Fault Repair Service.

For users in the European Union only

Information for Users on Collection and Disposal of Old Equipment and used Batteries



These symbols on the products, packaging, and/or accompanying documents mean that used electrical and electronic products and batteries should not be mixed with general household waste.

For proper treatment, recovery and recycling of old products and used batteries, please take them to applicable collection points, in accordance with your national legislation and the Directives 2002/96/EC and 2006/66/EC.

By disposing of these products and batteries correctly, you will help to save valuable resources and prevent any potential negative effects on human health and the environment which could otherwise arise from inappropriate waste handling.

For more information about collection and recycling of old products and batteries, please contact your local municipality, your waste disposal service or the point of sale where you purchased the items.

Penalties may be applicable for incorrect disposal of this waste, in accordance with national legislation.

For business users in the European Union

If you wish to discard electrical and electronic equipment, please contact your dealer or supplier for further information.



Information on Disposal in other Countries outside the European Union

These symbols are only valid in the European Union. If you wish to discard these items, please contact your local authorities or dealer and ask for the correct method of disposal.



Note for the battery symbol (bottom two symbol examples):

This symbol might be used in combination with a chemical symbol. In this case it complies with the requirement set by the Directive for the chemical involved.

For users in Germany only

- Machine Noise Information Ordinance, 3rd GPSGV: The highest sound pressure level is 70 dB (A) or less according to EN ISO 7779.
- This equipment is not for use at video display work stations according to BildscharbV.

For users in Finland, Norway and Sweden only

- This equipment is intended for installation in restricted access locations where only authorised personnel may gain access through the use of a special tool, lock and key or other means of security.

For users in New Zealand only

- This equipment shall not be set to make automatic calls to the Telecom '111' Emergency Service.
- The grant of a Telepermit for any item of terminal equipment indicates only that Telecom has accepted that the item complies with minimum conditions for connection to its network. It indicates no endorsement of the product by Telecom, nor does it provide any sort of warranty. Above all, it provides no assurance that any item will work correctly in all respects with another item of Telepermitted equipment of a different make or model, nor does it imply that any product is compatible with all of Telecom's network services.
- This equipment is not capable, under all operating conditions, of correct operation at the higher speeds for which it is designed. Telecom will accept no responsibility should difficulties arise in such circumstances.

1.3 Precautions

- Some parameters required for compliance with Telecom's Telepermit requirements are dependent on the equipment (PBX) associated with this modem. In order to operate within the limits for compliance with Telecom's Specifications, the associated PBX equipment shall be set to ensure that modem calls are answered between 3 and 30 seconds of receipt of ringing.
- Using the toll services of a company other than Telecom:
If the PBX is set up to use the toll services of a company other than Telecom, the telephone numbers dialled from the Caller Display listings within the PBX will be directed through the toll services of the other company because the telephone numbers include the toll access digit and area code digit. A toll charge may be incurred. Please check with the toll carrier concerned.
- **APPLICABLE ONLY TO TELECOM CUSTOMERS WHO HAVE AUTOMATIC ACCESS TO OTHER CARRIERS FOR TOLL CALLS**
When calling back a number from the Caller ID list, all numbers prefixed with "0 + AREA CODE" will be automatically forwarded to your toll carrier. This includes numbers in your local calling area. The zero + area code should either be removed when calling back local numbers, or check with your toll carrier that a charge will not be levied.
- All persons using this device for recording telephone conversations shall comply with New Zealand law. This requires that at least one party to the conversation is to be aware that it is being recorded. In addition, the principles enumerated in the Privacy Act 1993 shall be complied with in respect to the nature of the personal information collected, the purpose for its collection, how it is used, and what is disclosed to any other party.
- The SLT ports are not specifically designed for 3-wire-connected equipment. 3-wire-connected equipment might not respond to incoming ringing when attached to these ports.

For users in Australia only

- No External TRC Terminal is provided due to an Internal Link between PE and TRC.

For users in Taiwan only

- Lithium batteries can be found in the circuit boards of the mother board and optional service cards of the PBX.

Notice

Regarding removing or replacing a battery in the circuit board, consult your dealer.

Note

- When disposing of any of the above products, all batteries must be removed. Follow the applicable laws, regulations, and guidelines in your country/area regarding disposal of batteries.
- When replacing a battery, use only the same battery type, or an equivalent recommended by the battery manufacturer.



廢電池請回收

1.4 Data Security

In order to use the PBX safely and correctly, the Security Requirements below must be observed. Failure to do so may result in:

- Loss, leakage, falsification or theft of user information.
- Illegal use of the PBX by a third party.
- Interference or suspension of service caused by a third party.

What is User Information?

User Information is defined as:

1. Information stored on the Storage Memory Card:
System data, error data and activation key files.
2. Information sent from the PBX to a PC or a USB memory device:
System data, sound files for MOH (Music on Hold) and OGM (Outgoing Messages), and activation key files.

Requirements

1. The Storage Memory Card contains software for all the processes of the PBX and all the customer data. Therefore, do not allow unauthorised access to prevent data leakage.
2. Always make backups of data stored on the Storage Memory Card and/or perform regular system data backups to a USB memory device or a NAS.
For details about making backups of data stored on the Storage Memory Card, refer to "7.2.2 Utility—File—File Transfer PBX to PC" in the PC Programming Manual.
For details about backing up the system data to a USB memory device or a NAS, refer to "6.1 Tool—System Data Backup" in the PC Programming Manual.
3. To prevent illegal access from the Internet, activate a Firewall.
4. To avoid unauthorised access and possible abuse of the PBX, we strongly recommend:
 - a. Keeping the password secret.
 - b. Selecting a complex, random password that cannot be easily guessed.
 - c. Changing your password regularly.
5. Perform the following when sending the PBX for repair or handing it over to a third party.
 - a. Make a backup of data stored on the Storage Memory Card.
 - b. Using a formatter, format the Storage Memory Card so that information cannot be retrieved from it.
6. To prevent data leakage, render the Storage Memory Card physically unusable before disposal.
7. When user information is sent from the PBX to a PC or a USB memory device, the confidentiality of that information becomes the responsibility of the customer. Before disposing of the PC or the USB memory device, ensure that data cannot be retrieved from it by formatting the hard disk and/or rendering it physically unusable.

1.4 Data Security

Section 2

System Outline

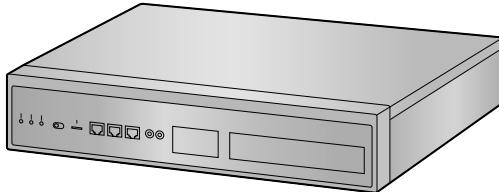
This section provides general information on the PBX, including the system capacity and specifications.

2.1 Basic System Construction

2.1.1 System Configurations

Main Unit

The main unit contains a mother board for controlling PBX functions.



Stand-alone System

A single KX-NS1000 PBX can be used as a stand-alone system. A single KX-NS1000 used as a stand-alone system controls all terminals, trunks, and applications.

Stacking PBXs as Legacy Gateways

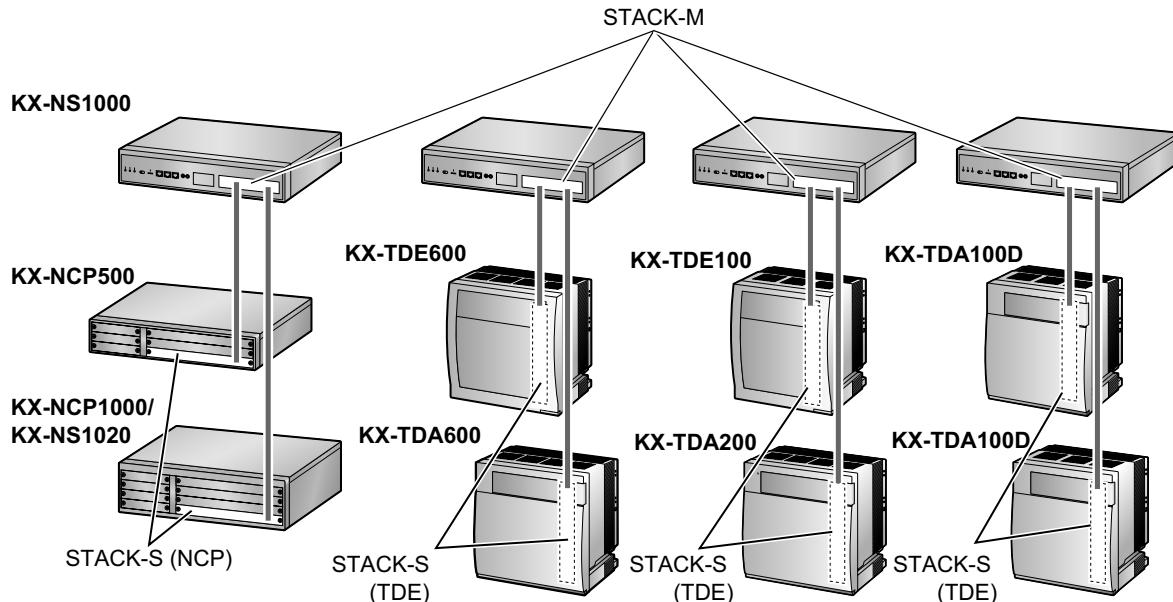
Up to 2 KX-TDA/KX-TDE/KX-NCP series PBXs and KX-TDA100D PBXs can be connected to a KX-NS1000 to expand the usage of legacy terminals and trunks. A PBX connected to a KX-NS1000 functions as a legacy gateway and will be controlled by the KX-NS1000.

To connect a PBX as a legacy gateway, install a STACK-M card in the KX-NS1000 and a STACK-S (NCP) or STACK-S (TDE) card in the PBX. Then, connect the STACK-M card and the STACK-S (NCP)/STACK-S (TDE) card with the stacking cable that is included with the STACK-S (NCP)/STACK-S (TDE) card.

For details about connecting PBXs as legacy gateways, see "4.6.2 STACK-S (NCP) Card (KX-NS0131)" and "4.6.3 STACK-S (TDE) Card (KX-NS0132)".

Note

- For details about connecting a KX-NS1020 as a legacy gateway to a KX-NS1000, refer to your KX-NS1020 Installation Manual.

Example:**One-Look Network with NS-Net¹**

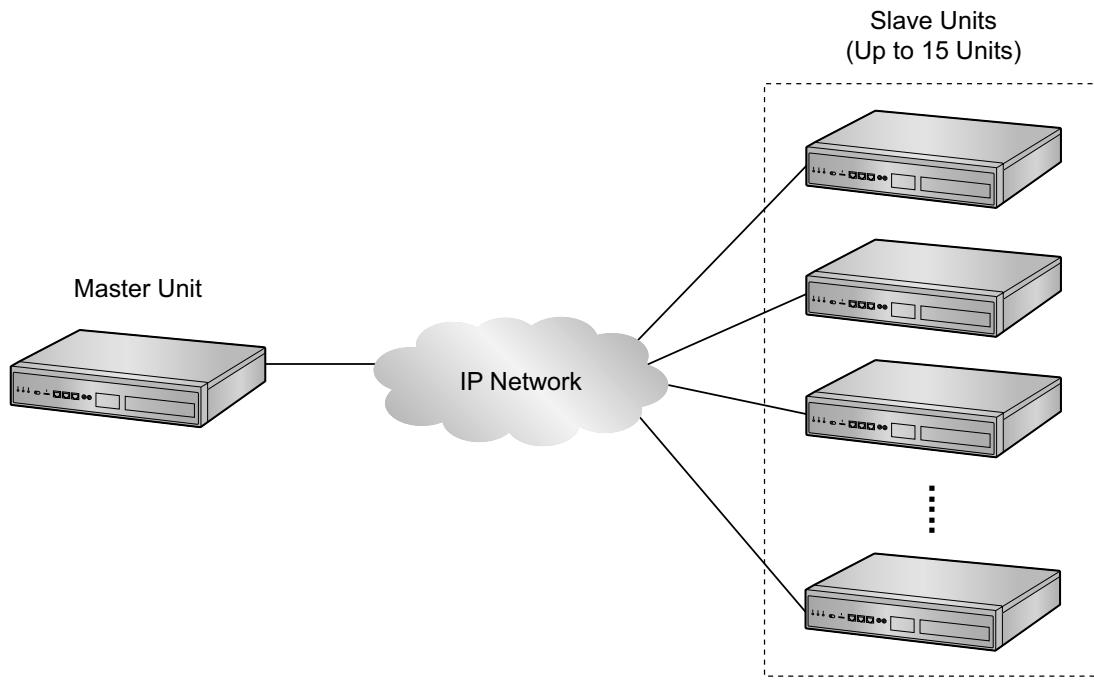
Multiple KX-NS1000 PBXs can be connected as a distributed networked system using a private IP network. The networked system is called a One-look network and it can contain up to 16 KX-NS1000 PBXs and up to 8 legacy gateways. In a One-look network, one PBX serves as the Master unit, which controls the other PBXs, known as Slave units. The Slave units share setup information and resources controlled by the Master unit. A One-look network is useful when the network will consist only of KX-NS1000 PBXs and a private IP network is feasible. A considerable amount of setup is done automatically by the PBXs, so setup and maintenance is much simpler than other type of networks, such as a TIE line network. All units can be programmed from one location. Resource sharing allows users to interact as if they were all connected to one PBX, which eliminates the need to manage information such as PBX access codes.

For details about programming the One-look network, refer to "5.5 Programming a One-look Network".

For details about using a One-look network, refer to "4.2 One-look Networking" in the Feature Guide.

¹ NS-Net is a network protocol only used for Panasonic products.

2.1.1 System Configurations



H.323 QSIG network

If the network will include non-KX-NS1000 PBXs (e.g., KX-TDE200, KX-NCP500), then an H.323 QSIG network is necessary.

An H.323 QSIG network is preferable if strict resource separation between sites is necessary. Although it is possible to reserve certain resources for certain extension users in a One-look network, the default is to share resources. On the other hand, in a QSIG network, resources are not available to extension users of other PBXs without explicit programming.

Programming and configuring an H.323 QSIG network is much more complex than a One-look network. It is also possible to connect a One-look network to other PBXs via QSIG. In an H.323 QSIG network, the One-look network appears as one PBX. The Master unit represents the One-look network.

For details about programming the H.323 QSIG network, refer to "5.6 Programming an H.323 QSIG Network".

For details about H.323 QSIG network, refer to "4.2.2 Network Type Comparison" in the Feature Guide.

One-look Networking Survivability

In a One-look network, the KX-NS1000 can provide failover functionality (One-look Network Survivability). This means that the system can continue to provide partial service even if the Master unit fails or if a network failure occurs between the Master unit and Slave units.

The following 2 types of failover are available:

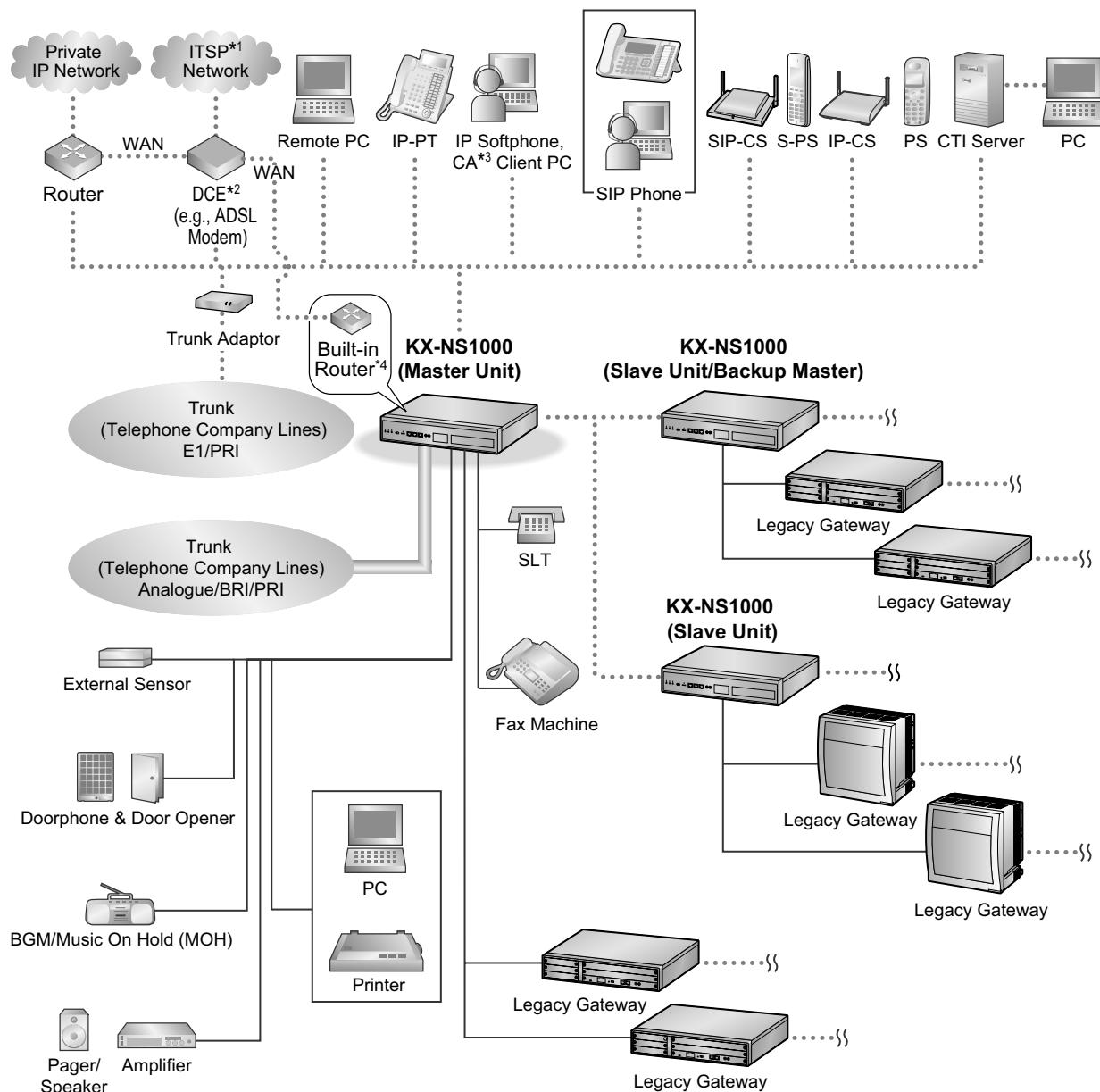
- Backup Master mode
- Isolated mode

In addition, the KX-NS1000 provides the Automatic Rerouting to Secondary PBX feature and UM Group Failover feature.

For an overview of One-look Networking Survivability, refer to "8.4.2 One-look Networking Survivability".

For details of One-look Networking Survivability, refer to "4.2.3 One-look Networking Survivability" in the Feature Guide.

2.1.2 System Connection Diagram



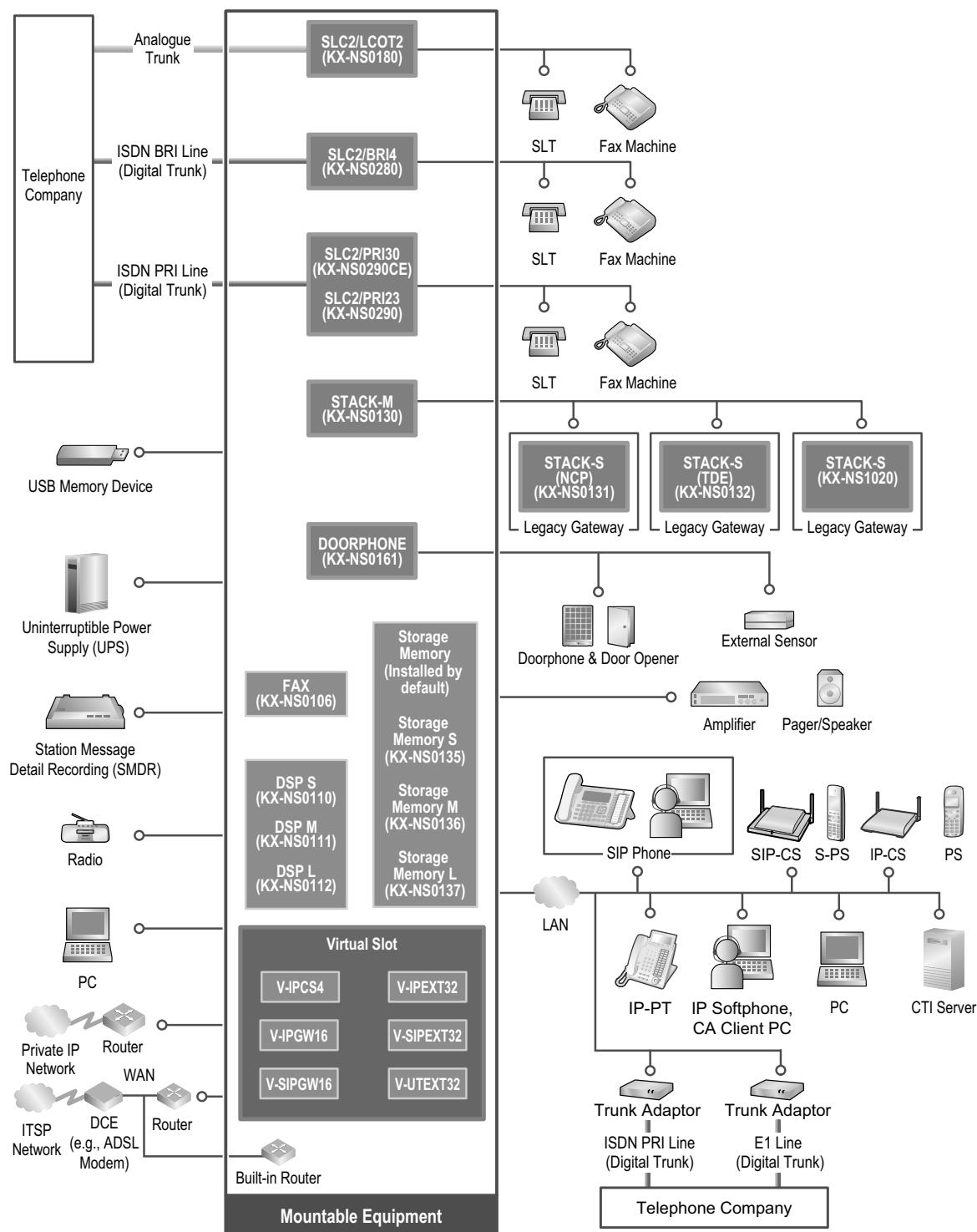
*¹ ITSP: Internet Telephony Service Provider

*² DCE: Data Circuit Terminating Equipment

*³ CA: Communication Assistant

*⁴ The built-in router is available if Built-in Router AK (KX-NSN101) is installed.

2.1.2 System Connection Diagram



2.2 Optional Equipment

2.2.1 Optional Equipment

Model No.	Model Name	Description
KX-NS0106	FAX Interface Card (FAX)	1-channel fax server. To be mounted on the mother board.
KX-NS0110	VoIP DSP Card (S Type) (DSP S)	A DSP card is a digital signal processor card with DSP resources that can be used for VoIP calls, conferences, the Unified Messaging feature, and the DISA/OGM feature. The DSP cards are compliant with ITU-T G.729A and G.711 codec methods.
KX-NS0111	VoIP DSP Card (M Type) (DSP M)	Depending on the amount of your DSP resource needs, DSP S, DSP M, or DSP L cards can be installed. The number of resources provided by each type of DSP card is as follows: <ul style="list-style-type: none"> • DSP S card: 63 • DSP M card: 127 • DSP L card: 254 Up to 2 DSP cards can be installed on the mother board.
KX-NS0112	VoIP DSP Card (L Type) (DSP L)	To operate the PBX, at least one DSP S, DSP M, or DSP L card must be installed in one of the DSP card slots.
KX-NS0135	Storage Memory (S Type) (Storage Memory S)	Storage Memory with maximum of 200 hours Voice Mail recording time.
KX-NS0136	Storage Memory (M Type) (Storage Memory M)	Storage Memory with maximum of 450 hours Voice Mail recording time.
KX-NS0137	Storage Memory (L Type) (Storage Memory L)	Storage Memory with maximum of 1000 hours Voice Mail recording time.
KX-NS0161	Doorphone Interface Card (DOORPHONE)	1-port doorphone card for 1 doorphone, 1 door opener, and 1 external sensor.
KX-NS0180	2-Port Analogue Trunk / 2-Port SLT Card (SLC2/LCOT2)	A combination card including: <ul style="list-style-type: none"> • 2 analogue trunk ports with Caller ID (FSK/FSK with Call Waiting Caller ID [Visual Caller ID]/DTMF). One port is a power failure transfer (PFT) port. • 2 extension ports with Caller ID (FSK) for SLTs.
KX-NS0280	4-Port BRI / 2-Port SLT Card (SLC2/BRI4)	A combination card including: <ul style="list-style-type: none"> • 4 ISDN Basic Rate Interface ports. • 2 extension ports with Caller ID (FSK) for SLTs. EURO-ISDN/ETSI compliant.

2.2.1 Optional Equipment

Model No.	Model Name	Description
KX-NS0290CE	PRI30 / 2-Port SLT Card (SLC2/PRI30)	A combination card including: <ul style="list-style-type: none">1 ISDN Primary Rate Interface port (30B channels).2 extension ports with Caller ID (FSK) for SLTs. EURO-ISDN/ETSI compliant.
KX-NS0290	PRI23 / 2-Port SLT Card (SLC2/PRI23)	A combination card including: <ul style="list-style-type: none">1 ISDN Primary Rate Interface port (23B channels).2 extension ports with Caller ID (FSK) for SLTs. NI (North American standard ISDN protocol) compliant.
KX-NS0130	Stacking Master Card (STACK-M)	A stacking card to be installed in a KX-NS1000. Up to 2 legacy gateways can be connected.
KX-NS0131	Stacking Card for KX-NCP Series (STACK-S (NCP))	A stacking card to be installed in the MPR card slot of a KX-NCP500 or KX-NCP1000 to be used as a legacy gateway.
KX-NS0132	Stacking Card for KX-TDE Series (STACK-S (TDE))	A stacking card to be installed in the MPR card slot or the BUS-S card slot of the PBX to be used as a legacy gateway. For the following PBXs, this card is installed in the MPR card slot: KX-TDE100, KX-TDE200, KX-TDA100, KX-TDA200, KX-TDE600, KX-TDA600, KX-TDA100D For the following PBXs, this card is installed in the BUS-S card slot: KX-TDE620, KX-TDA620

Note

For the maximum number of optional service cards that can be installed in the PBX, refer to "2.3.3 System Capacity".

2.3 Specifications

2.3.1 General Description

Main CPU		650 MHz Dual Core	
Power Input		100 V AC to 130 V AC: 0.95 A/200 V AC to 240 V AC: 0.6 A; 50 Hz/60 Hz	
Power Consumption (when fully mounted)		50 W (240 V: 132 VA, 200 V: 120 VA, 130 V: 104 VA, 100 V: 95 VA)	
External Backup Battery		External battery port is not supported. Support UPS: USB2.0: 1 port (Connector: Type A)	
Memory Backup Duration		7 years	
Dialling	Trunk	Dial Pulse (DP) 10 pps, 20 pps Tone (DTMF) Dialling with Caller ID (FSK/DTMF) 1600 Ω Maximum	
	Extension	Dial Pulse (DP) 10 pps, 20 pps Tone (DTMF) Dialling with Caller ID (FSK/DTMF) SLC1 port supports PFT in combination with the LCOT1 port connected to an analogue trunk.	
Mode Conversion		DP-DTMF, DTMF-DP	
Ring Frequency		20 Hz/25 Hz (selectable)	
Operating Environment	Temperature	0 °C to 40 °C	
	Humidity	10 % to 90 % (non-condensing)	
Conference Call Trunk		From 24 × 3-party conference call to 9 × 8-party conference call	
Music on Hold (MOH)		1 port (Level Control: -31.5 dB to +31.5 dB per 0.5 dB) MOH: Selectable Internal/External Music Source port	
External Paging		1 port (Volume Control: -15.5 dB to +15.5 dB per 0.5 dB)	
Serial Interface Port	RS-232C	1 (maximum 115.2 kbps)	
RJ45 Port	MNT Port	1 (for PC connection)	10BASE-T/100BASE-TX/ 1000BASE-T (Auto MDI/MDI-X)
	LAN Port	1 (for LAN connection)	
	WAN Port	1 (for WAN connection)	
Extension Connection Cable		SLT	1-pair wire (T, R)
Air-cooling method		FAN	
Dimension		430 mm (W) × 88 mm (H) × 340 mm (D)	
Weight (when fully mounted)		Under 5.1 kg	

2.3.2 Characteristics

Terminal Equipment Loop Limit	<ul style="list-style-type: none">SLT: 600 Ω including setDoorphone: 20 Ω
Minimum Leakage Resistance	15 000 Ω minimum
Maximum Number of Extension Instruments per Line	1 for SLT
Ring Voltage	75 Vrms at 20 Hz/25 Hz depending on the Ringing Load
Trunk Loop Limit	1600 Ω maximum
Hookswitch Flash/Recall Timing Range	24 ms to 2032 ms
Door Opener Current Limit	24 V DC/30 V AC, 1 A maximum
External Sensor Current Limit	Power to the external sensor is provided from the DOORPHONE card and must be grounded through the DOORPHONE card. For the connection diagram, refer to "4.7.1 DOORPHONE Card (KX-NS0161)". The PBX detects input from the sensor when the signal is under 100 Ω .
Paging Terminal Impedance	600 Ω
MOH (Music on Hold) Terminal Impedance	10 000 Ω

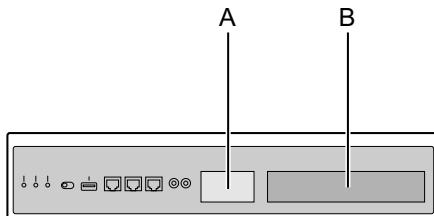
2.3.3 System Capacity

Type and Maximum Number of Slots

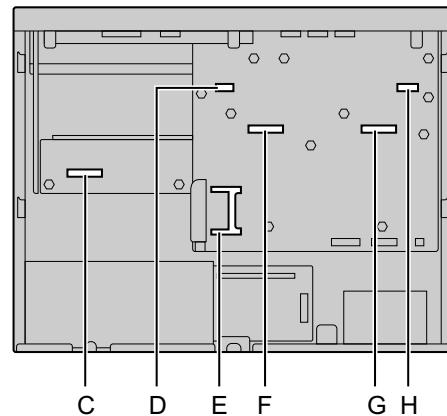
The PBX supports the following type and number of slots.

Slot Type		Maximum Number	
		Stand-alone System	One-look Network
Physical Slot	FAX Card Slot	1	16
	Storage Memory Card Slot	1	16
	DSP Card Slot	2	32
	Free Slot	1	16
	Doorphone Slot	1	16
Virtual Slot	Virtual Trunk Card	16	16
	Virtual Extension Card	20	32
	Virtual IP-CS Card	16	32

Front View



Inside View (The top cover is removed.)

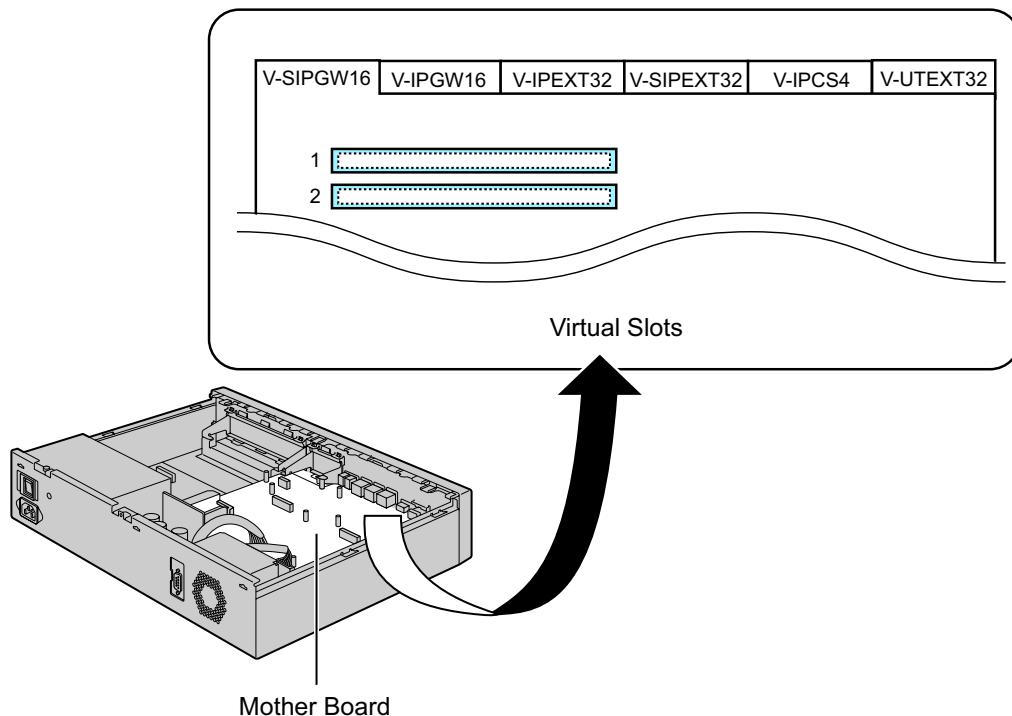


- A. Front cover plate for the Doorphone Slot
- B. Front cover plate for the Free Slot
- C. Free Slot
- D. Doorphone Slot
- E. Storage Memory Card Slot
- F. DSP Card Slot 2
- G. DSP Card Slot 1
- H. FAX Card Slot

2.3.3 System Capacity

Virtual Slots of the Mother Board

Example:



Maximum Optional Service Cards

The following number of card can be installed in the Physical Slots or Virtual Slots of the PBX. The maximum number of optional service card for legacy gateways is limited by the maximum number of extensions and trunks of the KX-NS1000.

Notice

The capacities shown in these tables are for the largest possible configuration for each PBX (i.e. the PBX is equipped with the largest capacity PSU available for that model). For more details about the capacity of each PBX model, refer to the Installation Manual of the corresponding PBX.

Note

- Any card that exceeds the capacity of the PBX will be ignored.
- When the PBX starts up with an invalid configuration, some cards will be ignored.

For KX-NS1000

Cards Installed in Physical Slots

Card Type	Maximum Number	
	Stand-alone System/ Stand-alone KX-NS1000 with 1 Legacy Gateway/ Stand-alone KX-NS1000 with 2 Legacy Gateways	One-look Network
Free Slot	1	16
SLC2/LCOT2		
SLC2/BRI4		
SLC2/PRI30	1	16 ¹
SLC2/PRI23		
STACK-M		
Doorphone Slot	1	16
DOORPHONE	1	16
DSP Card Slot	2	32
DSP S		
DSP M	2	32
DSP L		
FAX Card Slot	1	16
FAX	1	16
Storage Memory Card Slot	1	16

2.3.3 System Capacity

Card Type	Maximum Number	
	Stand-alone System/ Stand-alone KX-NS1000 with 1 Legacy Gateway/ Stand-alone KX-NS1000 with 2 Legacy Gateways	One-look Network
Storage Memory S	1	16
Storage Memory M		
Storage Memory L		

¹ The maximum number of STACK-M cards is 8.

Cards Installed in Virtual Slots

Card Type	Maximum Number		
	Stand-alone System/ Stand-alone KX-NS1000 with 1 Legacy Gateway/ Stand-alone KX-NS1000 with 2 Legacy Gateways	One-look Network	
Virtual Trunk Card	16	16	
V-IPGW16	3 ¹ /3 ² /6 ³	6 ¹ /6 ² /8 ³	
V-SIPGW16	16 ¹ /16 ² /10 ³	16	
Virtual Extension Card	20	32	
V-IPEXT32	8 ¹ /20 ² /8 ³	32	
V-SIPEXT32	20 ¹ /8 ² /12 ³		
V-UTEXT32			
Virtual IP-CS Card	16	32	
V-IPCS4	16	32	

¹ If **Standard Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

² If **IP-Extension Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

³ If **System Resource Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

Note

When the KX-NS1000 is stacked with other PBXs virtual cards can be installed only in the KX-NS1000.

For Legacy Gateways

Trunk Cards for Legacy Gateways

PBX Model	Card Name	Maximum Number		
		Stand-alone KX-NS1000 with 1 Legacy Gateway	Stand-alone KX-NS1000 with 2 Legacy Gateways	One-look Network
KX-NCP500	LCOT4	3	6	24
	BRI2			
	PRI23	2	4	16
	PRI30			
	T1	2	4	16
	E1			
KX-NCP1000/ KX-NS1020	LCOT4	4	8	32
	BRI2			
	PRI23	2	4	16
	PRI30			
	T1	2	4	16
	E1			
KX-TDA100/ KX-TDE100	LCOT8	6	12	38
	LCOT16			
	CLCOT8/ CLCOT8E			
	BRI4			
	BRI8			
	DID8			
	E&M8			
	PRI23	4	8	20
	PRI30			
	T1			
	E1			

2.3.3 System Capacity

PBX Model	Card Name	Maximum Number		
		Stand-alone KX-NS1000 with 1 Legacy Gateway	Stand-alone KX-NS1000 with 2 Legacy Gateways	One-look Network
KX-TDA100D	LCOT8	7	14	38
	LCOT16			
	CLCOT8/ CLCOT8E			
	BRI4			
	BRI8			
	DID8			
	E&M8			
	PRI23		8	20
	PRI30			
	T1			
	E1			
KX-TDA200/ KX-TDE200	LCOT8	8	16	38
	LCOT16			
	CLCOT8/ CLCOT8E			
	BRI4			
	BRI8			
	DID8			
	E&M8			
	PRI23		8	20
	PRI30			
	T1			
	E1			

PBX Model	Card Name	Maximum Number		
		Stand-alone KX-NS1000 with 1 Legacy Gateway	Stand-alone KX-NS1000 with 2 Legacy Gateways	One-look Network
KX-TDA600/ KX-TDA620/ KX-TDE600/ KX-TDE620	ELCOT16	10	16	38
	BRI4		20	
	BRI8		16	
	DID8		20	
	E&M8	5	10	20
	PRI23		9	
	PRI30		10	
	T1		9	
	E1			

Extension Cards for Legacy Gateways

PBX Model	Card Name	Maximum Number		
		Stand-alone KX-NS1000 with 1 Legacy Gateway	Stand-alone KX-NS1000 with 2 Legacy Gateways	One-look Network
KX-NCP500/ KX-NCP1000/ KX-NS1020	DHLC4	1	2	8
	DLC8	2	4	16
	DLC16			
	SLC8	2	4	16
	SLC16			
KX-TDA100/ KX-TDE100	DHLC8	6	12	42
	DLC8	6	12	48
	DLC16			32
	SLC8	6	12	48
	SLC16			
	MSLC16			
	CSLC16			
	MCSLC16	6	12	48
	MCSLC24	5	10	42
	CSIF4	4	8	16
	CSIF8			

2.3.3 System Capacity

PBX Model	Card Name	Maximum Number		
		Stand-alone KX-NS1000 with 1 Legacy Gateway	Stand-alone KX-NS1000 with 2 Legacy Gateways	One-link Network
KX-TDA100D	DLC8	7	14	64
	DLC16	7	14	32
	MCSLC16	7	14	64
	MCSLC24	5	10	42
	CSIF4	4	8	16
	CSIF8			
KX-TDA200/ KX-TDE200	DHLC8	8	16	42
	DLC8	8	16	64
	DLC16			32
	SLC8	8	16	64
	SLC16			
	MSLC16			
	CSLC16			
	MCSLC16	8	16	64
	MCSLC24	5	10	42
	CSIF4	4	8	16
	CSIF8			
KX-TDA600/ KX-TDA620/ KX-TDE600/ KX-TDE620	DHLC8	10	20	42
	DLC8	10	20	64
	DLC16			32
	SLC8	10	20	64
	CSLC16			
	ESLC16			
	EMSLC16			
	ECSLC24			42
	EMSLC24			
	CSIF4	4	8	16
	CSIF8			

Other Physical Cards for Legacy Gateways

PBX Model	Card Name	Maximum Number		
		Stand-alone KX-NS1000 with 1 Legacy Gateway	Stand-alone KX-NS1000 with 2 Legacy Gateways	One-look Network
KX-NCP500	OPB3	2	4	16
	DPH4	4	8	16
	DPH2	6	12	32
	EIO4	4	8	16
	ECHO16	2	4	8
	OPB3	3	6	16
KX-NCP1000/ KX-NS1020	DPH4	4	8	16
	DPH2	8	16	32
	EIO4	4	8	16
	ECHO16	2	4	8
	OPB3	4	8	16
	DPH4	4	8	16
KX-TDA100/ KX-TDA200/ KX-TDE100/ KX-TDE200/ KX-TDA100D	DPH2	8	16	32
	EIO4	4	8	16
	ECHO16	1	2	8
	OPB3	4	8	16
	DPH4	4	8	16
	DPH2	8	16	32
KX-TDA600/ KX-TDA620/ KX-TDE600/ KX-TDE620	EIO4	4	8	16
	ECHO16	2	4	8

Maximum Trunks and Extensions

The PBX supports the following number of trunks and extensions.

Notice

The capacities shown in these tables are for the largest possible configuration for each PBX (i.e. the PBX is equipped with the largest capacity PSU available for that model). For more details about the capacity of each PBX model, refer to the Installation Manual of the corresponding PBX.

2.3.3 System Capacity

For KX-NS1000 stand-alone system

Type	KX-NS1000
Total Number of Trunks	256
Trunk (Virtual Trunk Card)	256
H.323 Trunks	48 ¹ /48 ² /96 ³
SIP Trunks	256 ¹ /256 ² /160 ³
Trunk (Physical Trunk Card)	30
Total Number of Extensions	640
Extension (Virtual Extension Card)	640
IP-PT and IP Softphone	256 ¹ /640 ² /256 ³
SIP Phone	640 ¹ /256 ² /384 ³
SIP Phone	640 ¹ /256 ² /384 ³
S-PS	255
Extension (Physical Extension Card)	2

¹ If **Standard Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

² If **IP-Extension Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

³ If **System Resource Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

For KX-NS1000 with 1 legacy gateway

Type	KX-NCP500/ KX-NCP1000/ KX-NS1020	KX-TDE100/ KX-TDA100/ KX-TDA100D	KX-TDE200/ KX-TDA200	KX-TDE600/ KX-TDE620/ KX-TDA600/ KX-TDA620
Total Number of Trunks	256			
Trunk (Virtual Trunk Card)	256			
H.323 Trunks	48 ¹ /48 ² /96 ³			
SIP Trunks	256 ¹ /256 ² /160 ³			
Trunk (Physical Trunk Card)	64	120	128	160

Type	KX-NCP500/ KX-NCP1000/ KX-NS1020	KX-TDE100/ KX-TDA100/ KX-TDA100D	KX-TDE200/ KX-TDA200	KX-TDE600/ KX-TDE620/ KX-TDA600/ KX-TDA620
LCOT	12 ⁴ /16 ⁵	96 ⁶ /112 ⁷	128	160
	—	112 ⁷	—	—
	12 ⁴ /16 ⁵	96 ⁶ /112 ⁷	128	160
	46	92	92	115
	60	120	120	150
	48	96	96	120
	60	120	120	150
Total Number of Extensions		640		
Extension (Virtual Extension Card)		640		
IP-PT and IP Softphone		256 ¹ /640 ² /256 ³		
SIP Phone		640 ¹ /256 ² /384 ³		
SIP Phone		640 ¹ /256 ² /384 ³		
S-PS		255		
Extension (Physical Extension Card)	44	128	256	304
SLT	36	96 ⁶ /128 ⁷	168	240
DPT	40	128 ⁶ /104 ⁷	256	256

¹ If Standard Type is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)² If IP-Extension Type is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)³ If System Resource Type is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)⁴ For KX-NCP500⁵ For KX-NCP1000/KX-NS1020⁶ Except KX-TDA100D.⁷ Only KX-TDA100.

For KX-NS1000 with 2 legacy gateways

Type	KX-NCP500/ KX-NCP1000/ KX-NS1020	KX-TDE100/ KX-TDA100/ KX-TDA100D	KX-TDE200/ KX-TDA200	KX-TDE600/ KX-TDE620/ KX-TDA600/ KX-TDA620
Total Number of Trunks	256			

2.3.3 System Capacity

Type	KX-NCP500/ KX-NCP1000/ KX-NS1020	KX-TDE100/ KX-TDA100/ KX-TDA100D	KX-TDE200/ KX-TDA200	KX-TDE600/ KX-TDE620/ KX-TDA600/ KX-TDA620
Trunk (Virtual Trunk Card)	256			
H.323 Trunks	48 ¹ /48 ² /96 ³			
SIP Trunks	256 ¹ /256 ² /160 ³			
Trunk (Physical Trunk Card)	128	240	256	256
LCOT	24 ⁴ /32 ⁵	192 ⁶ /224 ⁷	256	256
CLCOT	—	224 ⁷	—	—
BRI	24 ⁴ /32 ⁵	192 ⁶ /224 ⁷	256	256
PRI23	92	184	184	230
PRI30	120	240	240	256
T1	96	192	192	240
E1	120	240	240	256
Total Number of Extensions	640			
Extension (Virtual Extension Card)	640			
IP-PT and IP Softphone	256 ¹ /640 ² /256 ³			
SIP Phone	640 ¹ /256 ² /384 ³			
SIP Phone	640 ¹ /256 ² /384 ³			
S-PS	255			
Extension (Physical Extension Card)	88	256	512	608
SLT	72	192 ⁶ /256 ⁷	336	480

Type	KX-NCP500/ KX-NCP1000/ KX-NS1020	KX-TDE100/ KX-TDA100/ KX-TDA100D	KX-TDE200/ KX-TDA200	KX-TDE600/ KX-TDE620/ KX-TDA600/ KX-TDA620
DPT	80	256 ^{*6} /208 ^{*7}	512	512

^{*1} If **Standard Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

^{*2} If **IP-Extension Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

^{*3} If **System Resource Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

^{*4} For KX-NCP500

^{*5} For KX-NCP1000/KX-NS1020

^{*6} Except KX-TDA100D.

^{*7} Only KX-TDA100D.

For One-look network

Type	One-look Network
Total Number of Trunks	600
Trunk (Virtual Trunk Card)	256
H.323 Trunks	96 ^{*1} /96 ^{*2} /128 ^{*3}
SIP Trunks	256
Trunk (Physical Trunk Card)	600
LCOT	600
BRI	
PRI23	
PRI30	
T1	
E1	
Total Number of Extensions	1000 ^{*4}

2.3.3 System Capacity

Type	One-link Network
Extension (Virtual Extension Card)	1000
IP-PT and IP Softphone	1000
SIP Phone	1000
SIP Phone	1000
S-PS	255
Extension (Physical Extension Card)	1000
SLT	1000
DPT	

¹ If **Standard Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

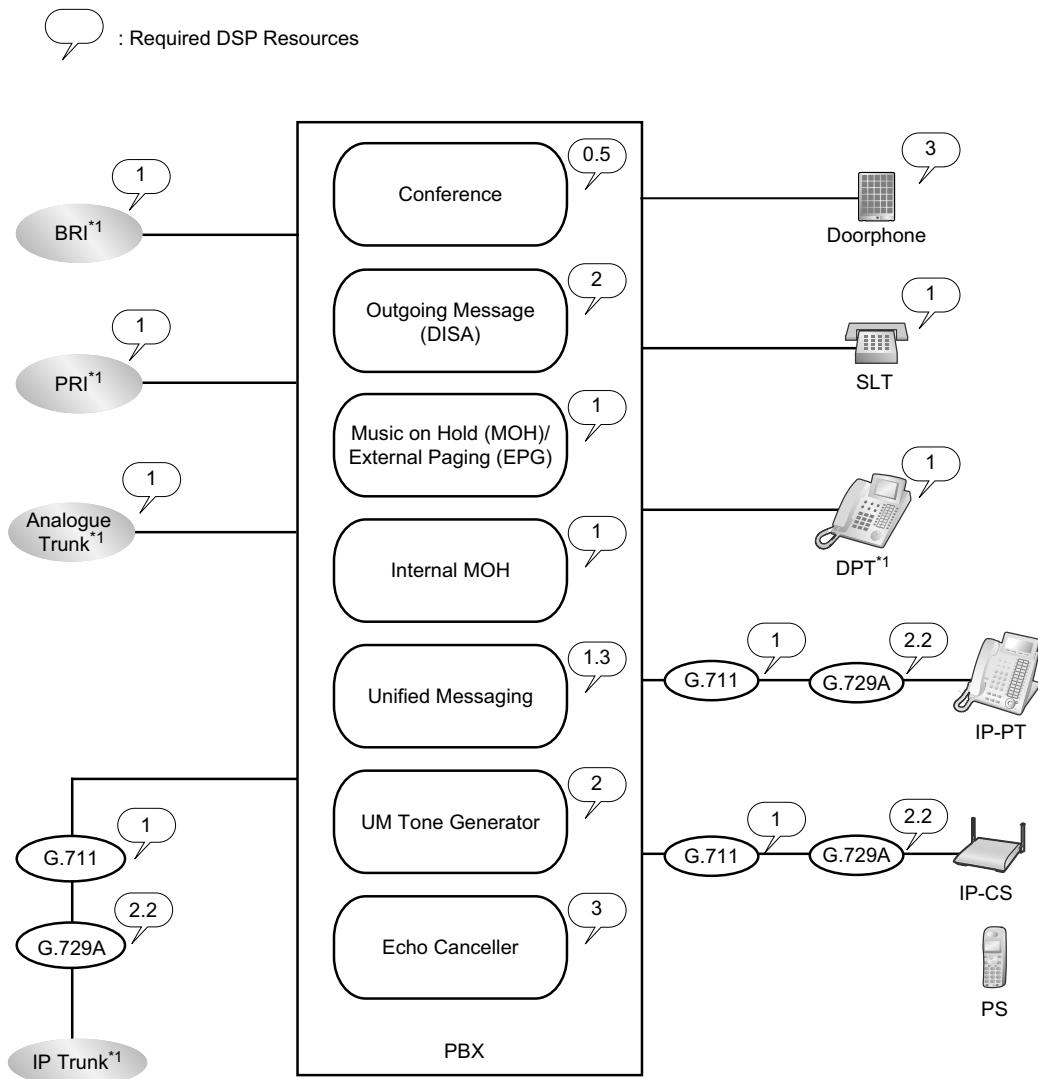
² If **IP-Extension Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

³ If **System Resource Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

⁴ The maximum number of extension ports is 640 per PBX, and the maximum number of Unified Messaging ports is 24 per PBX. When 24 ports for Unified Messaging are fully activated on the Master unit, the maximum number of extension ports will be less than 640. One Unified Messaging port is equal to 10 extension ports. Therefore, when all Unified Messaging ports are activated, only up to 400 extensions are available. This condition does not apply for Slave units.

DSP Resources

DSP cards provide digital signal processor (DSP) resources, and the PBX uses the resources to perform various PBX operations. The following illustration shows the concept of DSP resource usage. More complex situations may require additional resources, and in some cases the amount of DSP resources required may be less than expected.



*¹ Connections that arrive over a stacking connection require the same amount of DSP resources as shown in this example.

Note

This is an example for a stand-alone KX-NS1000.

Required DSP Resources Assessment

The maximum number of simultaneous calls, operations and features using IP protocols is determined by the DSP card installed in the PBX. According to the number of resources required, you can install up to 2 DSP cards.

To decide how much resources are required for the PBX, the DSP Resource Advisor can be useful.

2.3.3 System Capacity

Note

- Calls cannot be made or received when all of the DSP resources are being used.
- The number of required resources must not exceed the DSP resources installed to the PBX.
- For details about the DSP Resource Advisor, refer to "9.34.1.1 PBX Configuration—[1-5-1] Configuration—DSP Resource—Setting—DSP Resource Advisor" in the PC Programming Manual.
- For information about installing DSP cards, refer to "4.3.3 DSP S Card (KX-NS0110), DSP M Card (KX-NS0111), DSP L Card (KX-NS0112)".
- The number of available DSP resources is not restricted by any activation keys.

DSP Resource Reservation

DSP resources can be reserved for certain operations to avoid lack of resources for particular operations. When the PBXs are connected in a One-look network, you can specify how many resources to allocate to each branch.

The following examples show cases of allocating and reserving DSP resources.

Note

For details about reserving DSP resources, refer to "5.5.4.1 DSP Resource Reservation" and "5.5.4.2 DSP Resource Advisor" in the Feature Guide, and "9.34.1.1 PBX Configuration—[1-5-1] Configuration—DSP Resource—Setting—DSP Resource Advisor" in the PC Programming Manual.

Example

In this example, the DSP M (127 DSP resources) is installed and resources are reserved for the following operations:

Operation	Required Resources
VoIP (G.711) Calls	40
Conference Trunks	10
Unified Messaging	8
Two-way Recording Operations	3
OGM Operations	10
UM Tone (Fixed)	2^{*1}

^{*1} Because the system reserves 2 resources for internal system functions, the total amount of available resources indicated will be 2 less than the total resources of the installed card(s).

Reserved Resources

$$(40 \times 1) + (10 \times 0.5) + (8 \times 1.3) + (10 \times 2) + 2 \\ = 77.4$$

Free Resources

$$= 127 - 77.4 \\ = 49.6$$

Note

This is an example for a stand-alone KX-NS1000 without any stacking PBXs.

Expandable Resources with Legacy Gateways

Connecting a PBX as a legacy gateway can expand the types of available resources. However, some types of resources are not available. The following table shows the types of resources that are available when a legacy gateway used with a KX-NS1000.

Notice

When legacy gateways are used with a KX-NS1000, all IP-PTs are registered to the KX-NS1000. Therefore, no optional service cards nor DSP resources are required for the legacy gateways. For information about unsupported optional service cards, refer to "Unsupported System Components for Legacy Gateways" in "System Components".

Type	Resource	Availability
Optional Service Card	Physical Card for Legacy Trunks and Extensions	✓
	Virtual Card	— ¹
	RMT Card	—
	DPH/EIO/ECHO Card	✓
	ESVM/MSG Card	—
	MEC Card	—
	DSP Card	—
Terminal	DPT/APT/SLT	✓
	PT-interface CS/CS for CSIF Card	✓
	PS	✓
	IP-CS/IP-PT/KX-UT Series SIP Phone/SIP-CS	— ¹
	Doorphone	✓
	IP Softphone	— ¹
	KX-NT400	—
Activation Key	Any Activation key	—

¹ IP terminals, except for KX-NT265 (software version 2.00 or later only), are registered and controlled by the KX-NS1000.

Maximum Terminal Equipment

The following shows the number of each terminal equipment type supported by the PBX.

Notice

- When 2 legacy gateways are used, the maximum number for each terminal equipment type for the system is the sum of each PBX's maximum number. However, the maximum number of the following terminal equipment does not depend on the number of legacy gateways.
 - IP-PTs (maximum number: 256¹/640²/256³)
 - SIP phones (maximum number: 640¹/256²/384³)
 - S-PSs (maximum number: 255)
 - IP-CSs (maximum number: 64)
 - SIP-CSs (maximum number: 64)
 - PSs (maximum number: 512)

2.3.3 System Capacity

- Unified Messaging System (maximum number of channels: 24)
- Voice Processing System (maximum number of channels: 48)
- The capacities shown in these tables are for the largest possible configuration for each PBX (i.e. the PBX is equipped with the largest capacity PSU available for that model). For more details about the capacity of each PBX model, refer to the Installation Manual of the corresponding PBX.

For stand-alone system

Terminal Equipment Type	KX-NS1000
Telephone	640
SLT	2
IP-PT ⁴	256 ¹ /640 ² /256 ³
SIP	640 ¹ /256 ² /384 ³
SIP Phone	640 ¹ /256 ² /384 ³
S-PS	255
CS	64
IP-CS	64 ⁵
SIP-CS	64 ⁶
PS	512
Doorphone	1
Door Opener	1
External Sensor	1

¹ If **Standard Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

² If **IP-Extension Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

³ If **System Resource Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

⁴ KX-NT300 series, KX-NT500 series, and KX-NT265 (software version 2.00 or later only).

⁵ The maximum number of Air Sync Groups is 16. An Air Sync Group can contain up to 16 IP-CSs.

⁶ The maximum number of Air Sync Groups is 8. An Air Sync Group can contain up to 32 SIP-CSs.

For a KX-NS1000 and a KX-NCP500/KX-NCP1000/KX-NS1020

Terminal Equipment Type	KX-NCP500/KX-NCP1000/KX-NS1020
Telephone	640
SLT	36
KX-DT300/KX-DT500/KX-T7600 Series DPT	40
KX-T7560/KX-T7565 DPT	36
Other DPT	10

Terminal Equipment Type	KX-NCP500/KX-NCP1000/KX-NS1020
APT	4
IP-PT ¹	256 ² /640 ³ /256 ⁴
SIP	640 ² /256 ³ /384 ⁴
SIP Phone	640 ² /256 ³ /384 ⁴
S-PS	255
DSS Console	8
CS	64
PT-interface CS (2-channel)	11
PT-interface CS (8-channel) ⁵	5
IP-CS	64
SIP-CS	64
PS	512
Voice Processing System (VPS)	2
Doorphone	17
Door Opener	17 ⁶
External Sensor	17
External Relay	17 ⁶

¹ KX-NT300 series, KX-NT500 series, and KX-NT265 (software version 2.00 or later only).

² If **Standard Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

³ If **IP-Extension Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

⁴ If **System Resource Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

⁵ One 8-channel PT-interface CS counts as 2 CSs for the total number of CSs.

⁶ The DOORPHONE card of the KX-NS1000 can serve as a Door opener or as an External relay depending on its programming.

For a KX-NS1000 and a KX-TDA100/KX-TDA200/KX-TDE100/KX-TDE200/KX-TDA100D

Terminal Equipment Type	KX-TDA100/KX-TDE100/ KX-TDA100D	KX-TDA200/KX-TDE200
Telephone	640	640
SLT	96 ¹ /128 ²	128
KX-DT300/KX-DT500/ KX-T7600 Series DPT	128 ¹ /104 ²	256
KX-T7560/KX-T7565 DPT	96 ¹	128
Other DPT	32 ¹	128

2.3.3 System Capacity

Terminal Equipment Type	KX-TDA100/KX-TDE100/ KX-TDA100D	KX-TDA200/KX-TDE200
APT	24 ¹	64
IP-PT ³	256 ⁴ /640 ⁵ /256 ⁶	256 ⁴ /640 ⁵ /256 ⁶
SIP	640 ⁴ /256 ⁵ /384 ⁶	640 ⁴ /256 ⁵ /384 ⁶
SIP-Phone	640 ⁴ /256 ⁵ /384 ⁶	640 ⁴ /256 ⁵ /384 ⁶
S-PS	255	255
DSS Console	8	8
CS	64	64
PT-interface CS (2-channel)/CS for CSIF card	32 ¹ /26 ²	32
PT-interface CS (8-channel) ⁷	16 ¹ /13 ²	16
IP-CS	64	64
SIP-CS	64	64
PS	512	512
Voice Processing System (VPS)	2	2
Doorphone	17	17
Door Opener	17 ⁸	17 ⁸
External Sensor	17	17
External Relay	17 ⁸	17 ⁸

¹ Except KX-TDA100D.

² Only KX-TDA100D.

³ KX-NT300 series, KX-NT500 series, and KX-NT265 (software version 2.00 or later only).

⁴ If **Standard Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

⁵ If **IP-Extension Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

⁶ If **System Resource Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

⁷ One 8-channel PT-interface CS counts as 2 CSs for the total number of CSs.

⁸ The DOORPHONE card of the KX-NS1000 can serve as a Door opener or as an External relay depending on its programming.

For a KX-NS1000 and a KX-TDA600/KX-TDA620/KX-TDE600/KX-TDE620

Terminal Equipment Type	KX-TDA600/KX-TDA620/ KX-TDE600/KX-TDE620
Telephone	640
SLT	240
KX-T7600 Series DPT	256
Other DPT	128

Terminal Equipment Type	KX-TDA600/KX-TDA620/ KX-TDE600/KX-TDE620
APT	80
IP-PT ¹	256 ² /640 ³ /256 ⁴
SIP	640 ² /256 ³ /384 ⁴
SIP Phone	640 ² /256 ³ /384 ⁴
S-PS	255
DSS Console	64
CS	64
PT-interface CS (2-channel)/CS for CSIF card	32
PT-interface CS (8-channel) ⁵	16
IP-CS	64
SIP-CS	64
PS	512
Voice Processing System (VPS)	2
Doorphone	17
Door Opener	17 ⁶
External Sensor	17
External Relay	17 ⁶

¹ KX-NT300 series, KX-NT500 series, and KX-NT265 (software version 2.00 or later only).

² If **Standard Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

³ If **IP-Extension Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

⁴ If **System Resource Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

⁵ One 8-channel PT-interface CS counts as 2 CSs for the total number of CSs.

⁶ The DOORPHONE card of the KX-NS1000 can serve as a Door opener or as an External relay depending on its programming.

For One-look network

Terminal Equipment Type	One-look Network
Telephone	1000
SLT	1000
DPT	1000
APT	640
IP-PT ¹	1000
SIP	1000

2.3.3 System Capacity

Terminal Equipment Type	One-touch Network
SIP Phone	1000
S-PS	255
DSS Console	64
CS	128
PT-interface CS (2-channel)/CS for CSIF card	128
PT-interface CS (8-channel) ²	64
IP-CS	128 ³
SIP-CS	128 ⁴
PS	512
Voice Processing System (VPS)	8
Doorphone	64
Door Opener	64
External Sensor	64
External Relay	64

¹ IP terminals, except for KX-NT265 (software version 2.00 or later only), are registered and controlled by the KX-NS1000.

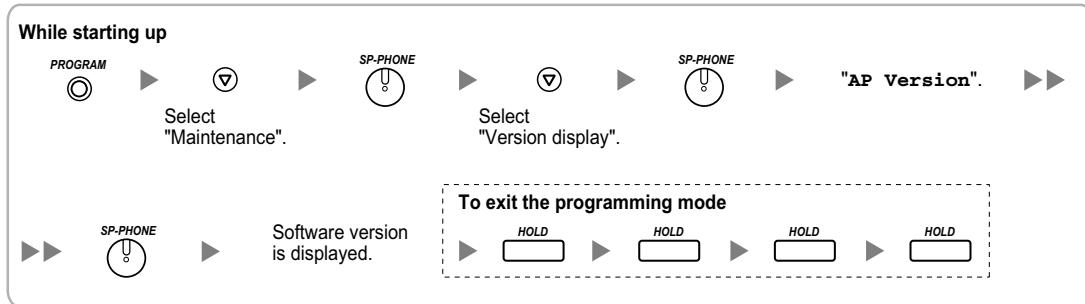
² One 8-channel PT-interface CS counts as 2 CSs for the total number of CSs.

³ The maximum number of Air Sync Groups is 16. An Air Sync Group can contain up to 16 IP-CSs.

⁴ The maximum number of Air Sync Groups is 8. An Air Sync Group can contain up to 32 SIP-CSs.

Note for KX-NT265 IP-PT users

The supported card varies depending on the software version of your KX-NT265 IP-PT. To confirm the version, follow the procedure below:



Section 3

Information about the Activation Keys

This section provides information on activation keys, including how to obtain activation keys.

3.1 Information about the Activation Keys

Activation keys are required to use IP trunks and IP telephones on a private IP network with a KX-NS1000. Also, to upgrade the software to use enhanced features, the corresponding activation keys for that feature are required. Some activation keys are provided by default, some are provided free for a limited period, and others are provided separately as activation key files.

Notice

When stacking PBXs to a KX-NS1000, the activation keys that were used with the PBXs cannot be used with the KX-NS1000.

3.1.1 Type and Maximum Number of Activation Keys

The PBX supports the following type and number of activation keys. The preinstalled activation keys on the mother board are shown with "[]".

When the number of preinstalled activation keys is not enough for the desired configuration or when you wish to use enhanced features, additional activation keys in the form of activation key files can be installed using Web Maintenance Console.

When the PBX is connected in a One-look network, activation keys should be installed on the appropriate PBX as shown in the tables below.

Note

- Store the downloaded activation key files in your PC or a memory device. They can then be reinstalled when changing the Storage Memory Card or in an emergency situation.
- For information about how to obtain the additional activation keys, refer to "3.1.2 Activation Key Code and Key Management System".
- For information about how to install the activation key files using Web Maintenance Console, refer to "5.4.4 Installing Additional Activation Keys".

IP Trunks

Model No.	Activation Key Type	Description	Maximum IP Trunks	
			Stand-alone System	One-look Network
KX-NSM102	2 IP Trunk	Allows the use of 2 IP trunks (H.323/SIP).	256 IP trunks (H.323/SIP) ^{**2}	
KX-NSM104	4 IP Trunk	Allows the use of 4 IP trunks (H.323/SIP).		
KX-NSM108	8 IP Trunk	Allows the use of 8 IP trunks (H.323/SIP).		
KX-NSM116	16 IP Trunk	Allows the use of 16 IP trunks (H.323/SIP).		

^{**1} You need to set the number of installed activation keys to be used for H.323 trunks through system programming. By default, all installed activation keys will be used for SIP trunks.

^{**2} Refer to "2.3.3 System Capacity" for the maximum number of H.323 trunks.

Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSM102	2 IP Trunk	✓	✓
KX-NSM104	4 IP Trunk		
KX-NSM108	8 IP Trunk		
KX-NSM116	16 IP Trunk		

IP Telephone Capacity**Note**

- Up to 30 IP-PTs/IP softphones/KX-UT series SIP phones/third party SIP phones can be used without needing any of the following IP telephone capacity activation keys.
- Activation keys for IP telephone capacity are not cumulative; the maximum overall capacity is determined by the highest-numbered installed activation key.
- In a One-look network, activation keys for IP telephone capacity and IP telephone capacity expansion are not cumulative; the maximum overall capacity depends on the system capacity. The total capacity for IP-PTs, IP softphones, KX-UT series SIP phones, and third party SIP phones is 1000.

IP Telephone Capacity Activation Keys

Model No.	Activation Key Type	Description	Maximum Capacity of IP Phones
			Per Site
KX-NSM005	Up to 50 IP Phone	Allows the use of between 31 and 50 IP-PTs/IP softphones/KX-UT series SIP phones/third party SIP phones.	Capacity for total of 50 IP-PTs/IP softphones/KX-UT series SIP phones/third party SIP phones
KX-NSM010	Up to 100 IP Phone	Allows the use of between 31 and 100 IP-PTs/IP softphones/KX-UT series SIP phones/third party SIP phones.	Capacity for total of 100 IP-PTs/IP softphones/KX-UT series SIP phones/third party SIP phones
KX-NSM030	Up to 300 IP Phone	Allows the use of between 31 and 300 IP-PTs/IP softphones/KX-UT series SIP phones/third party SIP phones.	Capacity for total of 300 IP-PTs/IP softphones/KX-UT series SIP phones/third party SIP phones
KX-NSM099	System MAX IP Phone	Allows the use of between 31 and 640 IP-PTs/IP softphones/KX-UT series SIP phones/third party SIP phones.	Capacity for total of 640 IP-PTs/IP softphones/KX-UT series SIP phones/third party SIP phones

3.1.1 Type and Maximum Number of Activation Keys

IP Telephone Capacity Expansion Activation Key

Model No.	Activation Key Type	Description	Maximum Capacity of IP Phones
			Per Site
KX-NSX910	Expansion from NSM005	<p>Allows the use of between 51 and 100 IP-PTs/IP softphones/ KX-UT series SIP phones/third party SIP phones.</p> <p>To expand the number of usable IP terminals using this activation key, the following licence must be already installed.</p> <ul style="list-style-type: none"> • KX-NSM005 	Capacity for total of 100 IP-PTs/IP softphones/KX-UT series SIP phones/third party SIP phones
KX-NSX930	Expansion from NSM010	<p>Allows the use of between 101 and 300 IP-PTs/IP softphones/ KX-UT series SIP phones/third party SIP phones.</p> <p>To expand the number of usable IP terminals using this activation key, one of the following licence sets must be already installed.</p> <ul style="list-style-type: none"> • KX-NSM005 + KX-NSX910 • KX-NSM010 	Capacity for total of 300 IP-PTs/IP softphones/KX-UT series SIP phones/third party SIP phones
KX-NSX999	Expansion from NSM030	<p>Allows the use of between 301 and 640 IP-PTs/IP softphones/ KX-UT series SIP phones/third party SIP phones.</p> <p>To expand the number of usable IP terminals using this activation key, one of the following licence sets must be already installed.</p> <ul style="list-style-type: none"> • KX-NSM005 + KX-NSX910 + KX-NSX930 • KX-NSM010 + KX-NSX930 • KX-NSM030 	Capacity for total of 640 IP-PTs/IP softphones/KX-UT series SIP phones/third party SIP phones

Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSM005	Up to 50 IP Phone	✓	✓
KX-NSM010	Up to 100 IP Phone		
KX-NSM030	Up to 300 IP Phone		
KX-NSM099	System MAX IP Phone		
KX-NSX910	Expansion from NSM005		
KX-NSX930	Expansion from NSM010		
KX-NSX999	Expansion from NSM030		

IP Telephone

Model No.	Activation Key Type	Description	Maximum IP Telephones	
			Stand-alone System	One-look Network
KX-NSM201	1 IPSoftphone/IP PT	Allows the use of 1 IP-PT/IP softphone/KX-UT series SIP phone.	Total 640 IP-PTs/IP softphones/ KX-UT series SIP phones ^{*12}	Total 1000 IP-PTs/IP softphones/ KX-UT series SIP phones ^{*1}
KX-NSM205	5 IPSoftphone/IP PT	Allows the use of 5 IP-PTs/IP softphones/KX-UT series SIP phones.		
KX-NSM210	10 IPSoftphone/IP PT	Allows the use of 10 IP-PTs/IP softphones/KX-UT series SIP phones.		
KX-NSM220	20 IPSoftphone/IP PT	Allows the use of 20 IP-PTs/IP softphones/KX-UT series SIP phones.		
KX-NSM501	1 IP PT	Allows the use of 1 IP-PT/KX-UT series SIP phone.	Total 640 IP-PTs/ KX-UT series SIP phones [8 IP-PTs/ KX-UT series SIP phones] ^{*23}	Total 1000 IP-PTs/ KX-UT series SIP phones [128 IP-PTs/ KX-UT series SIP phones] ^{*3}
KX-NSM505	5 IP PT	Allows the use of 5 IP-PTs/KX-UT series SIP phones.		
KX-NSM510	10 IP PT	Allows the use of 10 IP-PTs/KX-UT series SIP phones.		
KX-NSM520	20 IP PT	Allows the use of 20 IP-PTs/KX-UT series SIP phones.		

3.1.1 Type and Maximum Number of Activation Keys

Model No.	Activation Key Type	Description	Maximum IP Telephones	
			Stand-alone System	One-look Network
KX-NSM701	1 SIP Extension	Allows the use of 1 IP Conferencing Phone/third party SIP phone.	Total 640 IP Conferencing Phones/third party SIP phones ²	Total 1000 IP Conferencing Phones/third party SIP phones
KX-NSM705	5 SIP Extension	Allows the use of 5 IP Conferencing Phones/third party SIP phones.		
KX-NSM710	10 SIP Extension	Allows the use of 10 IP Conferencing Phones/third party SIP phones.		
KX-NSM720	20 SIP Extension	Allows the use of 20 IP Conferencing Phones/third party SIP phones.		

¹ You can set how many IP softphones can be used with the installed activation keys through system programming. By default, only IP softphones can be used with the installed activation keys.

² The number of telephones depends on the value selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

For details, refer to "Maximum Trunks and Extensions" in "2.3.3 System Capacity".

³ The capacity given in [square brackets] shows the number of activation keys preinstalled on the mother board.

Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSM201	1 IPSoftphone/IP PT	✓	✓
KX-NSM205	5 IPSoftphone/IP PT		
KX-NSM210	10 IPSoftphone/IP PT		
KX-NSM220	20 IPSoftphone/IP PT		
KX-NSM501	1 IP PT	✓	✓
KX-NSM505	5 IP PT		
KX-NSM510	10 IP PT		
KX-NSM520	20 IP PT		
KX-NSM701	1 SIP Extension	✓	✓
KX-NSM705	5 SIP Extension		
KX-NSM710	10 SIP Extension		
KX-NSM720	20 SIP Extension		

Networking

Model No.	Activation Key Type	Description	Maximum Activation Keys	
			Stand-alone System	One-look Network
KX-NSN001	One-look Network	Allows the use of multi-site connections using One-look network feature.	-	16 activation keys ¹
KX-NSN002	QSIG Network	Allows the use of enhanced QSIG network features (NDSS, Centralised Voice Mail, etc.).	1 activation key	

¹ This activation key must be installed to each PBX in the One-look network.

Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSN001	One-look Network	✓	✓
KX-NSN002	QSIG Network	✓	-

Feature Guide References for Related Features of Activation Keys

One-look Network

4.2.1 One-look Networking Overview

QSIG Network

- 4.3.1.4 Common Extension Numbering for 2 PBXs
- 4.3.2.2 Common Extension Numbering for Multiple PBXs
- 4.3.5 QSIG Enhanced Features
- 4.3.5.1 Network Direct Station Selection (NDSS)
- 4.3.5.2 Centralised Voice Mail

Built-in Router

Model No.	Activation Key Type	Description	Maximum Activation Keys	
			Stand-alone System	One-look Network
KX-NSN101	Built-in Router AK	Allows use of the Built-in Router.	1 activation key	16 (1/Site) activation keys

Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSN101	Built-in Router AK	✓	✓

Installation Manual References for Related Features of Activation Keys

8.6 Built-in Router

3.1.1 Type and Maximum Number of Activation Keys

IPsec (VPN)

Model No.	Activation Key Type	Description	Maximum Activation Keys	
			Stand-alone System	One-look Network
KX-NSN216	16ch IPsec AK	Allows the creation of up to 16 IPsec VPN connections.	2 activation keys	32 (2/Site) activation keys

Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSN216	16ch IPsec AK	✓	✓

Installation Manual References for Related Features of Activation Keys

8.6 Built-in Router

Unified Messaging System (Features)

Model No.	Activation Key Type	Description	Maximum Activation Keys	
			Stand-alone System	One-look Network
KX-NSU001	REC Time Expansion	Allows the use of 15 hours of recording time for Unified Messaging. This activation key works only for the Storage Memory Card provided with the PBX. Recording time can be increased further by upgrading the Storage Memory Card. For details, refer to "4.3.2 Storage Memory Card (installed by default), Storage Memory S Card (KX-NS0135), Storage Memory M Card (KX-NS0136), Storage Memory L Card (KX-NS0137)".	1 activation key	16 activation keys ¹
KX-NSU002	Two-way REC Control	Allows a manager/administrator to use the Automatic Two-way Recording feature to record other users.	1 activation key	16 activation keys ¹
KX-NSU003	Message Backup	Allows the automatic backup of messages.	1 activation key	16 activation keys ¹

¹ Activation keys must be installed to the site where the Unified Messaging mailboxes are located.

Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSU001	REC Time Expansion	✓	✓

Activation Keys		Master Unit	Slave Unit
KX-NSU002	Two-way REC Control	✓	✓
KX-NSU003	Message Backup	✓	✓

Feature Guide References for Related Features of Activation Keys

Two-way REC Control

3.2.1.4 Automatic Two-way Recording for Manager

Message Backup

3.1.2.5 System Backup/Restore

Unified Messaging System (Unified Messaging Ports)

Model No.	Activation Key Type	Description	Maximum Unified Messaging Ports	
			Stand-alone System	One-look Network
KX-NSU102	2 UM Port	Allows the use of 2 Unified Messaging ports.	24 Unified Messaging ports ¹ [2 Unified Messaging ports]	384 Unified Messaging ports ¹ [32 Unified Messaging ports]
KX-NSU104	4 UM Port	Allows the use of 4 Unified Messaging ports.		

¹ Activation keys must be installed to the site where the Unified Messaging mailboxes are located.

Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSU102	2 UM Port	✓	✓
KX-NSU104	4 UM Port		

Feature Guide References for Related Features of Activation Keys

3.1.1 Unified Messaging System Overview

3.1.1 Type and Maximum Number of Activation Keys

Unified Messaging System (Mailbox)

Model No.	Activation Key Type	Description	Maximum Mailboxes	
			Stand-alone System	One-look Network
KX-NSU201	UM/E-mail 1 User ¹	Allows the use of an e-mail (IMAP4) client and e-mail notification (voice/fax messages) for 1 user.	1024 mailboxes	16 384 mailboxes
KX-NSU205	UM/E-mail 5 Users ¹	Allows the use of an e-mail (IMAP4) client and e-mail notification (voice/fax messages) for 5 users.		
KX-NSU210	UM/E-mail 10 Users ¹	Allows the use of an e-mail (IMAP4) client and e-mail notification (voice/fax messages) for 10 users.		
KX-NSU220	UM/E-mail 20 Users ¹	Allows the use of an e-mail (IMAP4) client and e-mail notification (voice/fax messages) for 20 users.		
KX-NSU299	UM/E-mail All Users ¹	Allows the use of an e-mail (IMAP4) client and e-mail notification (voice/fax messages) up to the system's limit.		

¹ Activation keys must be installed to the site where the Unified Messaging mailboxes are located.

Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSU201	UM/E-mail 1 User		
KX-NSU205	UM/E-mail 5 Users		
KX-NSU210	UM/E-mail 10 Users	✓	✓
KX-NSU220	UM/E-mail 20 Users		
KX-NSU299	UM/E-mail All Users		

Feature Guide References for Related Features of Activation Keys

- 3.2.1.29 Message Waiting Notification—E-mail Device
- 3.3.1 Integration with Microsoft Outlook
- 3.3.2 IMAP Integration

Unified Messaging System (Two-way Recording/Two-way Transfer Users)

Model No.	Activation Key Type	Description	Maximum Users	
			Stand-alone System	One-look Network
KX-NSU301	2way REC 1 User	Allows the use of Two-way Recording/Two-way Transfer for 1 user.	640 users	1000 users
KX-NSU305	2way REC 5 Users	Allows the use of Two-way Recording/Two-way Transfer for 5 users.		
KX-NSU310	2way REC 10 Users	Allows the use of Two-way Recording/Two-way Transfer for 10 users.		
KX-NSU320	2way REC 20 Users	Allows the use of Two-way Recording/Two-way Transfer for 20 users.		
KX-NSU399	2way REC All Users	Allows the use of Two-way Recording/Two-way Transfer up to the system's limit.		

Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSU301	2way REC 1 User	✓	-
KX-NSU305	2way REC 5 Users		
KX-NSU310	2way REC 10 Users		
KX-NSU320	2way REC 20 Users		
KX-NSU399	2way REC All Users		

Feature Guide References for Related Features of Activation Keys

3.2.2.34 Two-way Record/Two-way Transfer

3.1.1 Type and Maximum Number of Activation Keys

Cellular Phone Extension

Model No.	Activation Key Type	Description	Maximum Cellular Phone Extensions	
			Stand-alone System	One-look Network
KX-NSE101	1 Mobile User	Allows the use of 1 cellular phone extension.	1152 cellular phone extensions	
KX-NSE105	5 Mobile Users	Allows the use of 5 cellular phone extensions.		
KX-NSE110	10 Mobile Users	Allows the use of 10 cellular phone extensions.		
KX-NSE120	20 Mobile Users	Allows the use of 20 cellular phone extensions.		

Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSE101	1 Mobile User	✓	-
KX-NSE105	5 Mobile Users		
KX-NSE110	10 Mobile Users		
KX-NSE120	20 Mobile Users		

Feature Guide References for Related Features of Activation Keys

- 2.2.2.3 Outside Destinations in Incoming Call Distribution Group
- 2.3.2 Call Forwarding (FWD)
- 2.16.1 Direct Inward System Access (DISA)
- 2.27.1 Cellular Phone Features—SUMMARY
- 4.3.6 Network ICD Group
- 4.3.6.1 PS Roaming by Network ICD Group

Communication Assistant (CA) User

Model No.	Activation Key Type	Description	Maximum Activation Keys	
			Stand-alone System	One-look Network
KX-NSA010	CA Thin Client	Allows the use of CA Client in a thin-client environment.	1	
KX-NSA020	CSTA Multiplexer	Allows the use of CSTA Multiplexer.	4	

3.1.1 Type and Maximum Number of Activation Keys

Model No.	Activation Key Type	Description	Maximum Activation Keys	
			Stand-alone System	One-touch Network
KX-NSA201	CA Pro 1 user	Allows the use of CA Client Pro for 1 user. ¹	240 ² users without CA server (Max. 1022 ³ users with CA server)	
KX-NSA205	CA Pro 5 users	Allows the use of CA Client Pro for 5 users. ¹		
KX-NSA210	CA Pro 10 users	Allows the use of CA Client Pro for 10 users. ¹		
KX-NSA240	CA Pro 40 users	Allows the use of CA Client Pro for 40 users. ¹		
KX-NSA249	CA Pro 128 users	Allows the use of CA Client Pro for 128 users. ¹		
KX-NSA301	CA Supervisor	Allows the use of CA Client Supervisor for 1 user.		
KX-NSA401	CA Console	Allows the use of CA Client Operator Console for 1 user.		
KX-NSA901	CA Network 1 user	Allows the use of CA Server network features for 1 user.		
KX-NSA905	CA Network 5 users	Allows the use of CA Server network features for 5 users.		
KX-NSA910	CA Network 10 users	Allows the use of CA Server network features for 10 users.		
KX-NSA940	CA Network 40 users	Allows the use of CA Server network features for 40 users.		
KX-NSA949	CA Network 128 users	Allows the use of CA Server network features for 128 users.		

¹ A maximum of 1022 CA users can be registered. However, CA Server is necessary to register more than 240 CA users.

² The maximum number of Supervisor users without CA server is 4 users.

³ The maximum number of Operator Console and Supervisor users combined when CA Server is used is 128 users.

3.1.1 Type and Maximum Number of Activation Keys

Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSA010	CA Thin Client		
KX-NSA020	CSTA Multiplexer		
KX-NSA201	CA Pro 1 user		
KX-NSA205	CA Pro 5 users		
KX-NSA210	CA Pro 10 users		
KX-NSA240	CA Pro 40 users		
KX-NSA249	CA Pro 128 users	✓	-
KX-NSA301	CA Supervisor		
KX-NSA401	CA Console		
KX-NSA901	CA Network 1 user		
KX-NSA905	CA Network 5 users		
KX-NSA910	CA Network 10 users		
KX-NSA940	CA Network 40 users		
KX-NSA949	CA Network 128 users		

CTI Licence

Model No.	Activation Key Type	Description	Maximum Activation Keys	
			Stand-alone System	One-look Network
KX-NSF101	CTI interface	Allows the use of the 3rd Party CTI interface.	1	

Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSF101	CTI interface	✓	

Feature Guide References for Related Features of Activation Keys

2.26.1 Computer Telephony Integration (CTI)

Partner Licence

Activation keys for partner devices are stored in the PBX. Partner devices refer to the activation keys in the PBX and determine whether they are enabled or disabled. A maximum number of 16 partner devices can refer to the activation keys and operate simultaneously. However, limitations on partner devices connected through

devices connected directly to the PBX depend on the specifications of the directly connected devices. The PBX does not limit these devices.

Note

- For information about purchasing licences, consult the partner entity or your dealer.
- To use devices by connecting them to CA Server, use a version of CA Server that corresponds to the partner licence feature.

Model No.	Activation Key Type	Description	Maximum Activation Keys	
			Stand-alone System	One-look Network
KX-NSB0001	Poltys C. Bridge	Allows the use of the Poltys Communication Bridge.	16	
KX-NSB0002	PSDN Option-1	Allows the use of the option feature of PSDN (Panasonic System Development Network).		
KX-NSB0003	PSDN Option-2			
KX-NSB0101	Poltys CA RCS-Start 1 user	Allows the use of the Poltys CA RCS for 1 user.		
KX-NSB0105	Poltys CA RCS-Start 5 users	Allows the use of the Poltys CA RCS for 5 users.		
KX-NSB0110	Poltys CA RCS-Start 10 users	Allows the use of the Poltys CA RCS for 10 users.		
KX-NSB0149	Poltys CA RCS-Start 128 users	Allows the use of the Poltys CA RCS for 128 users.		
KX-NSB0201	Poltys CA RCS-Extend 1 user	Allows the extension to use of the Poltys CA RCS for 1 user.		
KX-NSB0205	Poltys CA RCS-Extend 5 users	Allows the extension to use of the Poltys CA RCS for 5 users.		
KX-NSB0210	Poltys CA RCS-Extend 10 users	Allows the extension to use of the Poltys CA RCS for 10 users.		
KX-NSB0249	Poltys CA RCS-Extend 128 users	Allows the extension to use of the Poltys CA RCS for 128 users.		

¹ Combined with number of CA Client users.

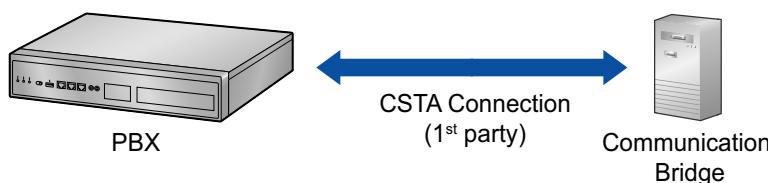
² If **Standard Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

³ If **IP-Extension Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

⁴ If **System Resource Type** is selected for **System Capacity Selection** in Easy Setup Wizard. (Refer to "5.4.1 Easy Setup Wizard".)

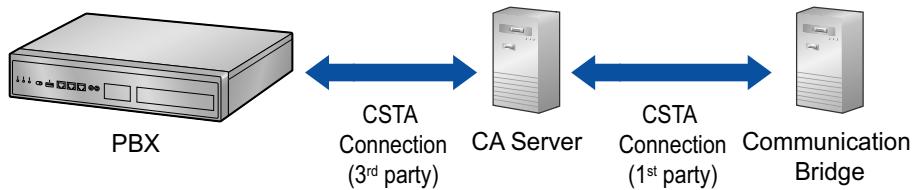
System connection diagram for the integration with the Communication Bridge

[Without CA server]



3.1.1 Type and Maximum Number of Activation Keys

[With CA server]



Installation in One-look Network System

Activation Keys		Master Unit	Slave Unit
KX-NSB0001	Poltys C. Bridge		
KX-NSB0002	PSDN Option-1		
KX-NSB0003	PSDN Option-2		
KX-NSB0101	Poltys CA RCS-Start 1 user		
KX-NSB0105	Poltys CA RCS-Start 5 users		
KX-NSB0110	Poltys CA RCS-Start 10 users		
KX-NSB0149	Poltys CA RCS-Start 128 users	✓	-
KX-NSB0201	Poltys CA RCS-Extend 1 user		
KX-NSB0205	Poltys CA RCS-Extend 5 users		
KX-NSB0210	Poltys CA RCS-Extend 10 users		
KX-NSB0249	Poltys CA RCS-Extend 128 users		

Feature Guide References for Related Features of Activation Keys

2.26.3 Integration with Communication Bridge

Call Centre Feature Enhancement

Model No.	Activation Key Type	Description	Maximum Activation Keys	
			Stand-alone System	One-look Network
KX-NSF201	Call Centre Enhance	Allows the use of queuing information announcement, ICD group monitor by ACD supervisor, and creation of ACD reports.	1	

Installation in One-look Network System

Activation Keys	Master Unit	Slave Unit
KX-NSF201	Call Centre Enhance	✓

Feature Guide References for Related Features of Activation Keys

- 2.2.2.4 Queuing Feature
 2.2.2.9 Supervisory Feature (ACD)

Packaged Activation Keys

These packaged activation keys include multiple activation keys. Installing one packaged activation key allows you to install multiple activation key features at once.

For details of each feature, refer to relevant section of this manual:

- E-mail (IMAP4) client and e-mail notification (voice/fax messages)
 → Unified Messaging System (Mailbox)
- Two-way Recording/Two-way Transfer
 → Unified Messaging System (Two-way Recording/Two-way Transfer Users)
- Cellular phone extension
 → Cellular Phone Extension
- CA Client Pro
 → Communication Assistant (CA) User

Model No.	Activation Key Type	Description
KX-NSP001	Std. Pkg 1 User	Allows the use of the following activation key features for 1 user: <ul style="list-style-type: none"> • E-mail (IMAP4) client and e-mail notification (voice/fax messages) • Two-way Recording/Two-way Transfer
KX-NSP005	Std. Pkg 5 Users	Allows the use of the following activation key features for 5 users: <ul style="list-style-type: none"> • E-mail (IMAP4) client and e-mail notification (voice/fax messages) • Two-way Recording/Two-way Transfer
KX-NSP010	Std. Pkg 10 Users	Allows the use of the following activation key features for 10 users: <ul style="list-style-type: none"> • E-mail (IMAP4) client and e-mail notification (voice/fax messages) • Two-way Recording/Two-way Transfer
KX-NSP020	Std. Pkg 20 Users	Allows the use of the following activation key features for 20 users: <ul style="list-style-type: none"> • E-mail (IMAP4) client and e-mail notification (voice/fax messages) • Two-way Recording/Two-way Transfer
KX-NSP101	Adv. Pkg 1 User	Allows the use of the following activation key features for 1 user: <ul style="list-style-type: none"> • E-mail (IMAP4) client and e-mail notification (voice/fax messages) • Two-way Recording/Two-way Transfer • Cellular phone extension • CA Client Pro

3.1.1 Type and Maximum Number of Activation Keys

Model No.	Activation Key Type	Description
KX-NSP105	Adv. Pkg 5 Users	Allows the use of the following activation key features for 5 users: <ul style="list-style-type: none"> • E-mail (IMAP4) client and e-mail notification (voice/fax messages) • Two-way Recording/Two-way Transfer • Cellular phone extension • CA Client Pro
KX-NSP110	Adv. Pkg 10 Users	Allows the use of the following activation key features for 10 users: <ul style="list-style-type: none"> • E-mail (IMAP4) client and e-mail notification (voice/fax messages) • Two-way Recording/Two-way Transfer • Cellular phone extension • CA Client Pro
KX-NSP120	Adv. Pkg 20 Users	Allows the use of the following activation key features for 20 users: <ul style="list-style-type: none"> • E-mail (IMAP4) client and e-mail notification (voice/fax messages) • Two-way Recording/Two-way Transfer • Cellular phone extension • CA Client Pro
KX-NSP201	Mobile Pkg 1 User	Allows the use of the following activation key features for 1 user: <ul style="list-style-type: none"> • E-mail (IMAP4) client and e-mail notification (voice/fax messages) • Cellular phone extension
KX-NSP205	Mobile Pkg 5 Users	Allows the use of the following activation key features for 5 users: <ul style="list-style-type: none"> • E-mail (IMAP4) client and e-mail notification (voice/fax messages) • Cellular phone extension
KX-NSP210	Mobile Pkg 10 Users	Allows the use of the following activation key features for 10 users: <ul style="list-style-type: none"> • E-mail (IMAP4) client and e-mail notification (voice/fax messages) • Cellular phone extension
KX-NSP220	Mobile Pkg 20 Users	Allows the use of the following activation key features for 20 users: <ul style="list-style-type: none"> • E-mail (IMAP4) client and e-mail notification (voice/fax messages) • Cellular phone extension

Preinstalled Activation Keys in the Mother Board

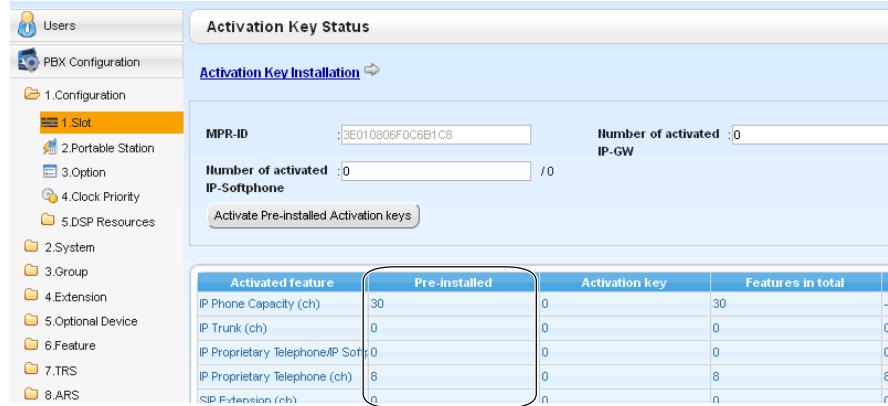
Preinstalled activation keys with no expiration date

The following type and number of activation keys are preinstalled on the mother board.

Activation Key	Activated Features
IP Phone Capacity (ch)	Capacity for up to 30 IP-PTs/IP softphones/ KX-UT series SIP phones/third party SIP phones
CA Basic-Express	1022 users
IP Proprietary Telephone (ch)	8 IP-PTs/KX-UT series SIP phones

Activation Key	Activated Features
UM Port (ch)	2 Unified Messaging ports

Example: Preinstalled Activation Keys in the Mother Board



Preinstalled activation keys for free trial

The following activation keys are preinstalled on the mother board for the 60-days free trial. They will expire 60 days after pressing the **Activate Pre-installed Activation key** button to begin the free trial.

Activation Key	Activated Features
One-look Network	One-look networking feature
Two-way Recording Control	Automatic Two-way Recording feature
Message Backup	Automatic backup of messages
UM/E-mail (128 user)	128 mailboxes
Two-Way Recording (30 users)	30 Two-way Recording/Two-way Transfer users
Mobile Extension (30 users)	30 cellular phone extensions
CA PRO (128 users)	128 CA Pro users
CA Supervisor (1 user)	1 CA Supervisor user
CA Operator Console (1 user)	1 CA Console user
CA Thin Client Server	Use CA in a thin-client environment
CSTA Multiplexer	Multiplexing for CSTA connections
CTI interface	3rd Party CTI interface
Activation Key for Call Centre Feature Enhancement	Queuing information announcement/ACD Supervisor/ACD Report
Built-in Router	Built-in router feature
16-channel IPsec Activation Key	IPsec connection
Polys C. Bridge	Allows the use of the Polys C. Bridge.

3.1.1 Type and Maximum Number of Activation Keys

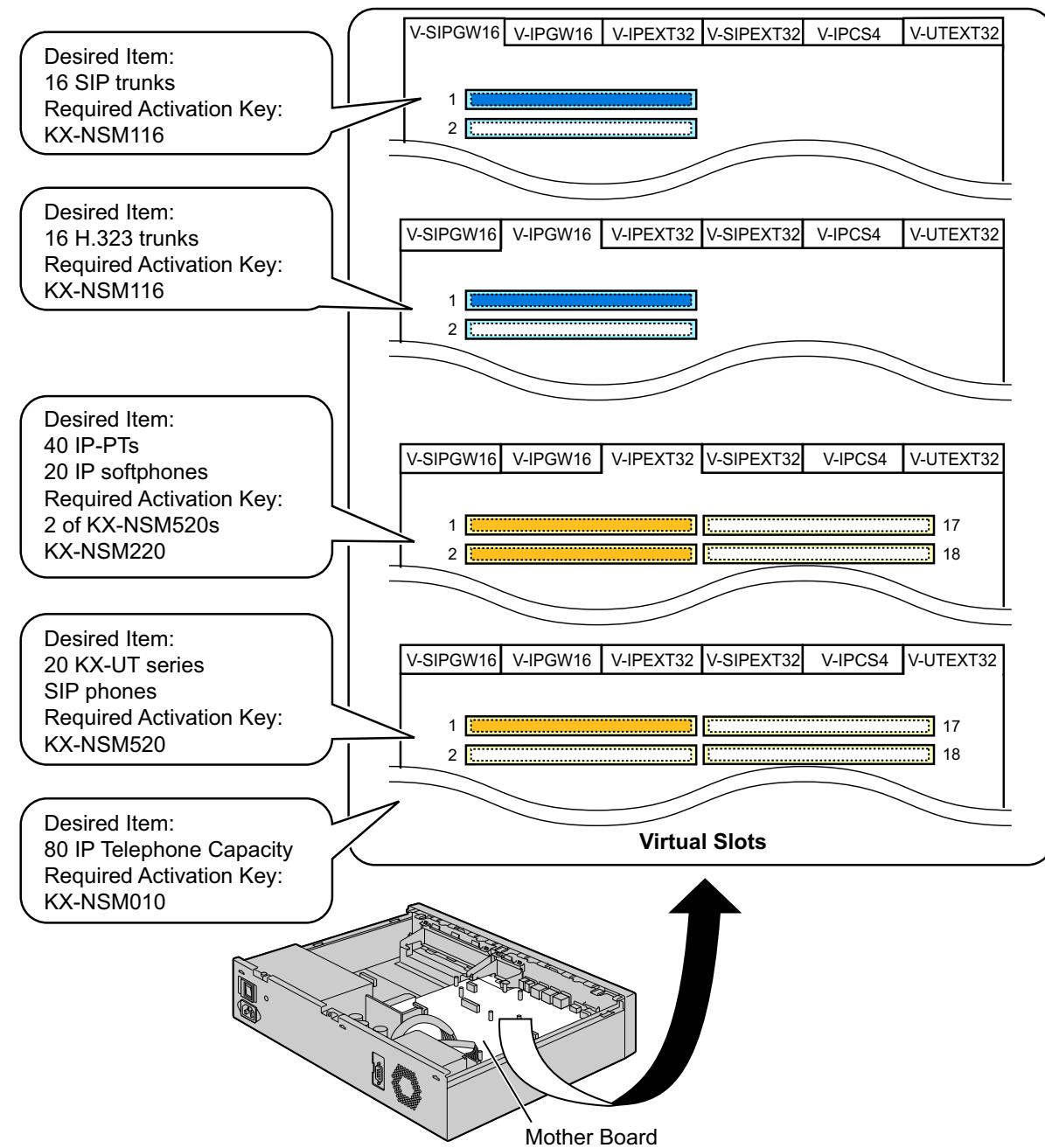
Activation Key	Activated Features
Poltys CA RCS-Start (5users)	Allows the use of the Poltys CA RCS. ¹

¹ If you activate the Poltys CA RCS-Start (5users) activation key, Poltys CA RCS-Extend (5users) will also be activated.

Activation Key Installation Example

The following illustration shows an example of when using 16 SIP trunks, 16 H.323 trunks, 40 IP-PTs, 20 IP softphones, and 20 KX-UT series SIP phones on a private IP network using the mother board.

Example:



Note

- Up to 30 IP-PTs/IP softphones/KX-UT series SIP phones/third party SIP phones can be used without needing any of the IP telephone capacity activation key files.
- Activation keys for IP telephone capacity are not cumulative; the maximum overall capacity is determined by the highest-numbered installed activation key. In this case, the Up to 100 IP Phone activation key (KX-NSM010) is used for 80 IP telephones.

3.1.2 Activation Key Code and Key Management System

To obtain additional activation keys, you need to purchase the appropriate activation key codes and access the Key Management System. You can download the activation keys as an activation key file from the Key Management System.

To download the activation keys, enter the MPR ID number shown on the back of the main unit, and activation key number and registration ID provided on each activation key code.

For information about the type of activation key codes available, refer to "3.1.1 Type and Maximum Number of Activation Keys".

For details about installing the downloaded activation key file(s) in the directory where the activation key files are stored, using Web Maintenance Console, refer to "5.4.4 Installing Additional Activation Keys".

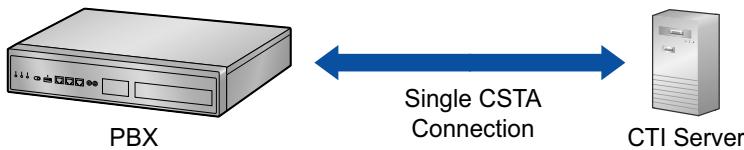
Note

- You can only download the activation key file once using the activation key number and registration ID provided on the activation key code.
- Up to 8 activation keys can be downloaded as one activation key file.
- Up to 997 activation key files can be installed in the optional upgrade Storage Memory Card.
- It is possible to send the activation key file to a specified e-mail address at the same time as downloading it to a PC.
- Make sure to backup the downloaded activation key files on your PC.
- When the mother board has to be replaced due to a system malfunction, the MPR ID for the mother board is no longer valid. In this case, you need a temporary activation key for maintenance purposes. The temporary activation key can only be used for a limited time period, and can be downloaded from the Key Management System in the same way as downloading activation key files.

3.1.3 Using CTI Applications

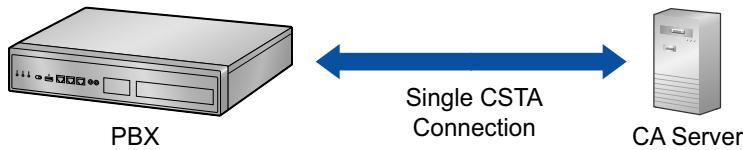
To use CTI applications with the KX-NS1000, KX-NSF101 (CTI interface) is required. One KX-NSF101 supports one CTI application. However, Communication Assistant (CA) Server does not require KX-NSF101. In the example below, one KX-NSF101 is required for using one CTI application.

Example 1



In the example below, an activation key is not required to use CA Server.

Example 2

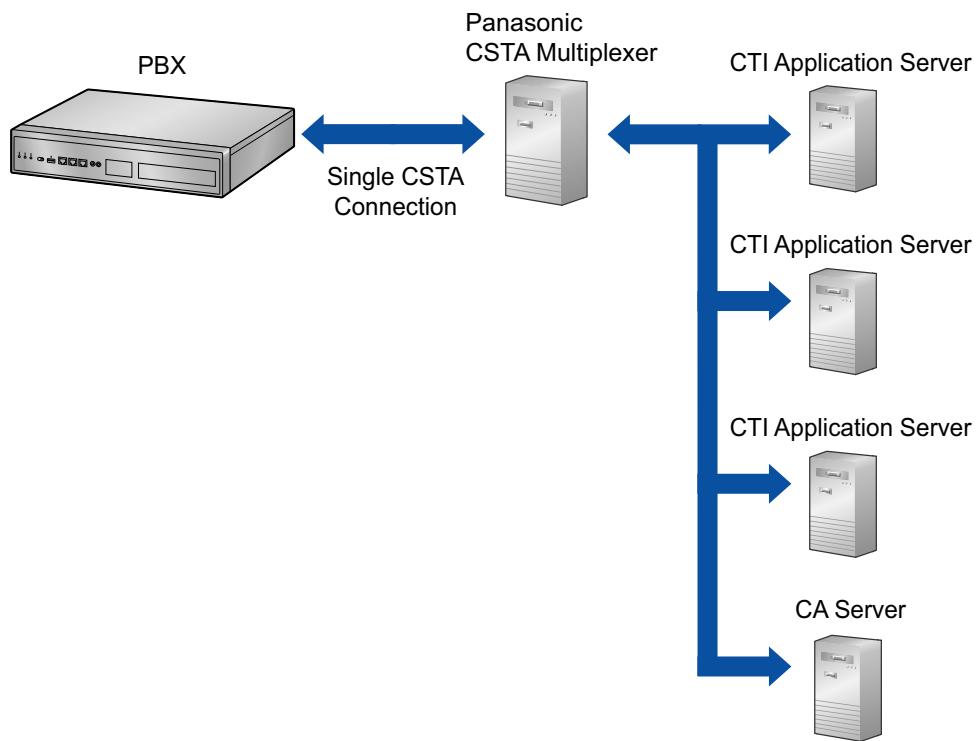


To use 2 or more CTI applications, the CSTA Multiplexer application is required, along with one KX-NSA020 (CSTA Multiplexer) for each CTI application. KX-NSF101 is included in KX-NSA020. Therefore, when KX-NSA020 is installed, KX-NSF101 is not required.

In the example below, three KX-NSA020 are required for three CTI applications. (CA Server does not require a KX-NSA020.)

3.1.3 Using CTI Applications

Example 3



Note

- Up to 4 CTI application servers can be used at the same time when using a CSTA multiplexer.
- An Activation Key for Multiple CSTA Connection (KX-NSA020) is required for each CTI application.
- When a 3rd party CSTA multiplexer is used, a Activation Key for CTI interface (KX-NSF101) is required for the CSTA connection. (In this case, Activation Key for Multiple CSTA Connection [KX-NSA020] is not required.)
- For details regarding KX-NSF101, refer to "CTI Licence" in "3.1.1 Type and Maximum Number of Activation Keys".
- For details regarding KX-NSA020, refer to "Communication Assistant (CA) User" in "3.1.1 Type and Maximum Number of Activation Keys".

Section 4

Installation

This section describes the procedures to install the PBX. Detailed instructions for planning the installation site, installing the main unit and optional service cards, and cabling of peripheral equipment are provided. Further information on peripheral equipment installation is included.

4.1 Before Installation

4.1.1 Before Installation

Please read the following notes concerning installation and connection before installing the PBX and terminal equipment.

Be sure to comply with all applicable laws, regulations, and guidelines.

Notice

Panasonic assumes no responsibility for injuries or property damage resulting from failures arising out of improper installation or operation inconsistent with this documentation.

Safety Installation Instructions

WARNING

When installing telephone wiring, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Anti-static precautions should be taken during installation.

Installation Precautions

The PBX is suitable for mounting on a 19-inch rack, mounting on a wall, or placing on a desktop, and should be installed in a location where it is accessible for inspections and maintenance.

To prevent malfunction, noise, or discolouration, follow the instructions below:

WARNING

Do not install the system in the following locations:

- Areas where shocks or vibrations are frequent or strong. Such activity may lead to the product falling over and causing injury, or may impair the product's performance.
- Areas with high amounts of dust. High amounts of dust can lead to fire or electric shock, and impair the performance of the product.

CAUTION

Do not install the system in the following locations:

- In direct sunlight and hot, cold, or humid places. (Temperature range: 0 °C to 40 °C)
- Areas where sulphuric gases may be present, such as near thermal springs.
- Near devices that generate high frequencies, such as sewing machines or electric welders.
- Locations where other objects will obstruct the area around the PBX. Be especially careful to leave at least 5 cm to the sides of the PBX for ventilation.
- Locations where condensation can occur.

Notice

Do not install the system in the following locations:

- On or near computers, or other office equipment, as well as microwave ovens or air conditioners. (It is preferable not to install the system in the same room as the above equipment.)
- Within 1.8 m of radios and televisions. (Both the PBX and PTs should be at least 1.8 m away from such devices.)

Do not perform the following:

- Do not block the openings of the PBX.
- Do not stack up the optional service cards.

Wiring Precautions

Be sure to follow these instructions when wiring the unit:

CAUTION

- Avoid using the same AC outlet for computers and other office equipment, as noise generated by such equipment may hamper system performance or interrupt the system.
- Unplug the system from its power source when wiring, and plug the system back in only after all wiring is completed.
- Trunks should be installed with surge protectors. For details, refer to "4.2.12 Surge Protector Installation".

Notice

- Use 1-pair telephone cables when connecting SLTs, data terminals, answering machines, computers, etc.
- Mis-wiring may cause the PBX to operate improperly. Refer to "Section 4 Installation" when wiring the system.
- If an extension does not operate properly, disconnect the telephone from the extension line and connect it again, or turn off the PBX using the power switch, then turn it on again.
- Use twisted pair cable for trunk connection.
- To prevent signal noise from interfering with the performance of the product, do not run unshielded telephone cables near AC power cables, computer cables, AC power sources, etc. When running cables near other noise-generating devices or cables, use shielded telephone cables or shield the telephone cables with metal tubing.

Preparing the Network Environment

Be sure to prepare your network's environment for the installation of the PBX according to the intended PBX networking configuration. For details about PBX network configurations, refer to "Section 8 Networking Information".

4.2 Installation of the PBX

4.2.1 Unpacking

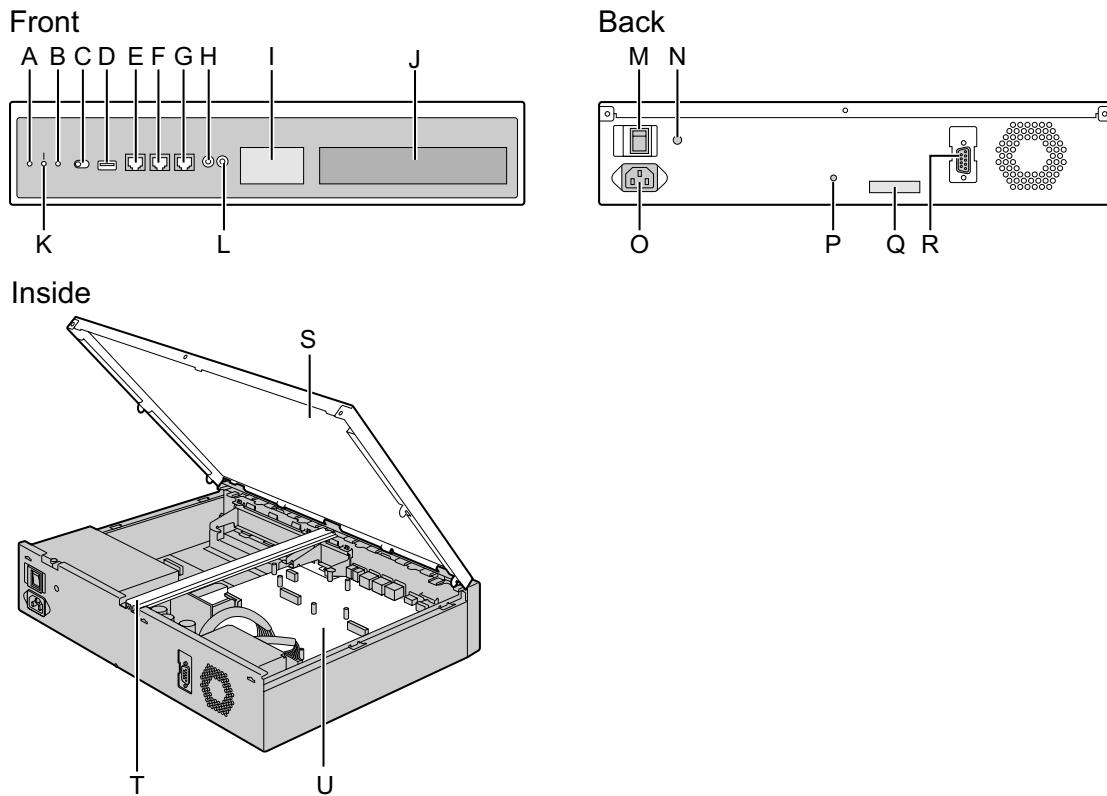
Unpack the box and check the items below:

- Main unit
- CD-ROM(s)^{*1}
- AC power cord^{*2}
- Hook clip
- 19-inch rack attachment bracket x 2
- Screw x 6

^{*1} The number of included CD-ROMs varies according to the country/area.

^{*2} The KX-NS1000BX and KX-NS1000XE are supplied with 2 types of AC power cord. Please use whichever is appropriate for the country/area.

4.2.2 Names and Locations



- A.** STATUS Indicator
- B.** MASTER Indicator^{*1}
- C.** System Mode Switch
- D.** USB Port
- E.** MNT Port
- F.** LAN Port
- G.** WAN Port
- H.** MOH Port
- I.** Doorphone Slot
- J.** Free Slot
- K.** BATT ALARM Indicator
- L.** Pager Port
- M.** Power Switch
- N.** Earth Terminal
- O.** AC Inlet
- P.** Hook Clip Hole
- Q.** MPR ID
- R.** RS-232C Port
- S.** Top Cover
- T.** Support Bar
- U.** Mother Board

^{*1} For details about the MASTER indicator, refer to "LED Indications".

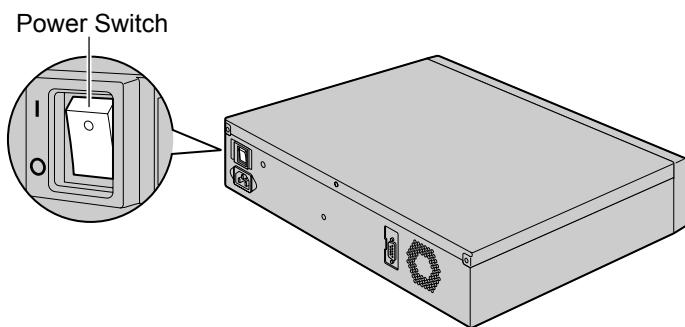
4.2.3 Opening/Closing the Top Cover

Opening the Top Cover

CAUTION

When opening the top cover, the power switch must be turned off.

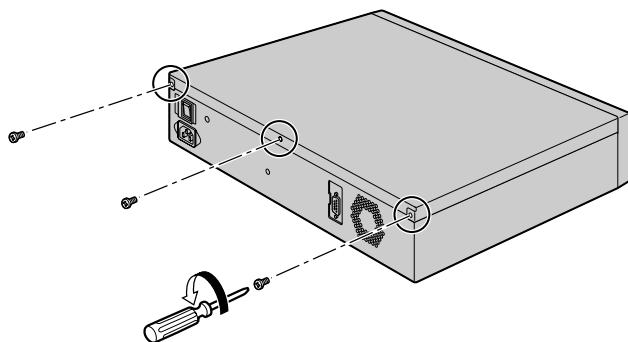
1. Confirm that the power switch is turned off.



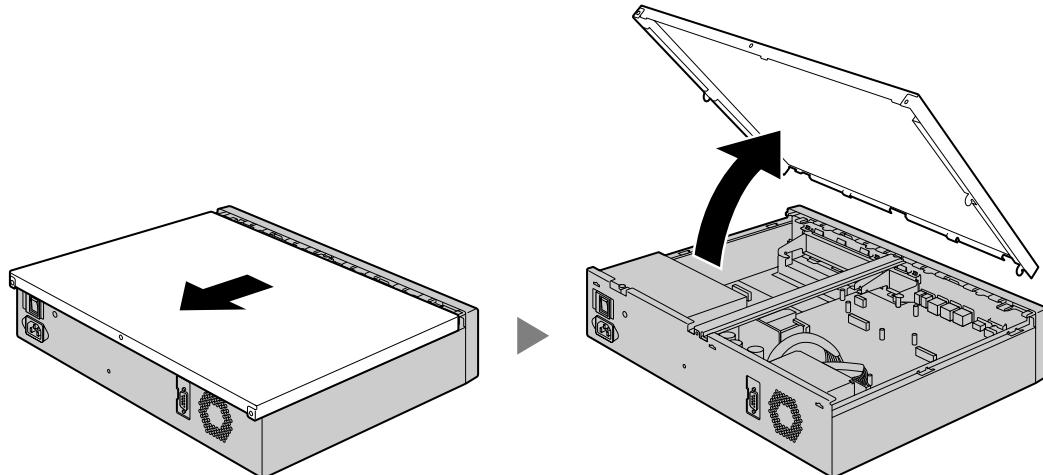
Note

In order to turn off the PBX's power, a system shutdown using Web Maintenance Console must first be performed. For details, refer to "5.5 System Control—System Shutdown" in the PC Programming Manual.

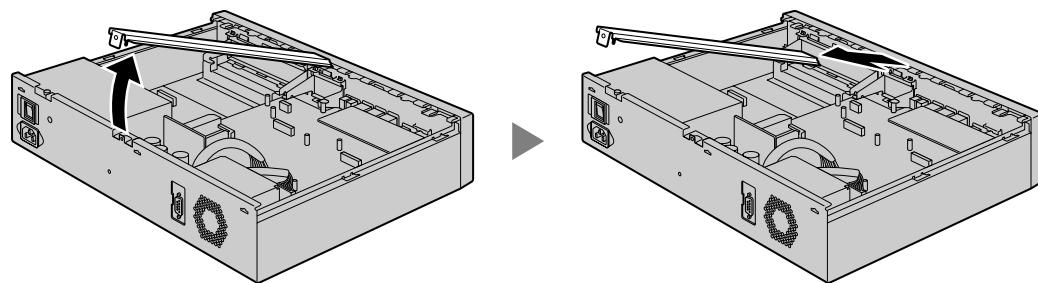
2. Turn the screws anticlockwise to loosen.



3. Slide the top cover then lift it off.

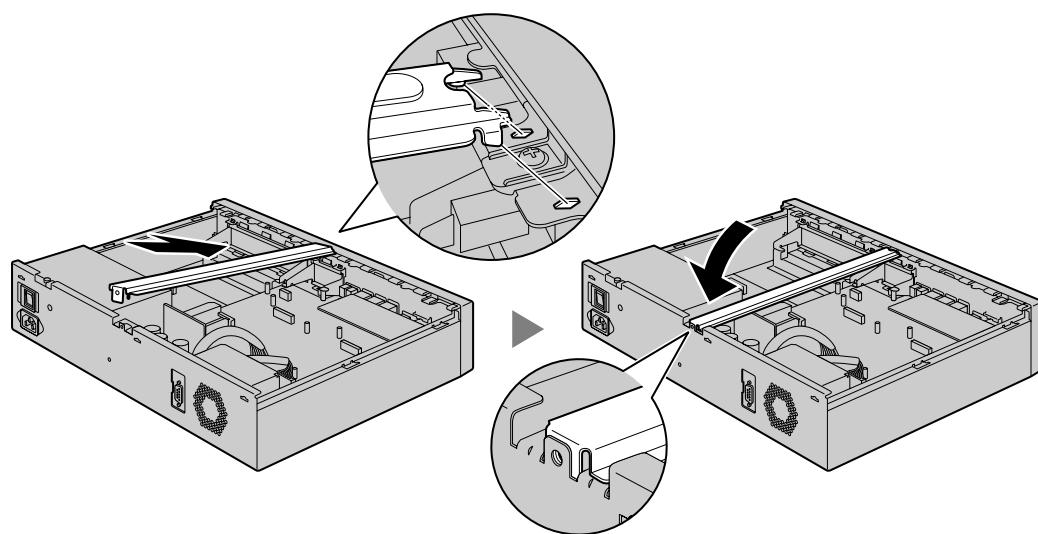


4. Remove the support bar from the PBX.



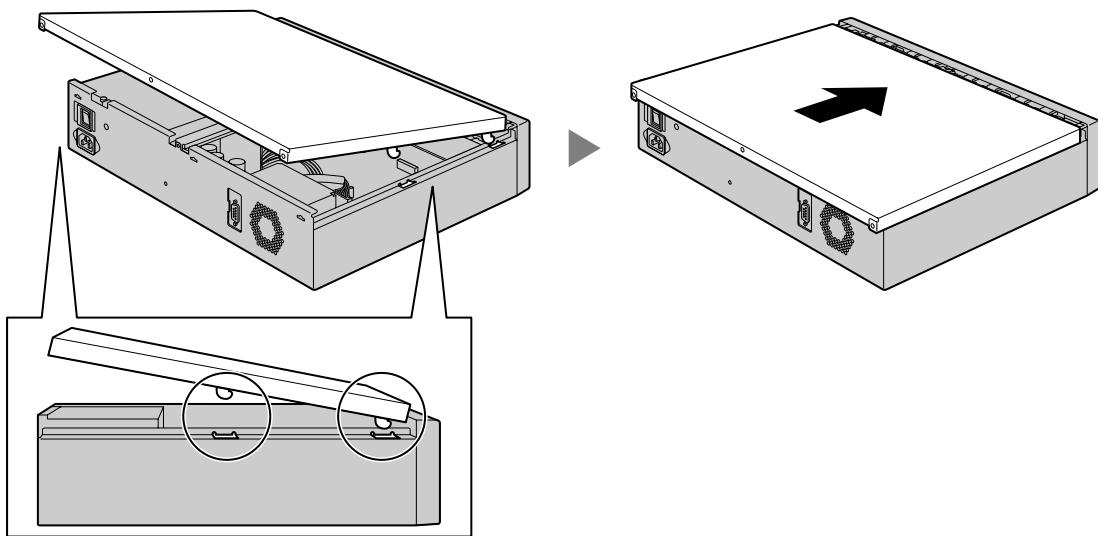
Closing the Top Cover

1. Place the support bar onto the PBX.

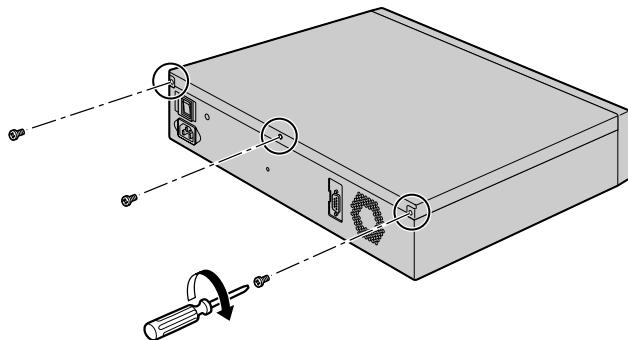


4.2.3 Opening/Closing the Top Cover

2. Place the top cover onto the PBX. Then slide the top cover until it closes properly.



3. Turn the screws clockwise to tighten.

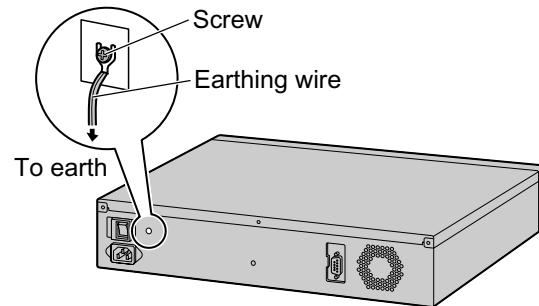


CAUTION

For safety reasons, close the top cover and tighten the screws before operating the PBX.

4.2.4 Frame Earth Connection

1. Loosen the screw.
2. Insert an earthing wire (user-supplied).
3. Tighten the screw.
4. Connect the earthing wire to earth.



WARNING

- Proper earthing (connection to earth) is very important to reduce the risk to the user of electrocution or to protect the PBX from the bad effects of external noise in the case of a lightning strike.
- The earthing wire of the AC cable has an effect against external noise and lightning strikes, but it may not be enough to protect the PBX and to ensure electromagnetic compatibility. A permanent connection between earth and the earth terminal of the PBX must be made.

CAUTION

For earthing wire, green-and-yellow insulation is required, and the cross-sectional area of the conductor must be more than 0.75 mm² or 18 AWG.

Notice

Be sure to comply with applicable local regulations (e.g., laws, guidelines).

4.2.5 Installing/Removing the Optional Service Cards

CAUTION

- Before touching the product (PBX, cards, etc.), discharge static electricity by touching ground or wearing an earthing strap. Failure to do so may cause the PBX to malfunction due to static electricity.
- When installing or removing the optional service cards, the power switch must be turned off.
- When installing or removing the optional service cards, do not put pressure on any parts of the mother board. Doing so may result in damage to the PBX.

Note

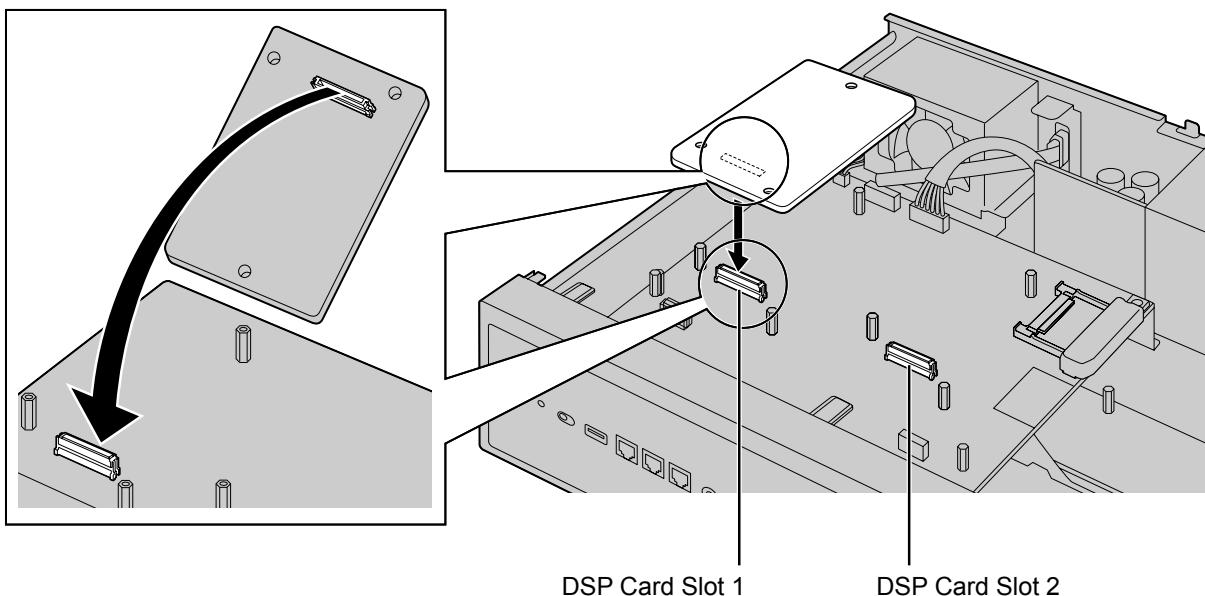
Make sure the AC power cord is not connected to the AC inlet of the PBX.

Installing a DSP Card in a DSP Card Slot

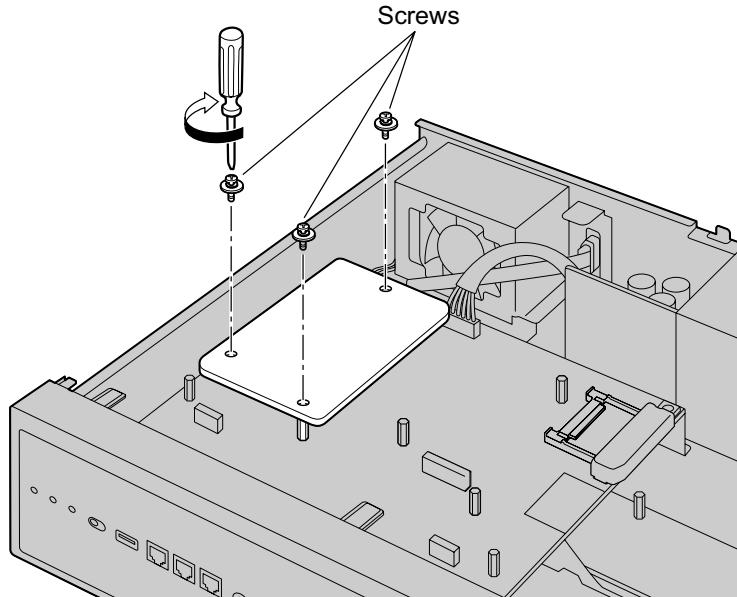
1. Position a DSP card in an open DSP card slot. Then holding the card firmly in place, lower the rear end so that the holes of the card are aligned with the screw holes.

Note

There are 2 DSP card slots on the mother board. When installing only 1 DSP card, only one DSP card slot will be used.

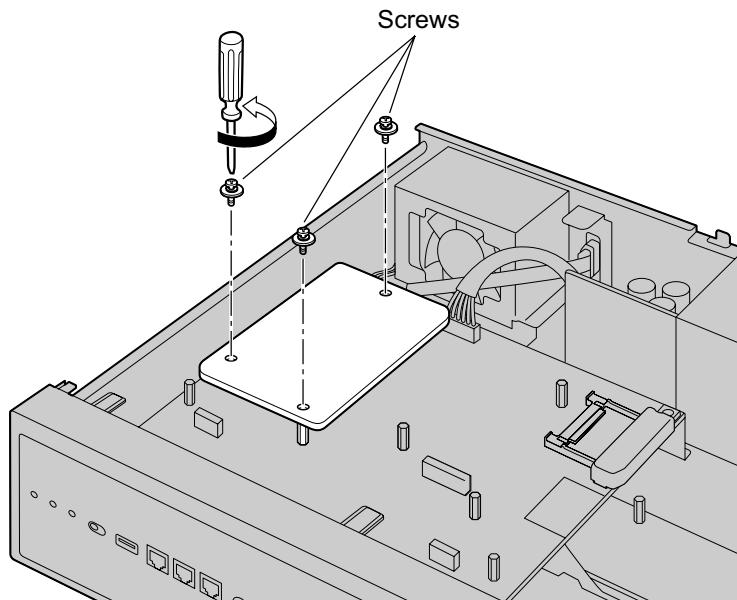


2. Insert the screws into the holes on the card, and tighten the screws to secure the card.



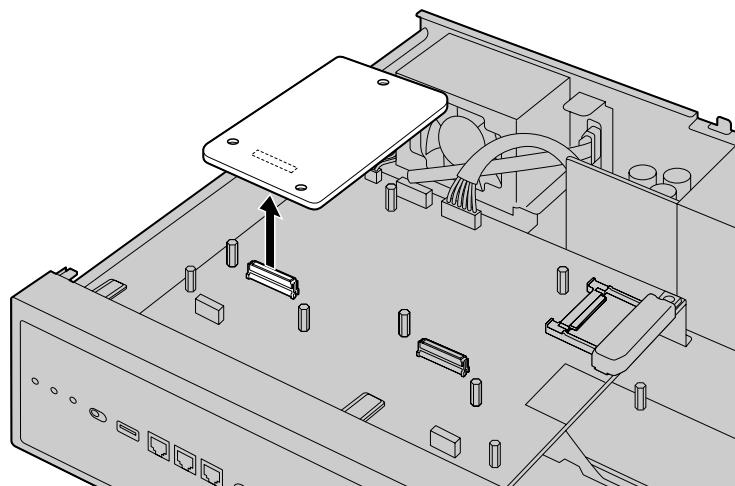
Removing a DSP Card Installed in the DSP Card Slot

1. Loosen and remove the screws.



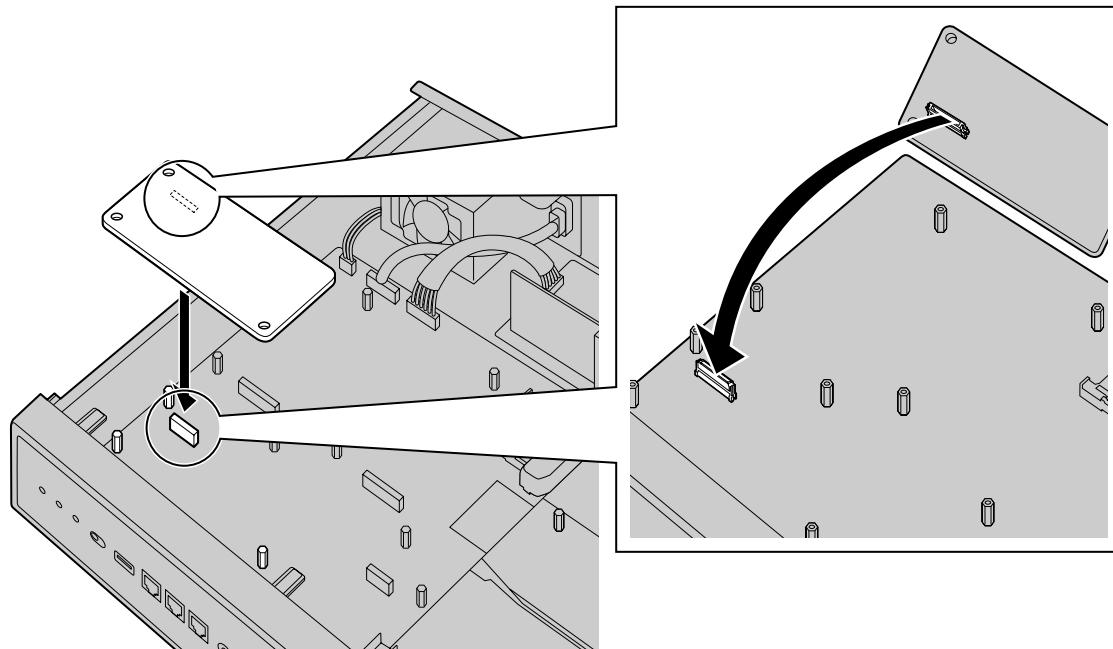
4.2.5 Installing/Removing the Optional Service Cards

2. Holding the rear end of the card, pull the card in the direction of the arrows.

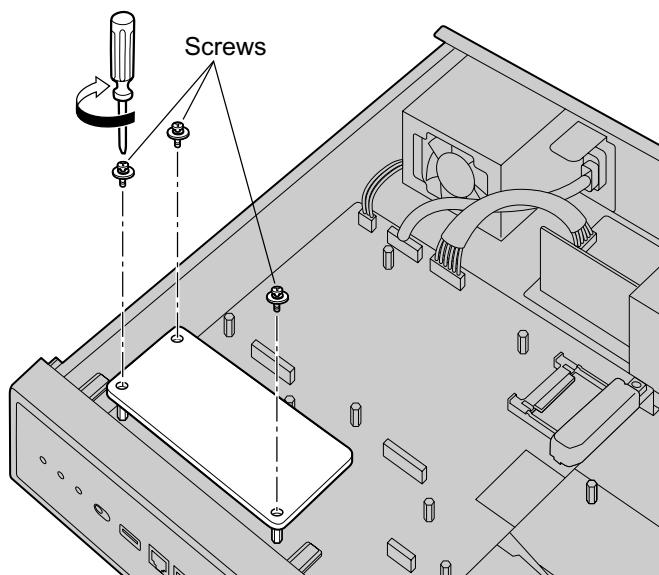


Installing the FAX Card in the FAX Card Slot

1. Position the FAX card in the FAX card slot. Then, holding the card firmly in place, lower the rear end so that the holes of the card are aligned with the screw holes.

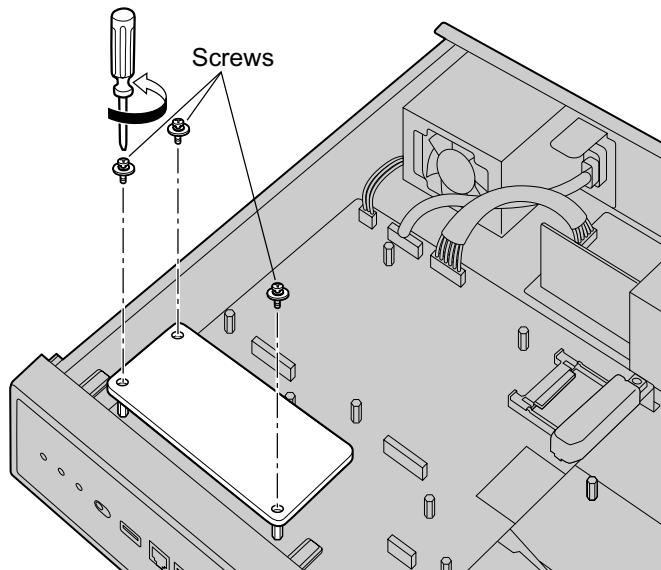


2. Insert the screws into the holes on the card, and tighten the screws to secure the card.

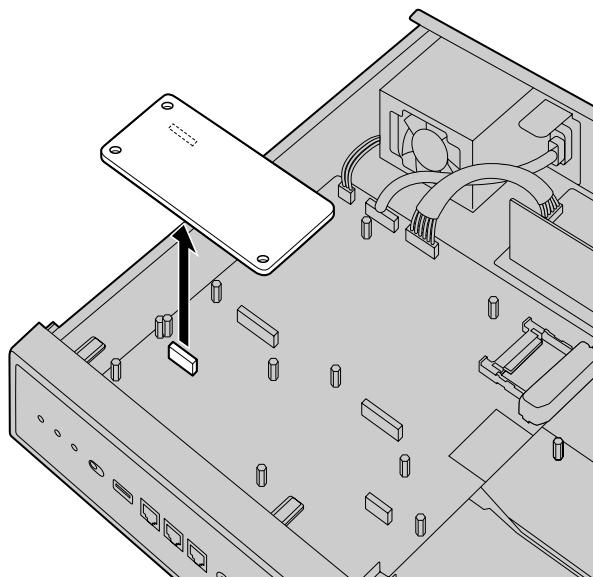


Removing a Fax Card Installed in the Fax Card Slot

1. Loosen and remove the screws.



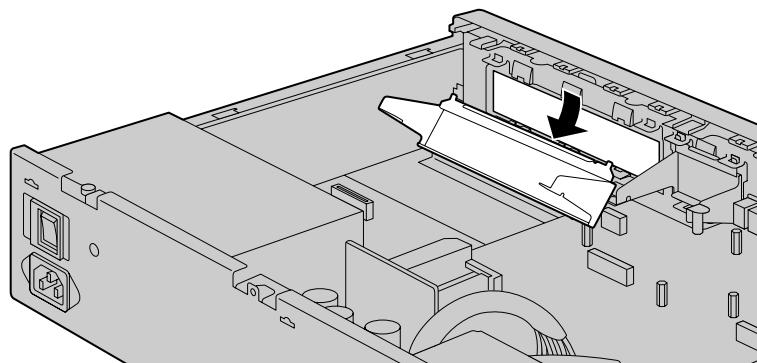
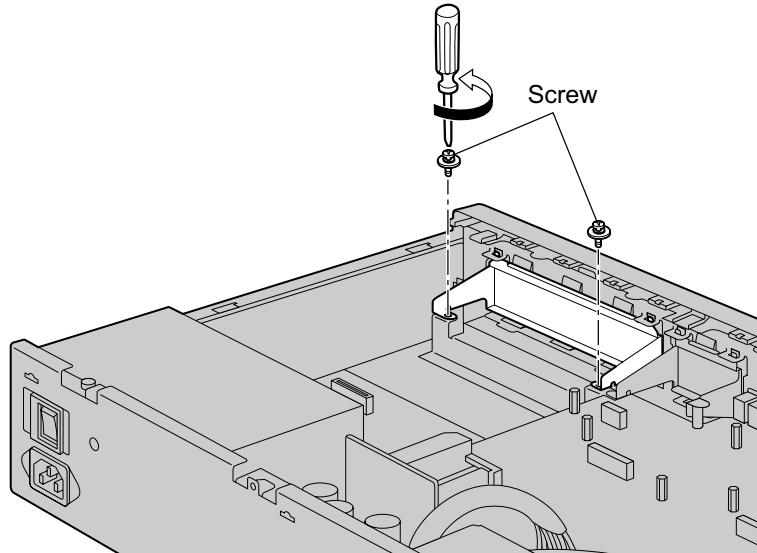
2. Holding the rear end of the card, pull the card in the direction of the arrows.



Installing an Optional Service Card in the Free Slot

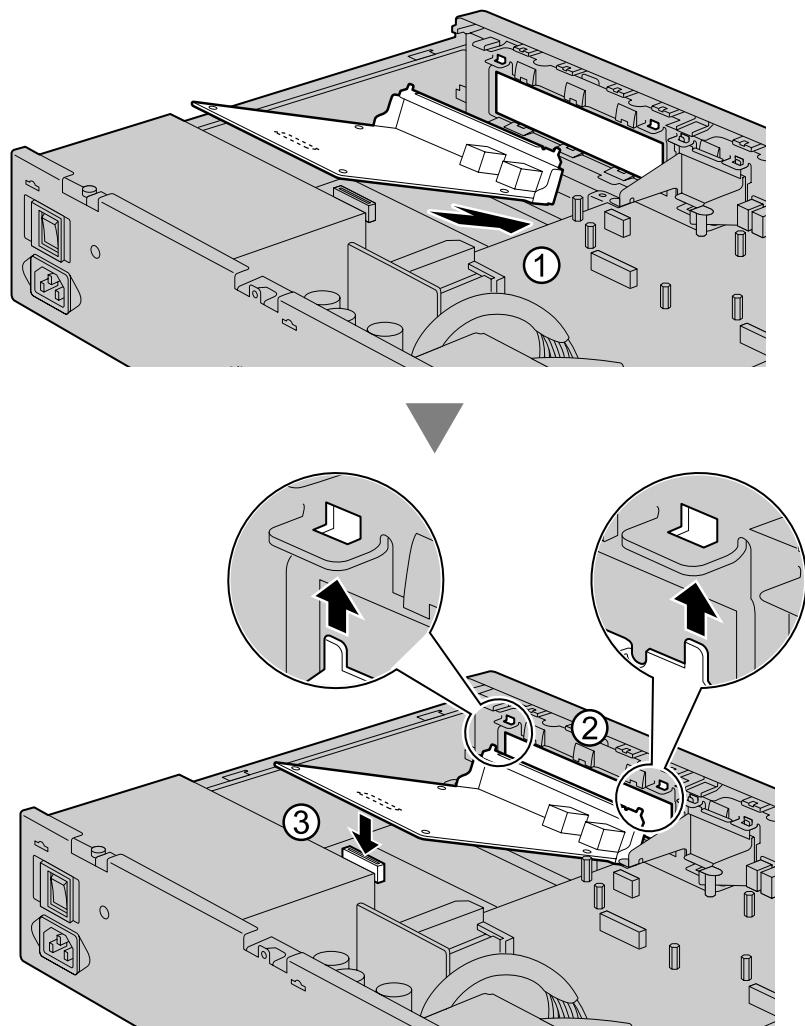
In the PBX's Free slot, you can install one of the following cards: SLC2/LCOT2, SLC2/BRI4, SLC2/PRI30, SLC2/PRI23, STACK-M. Some of the optional service cards require DIP switch settings which must be done before installing the card. For details, refer to the description of each optional service card in "4.5 Physical Trunk and Extension Cards", "4.6.1 STACK-M Card (KX-NS0130)", and "4.7 The Doorphone Card".

1. Remove the front cover plate for the Free slot.

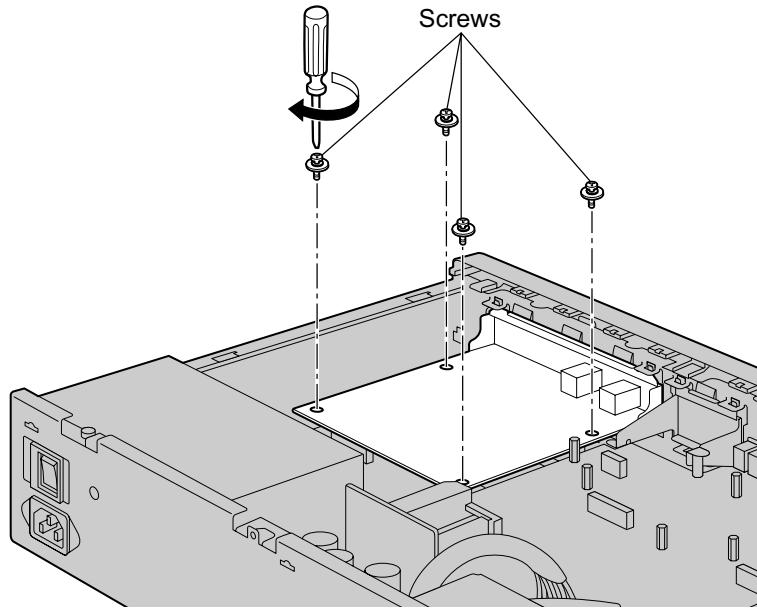


4.2.5 Installing/Removing the Optional Service Cards

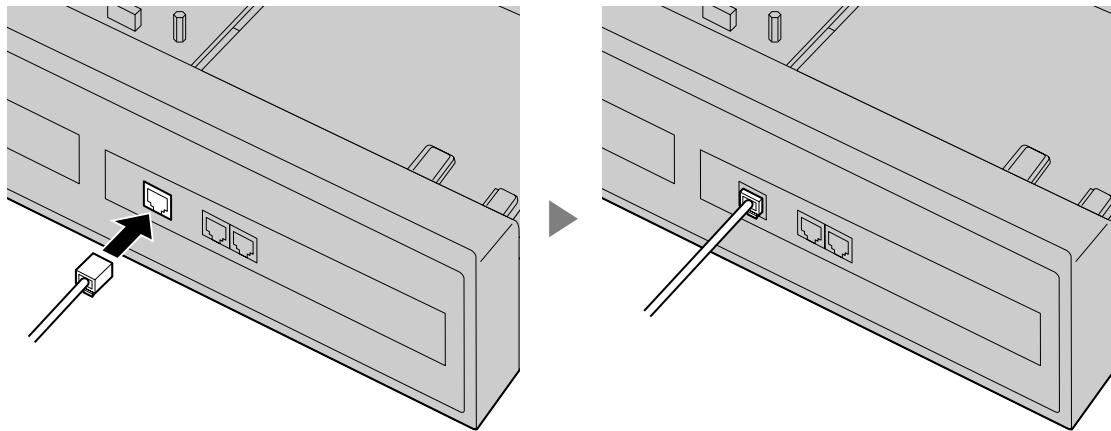
2. Position the card in the open slot, making sure that the tabs on the both sides of the card fit into place. Then, holding the card firmly in place, lower the rear end so that the holes of the card are aligned with the screw holes.



3. Insert the screws into the holes on the card, and tighten the screws to secure the card.



4. Connect cables to appropriate ports of the card. For details about pin assignments, refer to the appropriate section in "4.5 Physical Trunk and Extension Cards".

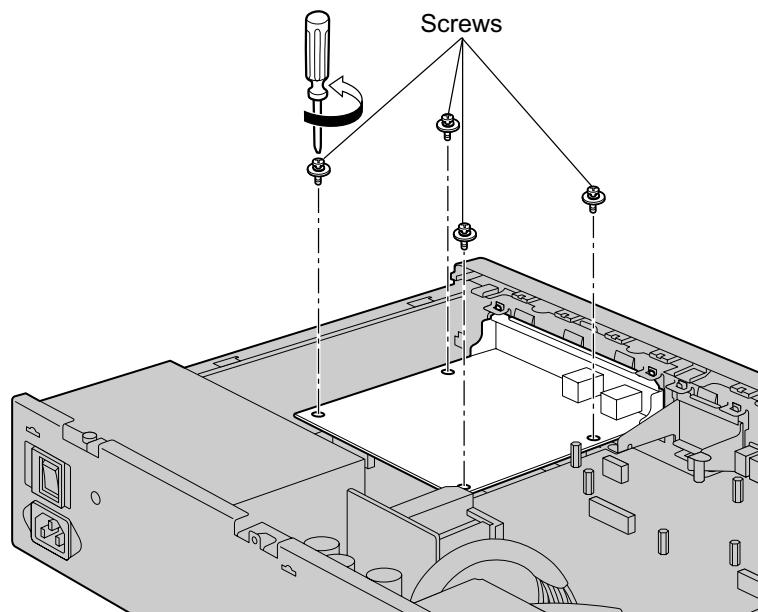


Note

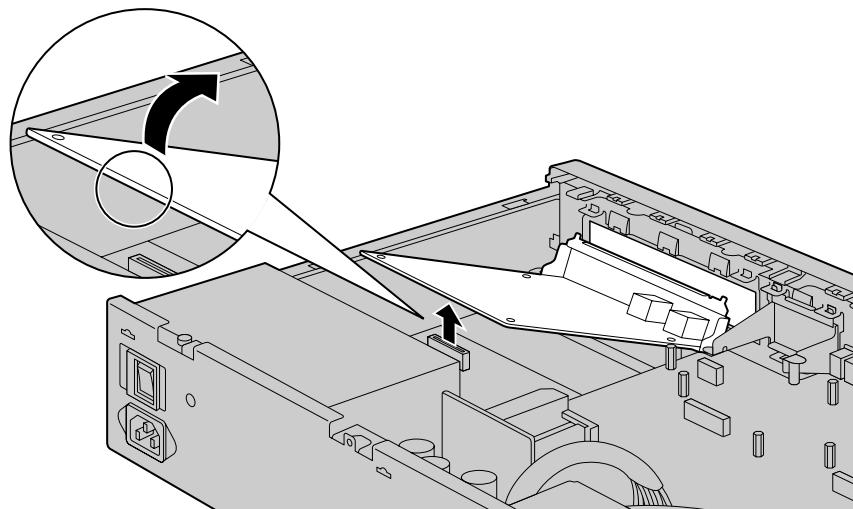
Make sure to connect cables after installing the card in the PBX, not before.

Removing Optional Service Card from the Free Slot

1. Loosen and remove the screws.

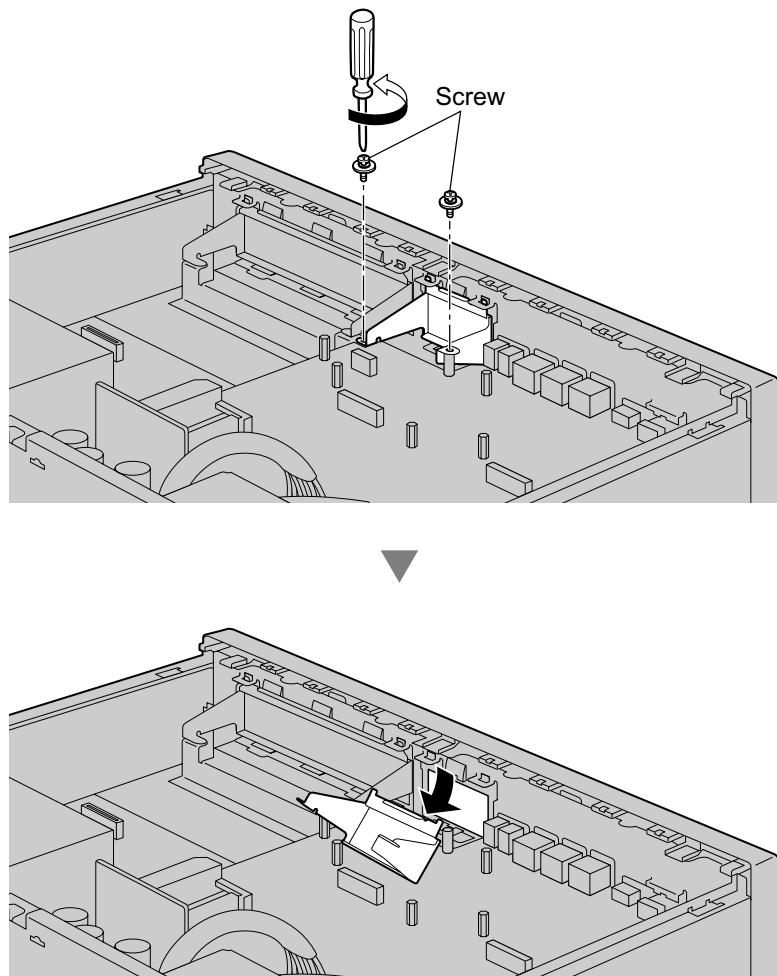


2. Holding the rear end of the card, pull the card in the direction of the arrows.



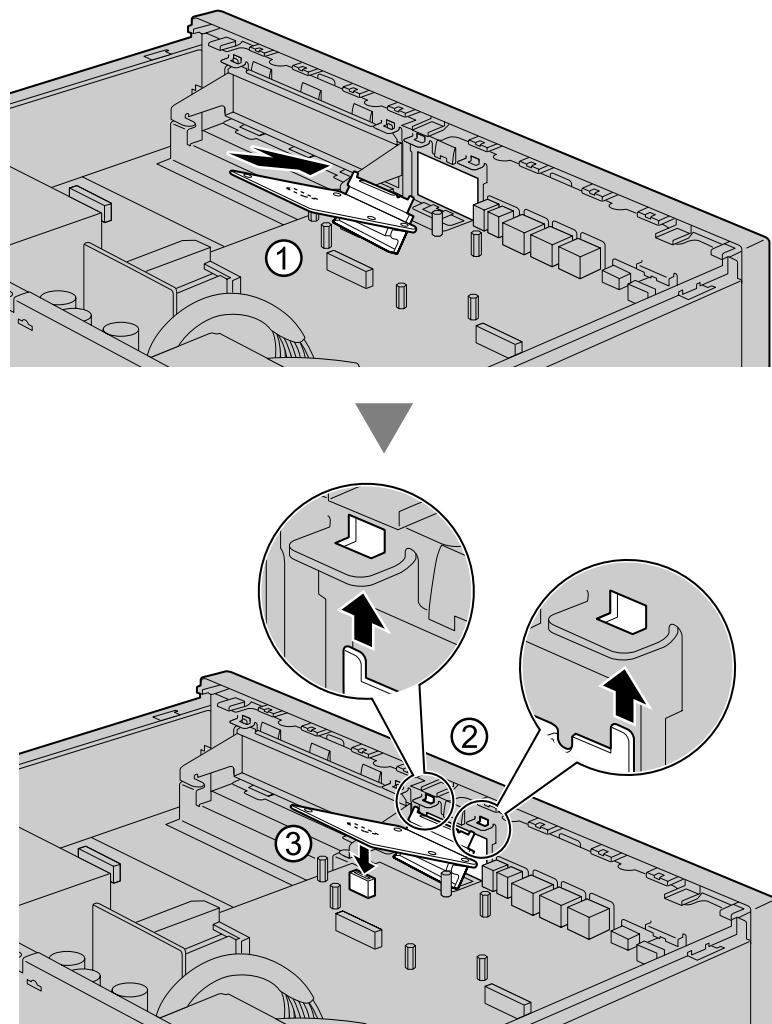
Installing the DOORPHONE Card in the Doorphone Slot

1. Remove the front cover plate for the Doorphone Slot.

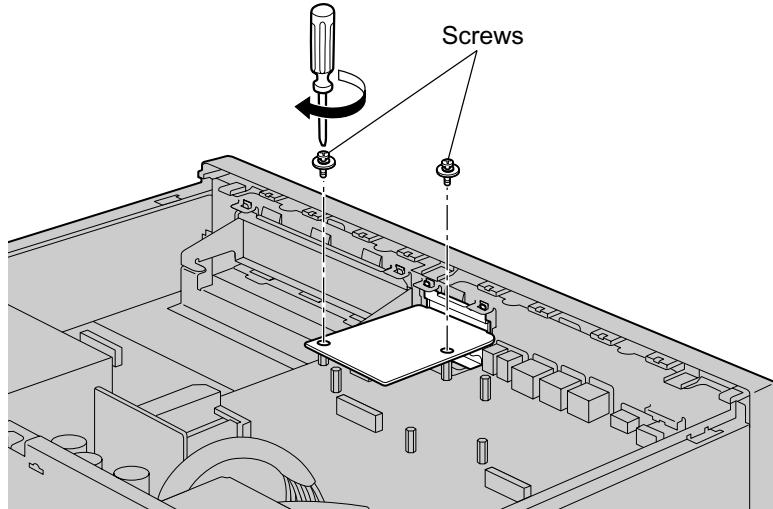


4.2.5 Installing/Removing the Optional Service Cards

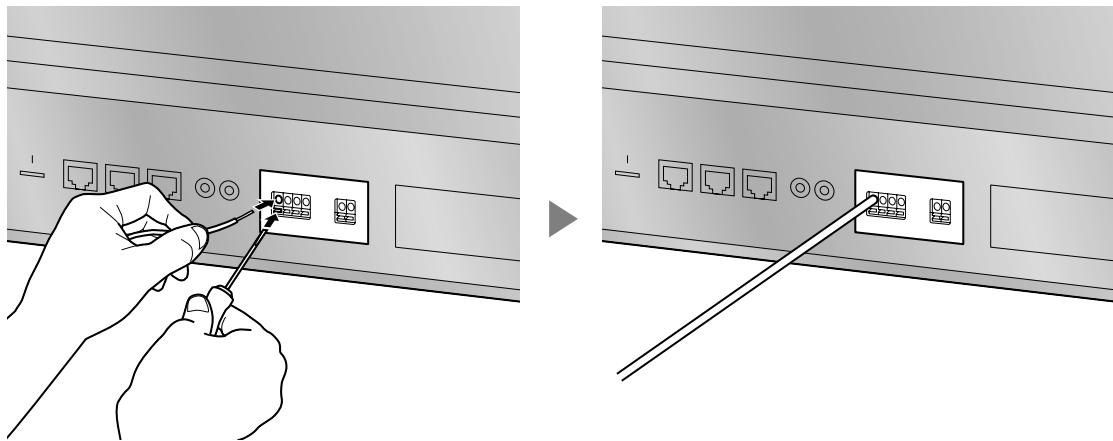
2. Position the card in the open slot, making sure that the tabs on the both sides of the card fit into place. Then, holding the card firmly in place, lower the rear end so that the holes of the card are aligned with the screw holes.



3. Insert the screws into the holes on the card, and tighten the screws to secure the card.



4. Connect cables to appropriate ports of the card. For details about pin assignments, refer to "4.7.1 DOORPHONE Card (KX-NS0161)" and "4.9 Connecting to a Doorphone, Door Opener, and/or External Sensor".

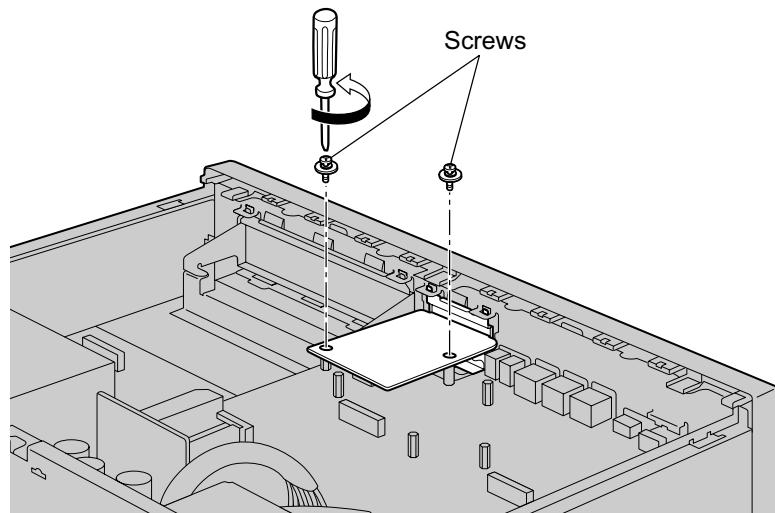


Note

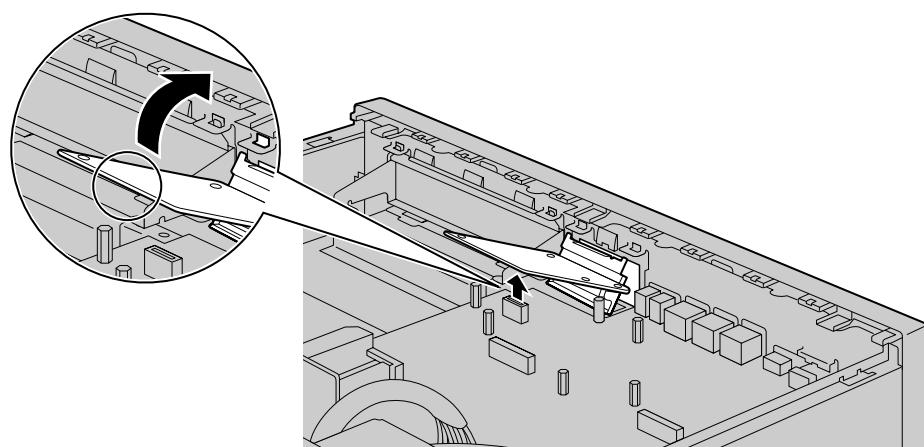
Make sure to connect cables after installing the card in the PBX, not before.

Removing the DOORPHONE Card from the Doorphone Slot

1. Loosen and remove the screws.



2. Holding the rear end of the card, pull the card in the direction of the arrows.



4.2.6 Installing/Removing the Storage Memory Card

Before Removing the Storage Memory Card

When removing the Storage Memory Card after the PBX has been in use, make a backup of the running system data so the current data can be restored after installing a new Storage Memory Card. For details about making backup files, refer to "7.2.2 Utility—File—File Transfer PBX to PC" in the PC Programming Manual.

Backup files cannot be made for some data. For details about which data is not backed up, refer to "Saving Modified Data" in the PC Programming Manual. For details about restoring Unified Message data from a backup, refer to "6.10 Tool—UM Data Restore" in the PC Programming Manual.

When you want to back up Unified Messaging system data, a separate backup procedure is required. For details about backing up Unified Messaging data, refer to "6.9 Tool—UM Data Backup" in the PC Programming Manual.

Upgrading from the Initially Installed Storage Memory Card

To increase Voice Mail recording time, you can install an optional Storage Memory Card.

For details about optional Storage Memory Cards, refer to "4.3.2 Storage Memory Card (installed by default), Storage Memory S Card (KX-NS0135), Storage Memory M Card (KX-NS0136), Storage Memory L Card (KX-NS0137)".

System Prompts

The Storage Memory Card (installed by default) and optional Storage Memory Cards contain system prompts for Unified Messaging. However, system prompts language data stored in the Storage Memory Card (installed by default) differ from those found in the optional Storage Memory Cards.

For information about the system prompt languages in each Storage Memory Card, refer to "9.2 System Prompt Languages".

The system prompt language data you are using on the initially installed Storage Memory Card must be backed up if you want to continue using that Storage Memory Card's system prompt language data. After backing up the system prompt language data, install the optional Storage Memory Card, and then restore the backed up system prompt language data to the new Storage Memory Card.

This procedure is described below.

Notice

If this is the first time the KX-NS1000 is being started, complete the Easy Setup Wizard before performing the following procedure. For details about Easy Setup Wizard, refer to "5.4.1 Easy Setup Wizard".

1. Insert a USB memory device into the USB port of the PBX.
(For details, refer to "Using a USB memory device" in "4.10 Connection of Peripherals".)
2. Back up the desired system prompts to the USB memory device.
(For details, refer to "6.9 Tool—UM Data Backup" in the PC Programming Manual.)
3. Shut down the PBX, and then turn the power switch off.
(For details about shutting down the PBX, refer to "5.5 System Control—System Shutdown" in the PC Programming Manual.)
4. Remove the Storage Memory Card (installed by default), and then install an optional Storage Memory Card.
(For details, refer to "4.3.2 Storage Memory Card (installed by default), Storage Memory S Card (KX-NS0135), Storage Memory M Card (KX-NS0136), Storage Memory L Card (KX-NS0137)".)
5. Start the PBX as described in "System Initialisation Procedure" in "4.13 Starting the KX-NS1000".
6. Perform Easy Setup Wizard.
(For details, refer to "5.4.1 Easy Setup Wizard".)
7. Restore the system prompts backed up in step 2. For details, refer to "6.10 Tool—UM Data Restore" in the PC Programming Manual.

Installing/Removing the Storage Memory Card

CAUTION

- Before touching the product (PBX, cards, etc.), discharge static electricity by touching ground or wearing an earthing strap. Failure to do so may cause the PBX to malfunction due to static electricity.
- When installing or removing the Storage Memory Card, the power switch must be turned off.
- When installing or removing the Storage Memory Card, do not put pressure on any parts of the mother board. Doing so may result in damage to the PBX.
- The Storage Memory Card contains software for all the processes of the PBX and all the customer data. Therefore, do not allow unauthorised access to prevent data leakage.
- To prevent data leakage, render the Storage Memory Card physically unusable before disposal.

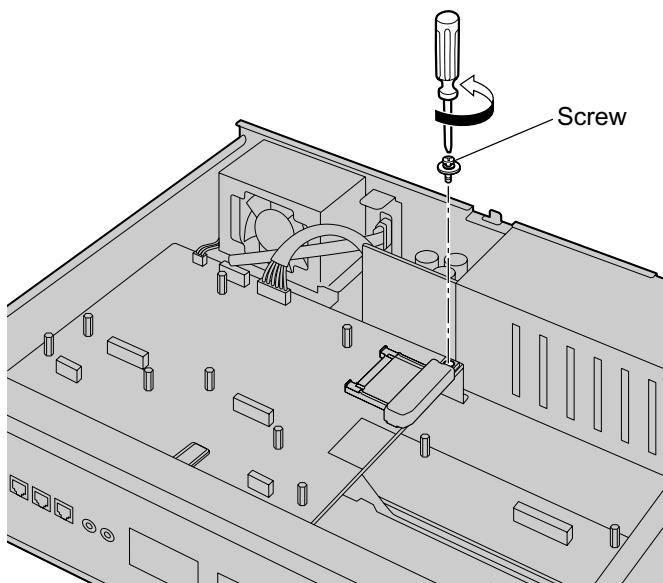
Notice

- Use only the Storage Memory Card included with the PBX, or a Panasonic optional upgrade Storage Memory Card.
- The Storage Memory Card must be inserted in the Storage Memory Card slot of the mother board before startup.

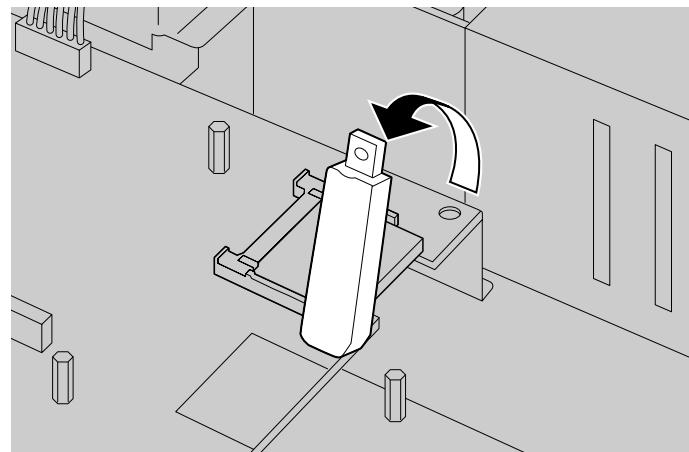
Note

- The ▲ is shown on the label of your Storage Memory Card to indicate the direction for inserting the Storage Memory Card.
- The maximum length of file names for files that are to be stored in the Storage Memory Card is 60 characters.

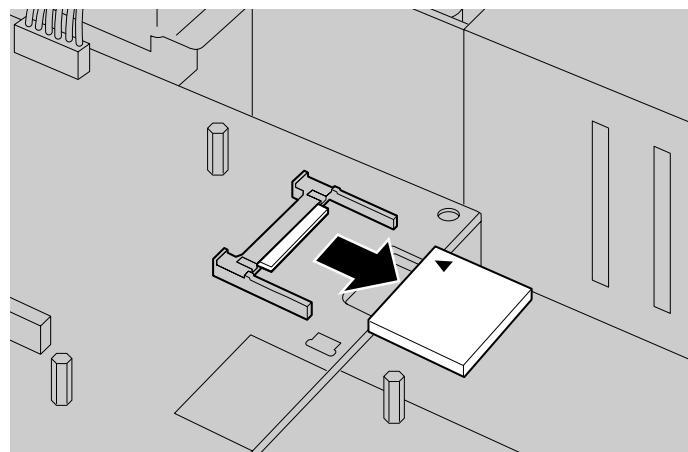
1. Turn the screw anticlockwise to loosen.



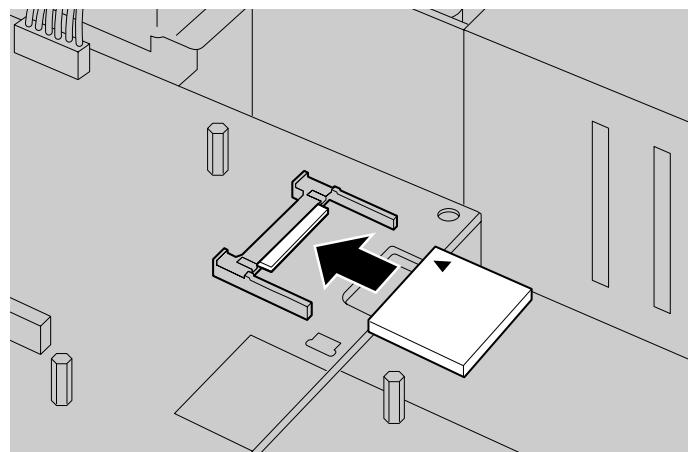
2. Remove the Storage Memory Card slot cover.



3. Remove the Storage Memory Card installed in the slot on the mother board.

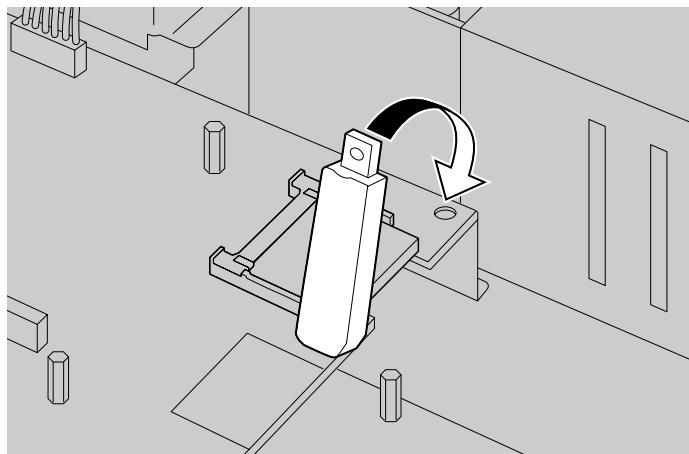


4. Insert the new Storage Memory Card into the slot on the mother board.

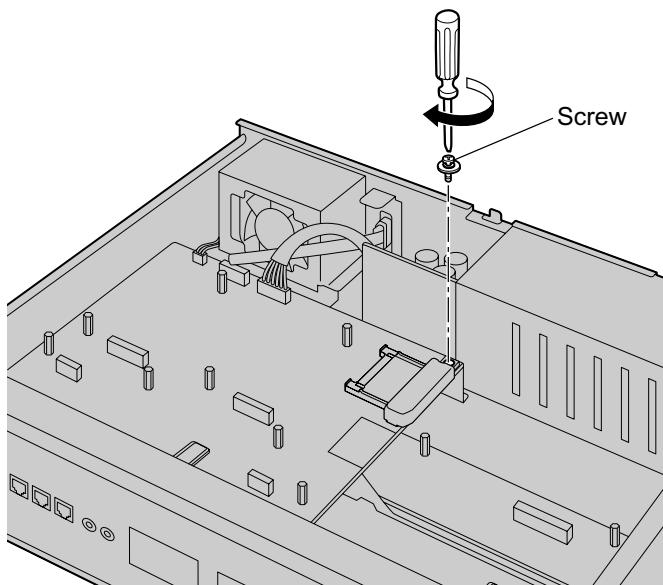


4.2.6 Installing/Removing the Storage Memory Card

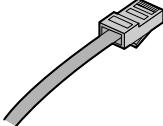
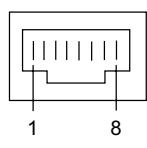
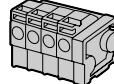
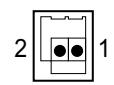
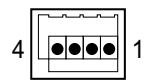
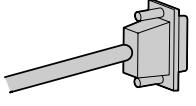
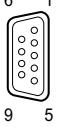
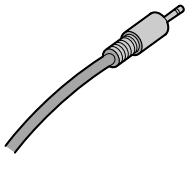
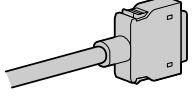
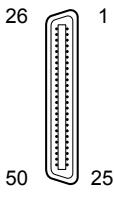
5. Place the cover as shown below.



6. Turn the screw clockwise to tighten.



4.2.7 Types of Connectors

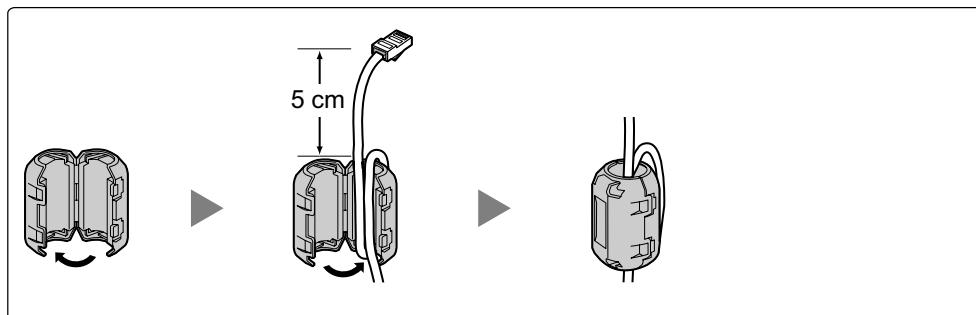
Connector Type	Pin Number	Used for
RJ45  (Twisted pair cable)	 1 8	<ul style="list-style-type: none"> • Mother board • SLC2/LCOT2 (KX-NS0180) • SLC2/BRI4 (KX-NS0280) • SLC2/PRI30 (KX-NS0290CE) • SLC2/PRI23 (KX-NS0290)
4-pin Terminal Block 2-pin Terminal Block  	 2 1  4 1	<ul style="list-style-type: none"> • DOORPHONE (KX-NS0161)
RS-232C  (Shielded cable)	 6 1 9 5	<ul style="list-style-type: none"> • Main Unit
Mini Plug 	 2 4	<ul style="list-style-type: none"> • Mother board
Stacking Connector 	 26 1 50 25	<ul style="list-style-type: none"> • STACK-M (KX-NS0130) • STACK-S (NCP) (KX-NS0131) • STACK-S (TDE) (KX-NS0132)

4.2.8 Attaching a Ferrite Core

A ferrite core must be attached when an RJ45 connector is connected to the SLC2/PRI30, SLC2/PRI23 or SLC2/BRI4 card.

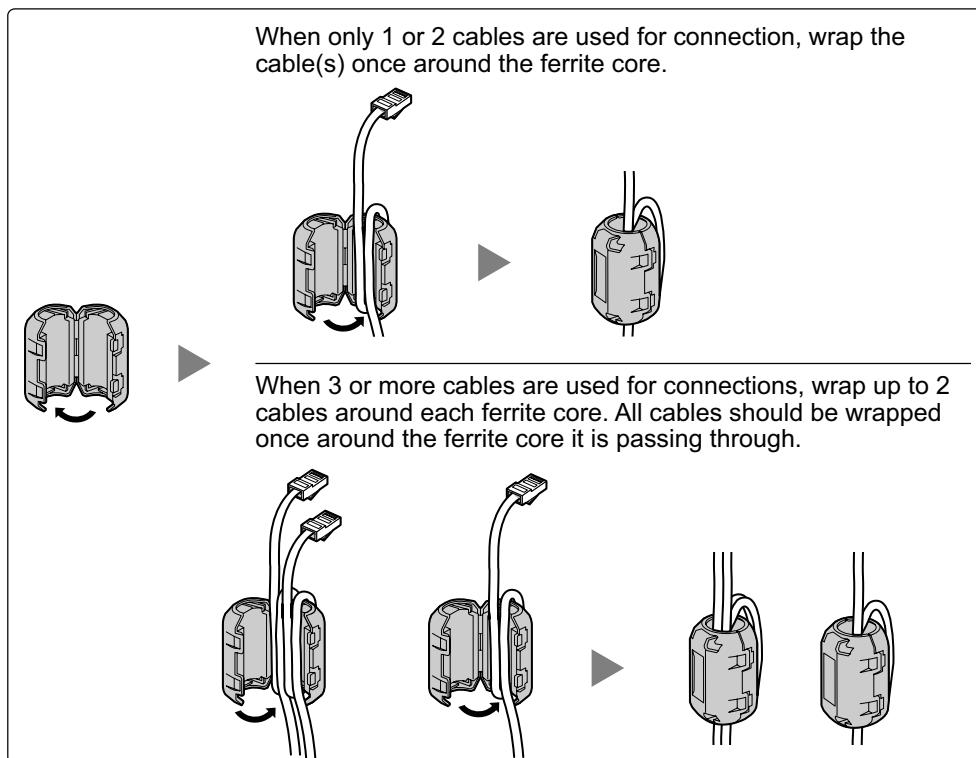
For the SLC2/PRI23 and SLC2/PRI30 Cards

For the cable to connect to the ISDN Primary Rate Interface port, wrap the cable once around the ferrite core, then close the case of the ferrite core. Attach the ferrite core 5 cm away from the connector. The ferrite core is included with the card.



For the SLC2/BRI4 Card

For the cables to connect to the ISDN Basic Rate Interface ports, attach the ferrite cores, then close the cases of the ferrite cores. Attach the ferrite cores as close to the card's connectors as possible. The ferrite cores are included with the card.



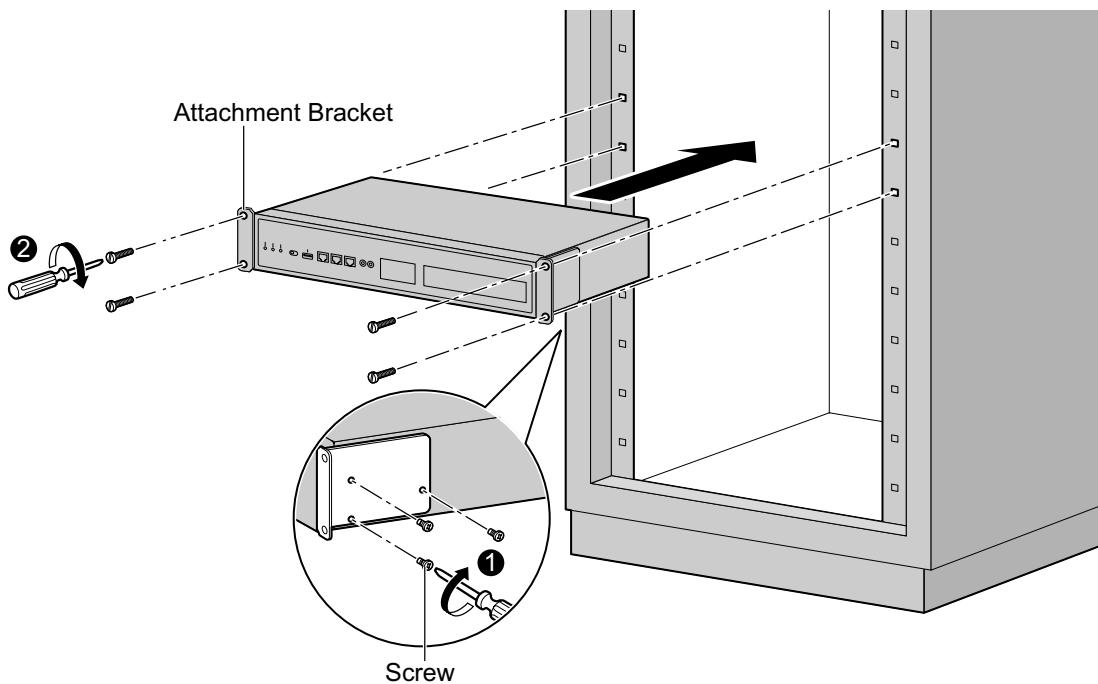
4.2.9 19-inch Rack Mounting

WARNING

- Be careful not to drop any components. Dropping components may damage them or cause an injury.
- When mounting the PBX on a 19-inch rack, only use the 19-inch rack mounting equipment (attachment bracket, screws) included with the PBX.

CAUTION

- When the PBX is mounted on a 19-inch rack, make sure that the installation of the unit does not cause the temperature of the rack to exceed its limit.
 - When the PBX is mounted on a 19-inch rack, do not block the openings of the PBX. Allow space of at least 10 cm around the PBX's fan.
 - If the PBX is not installed properly using the securing correct methods, the PBX may fall causing serious damage.
 - When this product is no longer in use, make sure to detach it from the rack.
1. Fix the attachment brackets to the left and right sides of the PBX with 3 screws on each side. (Recommended torque: 0.8 N·m [8.2 kgf·cm] to 1.0 N·m [10.2 kgf·cm]) → ①
 2. Place the PBX in the 19-inch rack and fix both attachment brackets to the rack with the rack's proprietary mounting equipment. → ②



4.2.10 Placing the PBX on a Desktop

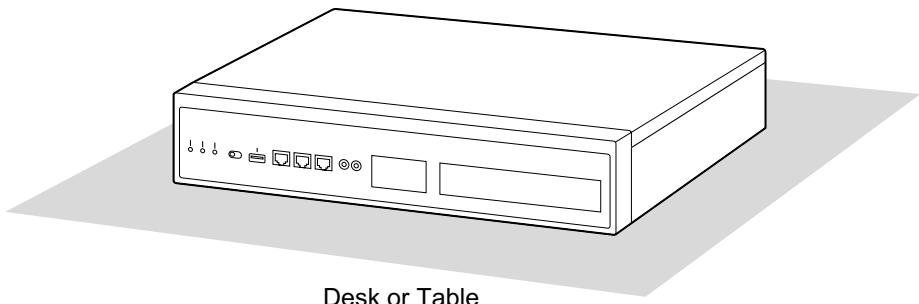
When placing the PBX on a desktop, make sure to follow these instructions.

WARNING

Be careful not to drop any components. Dropping components may damage them or cause an injury.

CAUTION

- When the PBX is placed on a desktop, make sure that the PBX is placed as indicated in the diagram below. Do not place it on its side or upside down.
- Do not block the openings of the PBX. Allow space of at least 20 cm above and 10 cm at the sides of the PBX.
- Make sure that the surface behind the PBX is not made of wood.



4.2.11 Wall Mounting

The PBX can be mounted on a concrete wall using the optional wall mounting kit.

WARNING

- Make sure that the wall that the unit will be attached to is strong enough to support the unit (approx. 35 kg). If not, it is necessary for the wall to be reinforced.
- Only use the wall-mounting equipment (anchor plugs, screws, metal brackets) included with the PBX and the wall mounting kit. Make sure that the wall is made of concrete.
- Be careful not to drop any components. Dropping components may damage them or cause an injury.
- Proper earthing (connection to earth) is very important to reduce the risk to the user of electrocution or to protect the PBX from the bad effects of external noise in the case of a lightning strike. (See "4.2.4 Frame Earth Connection".)

CAUTION

- Make sure to install all necessary optional service cards in the PBX before performing the wall mounting procedure. If it is necessary to install or remove a card, make sure to detach the PBX from the wall before installing or removing the card.
- Do not block the openings of the PBX. Allow space of at least 20 cm above and 10 cm at the sides of the PBX.
- Make sure that the surface behind the PBX is flat and free of obstacles, so that the openings on the back of the PBX will not be blocked.
- Make sure that the surface behind the PBX is not made of wood.
- If the PBX is not installed properly using the securing correct methods, the PBX may fall causing serious damage.
- When placing the PBX onto the wall, make sure that the arrows on the metal brackets are pointing upward. If the arrows are not pointing upward, the PBX may fall, resulting in injury.
- When driving the screws into the wall, be careful to avoid touching any metal laths, wire laths or plates in the wall.
- When this product is no longer in use, make sure to detach it from the wall.

Note

For details about dimensions and weight of the PBX, see "2.3.1 General Description".

Necessary Items

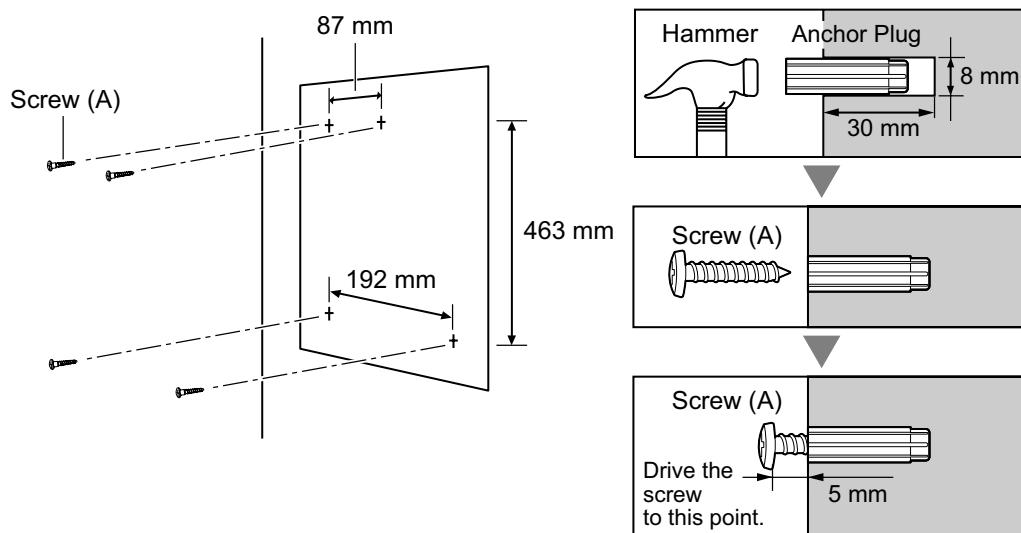
Included in the PBX		
Screw B		6
Included in the wall mounting kit (KX-A247)		
Top Bracket		1
Bottom Bracket		1
Anchor Plug (For use in concrete)		4
Screw A (For use in concrete)		4

4.2.11 Wall Mounting

Wall Mounting Procedures

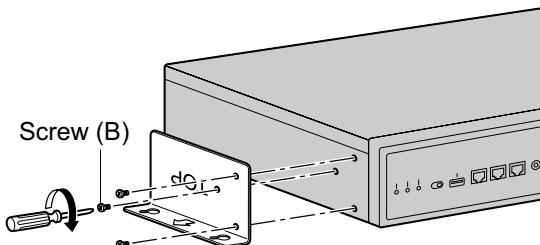
1. Measure the actual space as indicated below to mark the 4 screw positions on the wall. Install 4 anchor plugs in the wall and drive in 4 screws (A) leaving a gap of 5 mm between the screw head and the wall.

Installation procedure for concrete walls.

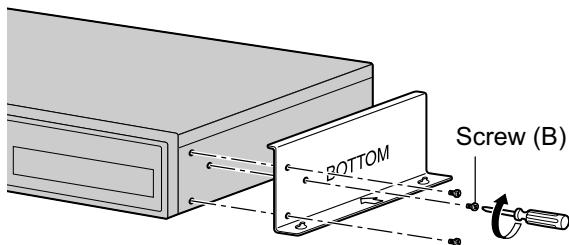


Note

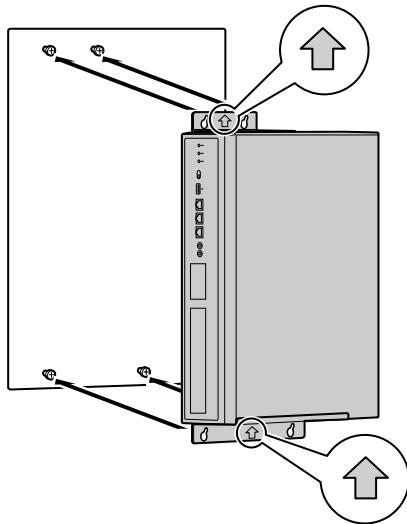
- As indicated above, do not tighten the screws fully. You will tighten the screws in step 6.
 - The pull-out strength of the installation area must be at least 294 N (30 kgf) per screw.
2. Fix the Top Bracket to the left side of the PBX with 3 screws (B). (Recommended torque: 0.8 N·m [8.2 kgf·cm] to 1.0 N·m [10.2 kgf·cm])



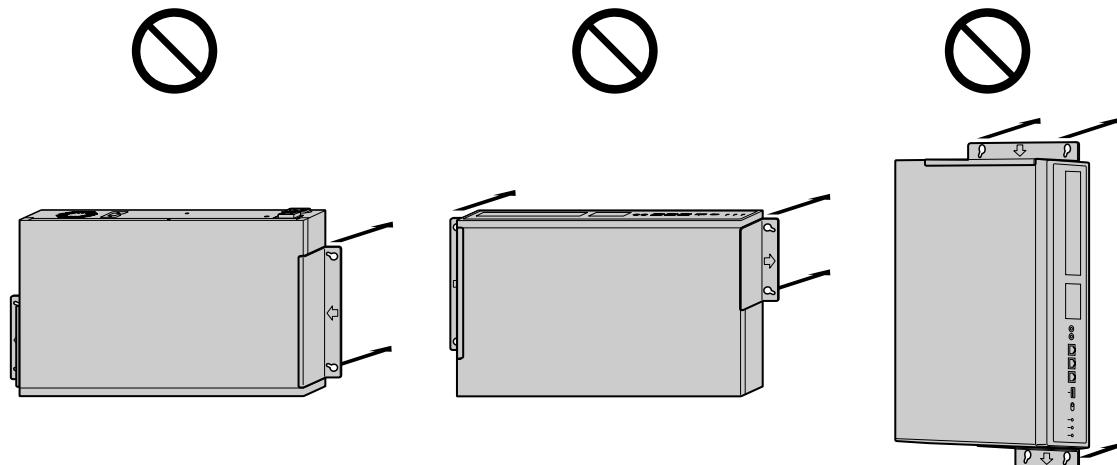
3. Fix the Bottom Bracket to the right side of the PBX with 3 screws (B). (Recommended torque: 0.8 N·m [8.2 kgf·cm] to 1.0 N·m [10.2 kgf·cm])



4. Place the PBX onto the wall, making sure that the guide holes hook onto the screw heads.

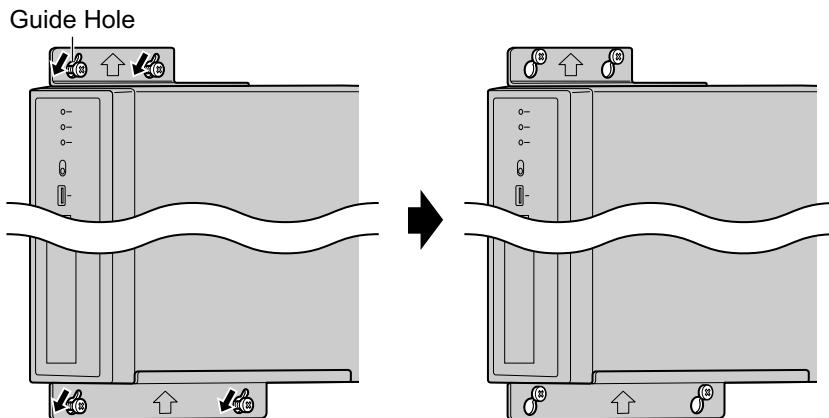
**CAUTION**

When placing the PBX onto the wall, make sure that the arrows on the metal brackets are pointing upward. If the arrows are not pointing upward, the PBX may fall, resulting in injury. The following illustrations are bad examples of wall mounting.

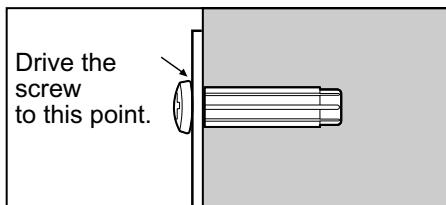


4.2.11 Wall Mounting

5. Slide the PBX down into the guide holes.



6. Fully tighten all 4 screws (A).



4.2.12 Surge Protector Installation

CAUTION

Performing surge protection is essential. Make sure to follow the instructions in this section.

Overview

A massive electrical surge can be caused if lightning strikes a telephone cable 10 m above ground, or if a telephone line comes into contact with a power line. A surge protector is a device that is connected to a trunk to prevent potentially dangerous electrical surges from entering the building via the trunk and damaging the PBX and connected equipment.

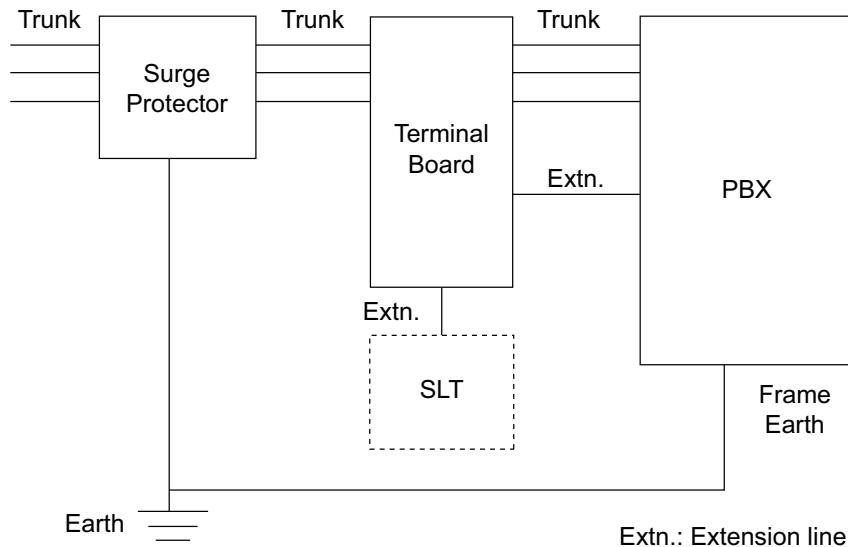
To protect the system from electrical surges, we strongly recommend connecting the system to a surge protector that meets the following specifications:

- Surge arrestor type: 3-electrode arrestor
- DC spark-over voltage: 230 V
- Maximum peak current: at least 10 kA

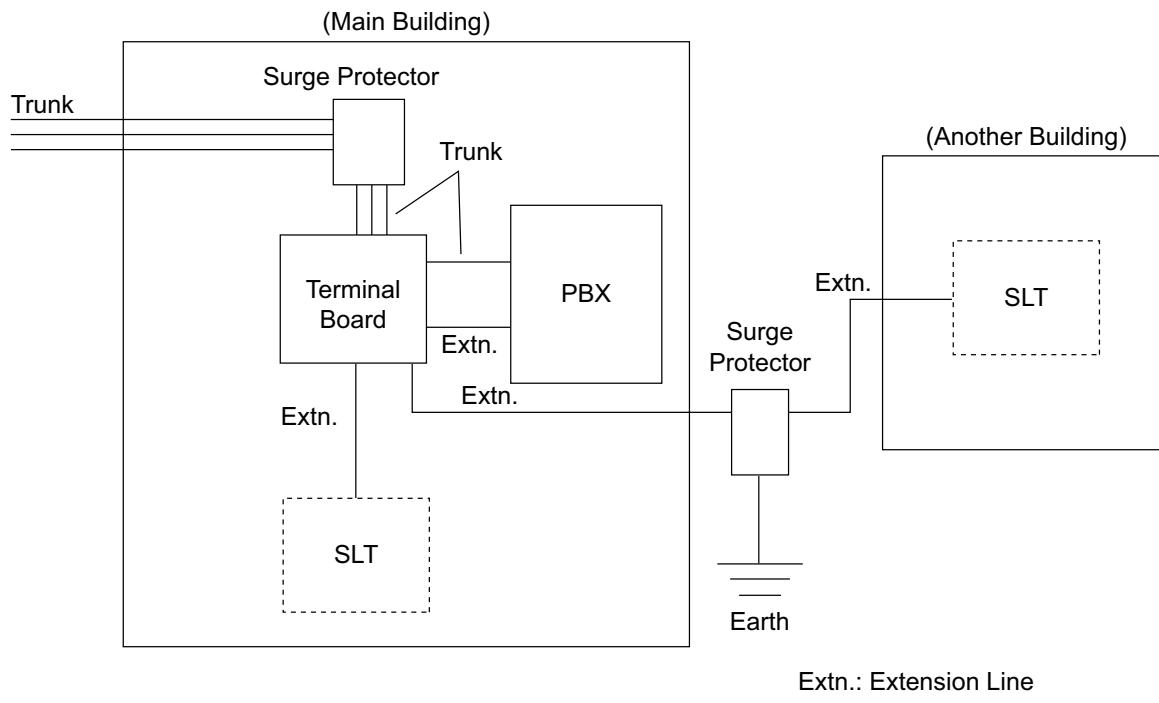
Additionally, proper earthing is very important for the protection of the system (refer to "4.2.4 Frame Earth Connection").

Many countries/areas have regulations requiring surge protection. Be sure to comply with all applicable laws, regulations, and guidelines.

Installation



Outside Installation



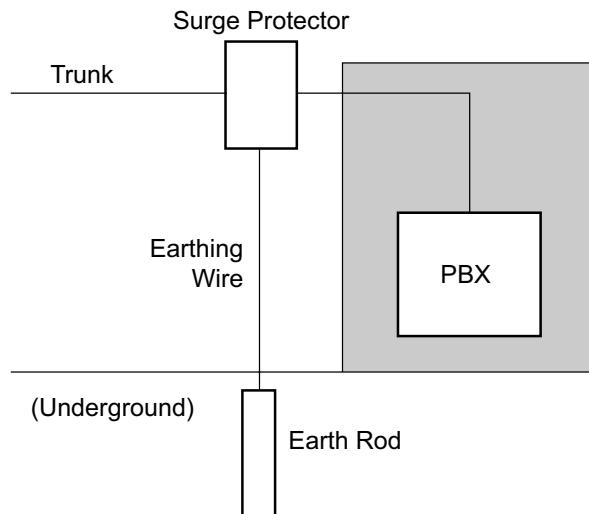
If you install an extension outside of the building, the following precautions are recommended:

- Install the extension wire underground.
- Use a conduit to protect the wire.

Note

The surge protector for an extension is different from that for trunks.

Installation of an Earth Rod



1. Connect the earth rod to the surge protector using an earthing wire with a cross-sectional area of at least 1.3 mm².
2. Bury the earth rod near the protector. The earthing wire should be as short as possible.
3. The earthing wire should run straight to the earth rod. Do not run the wire around other objects.
4. Bury the earth rod at least 50 cm underground.

Note

- The above figures are recommendations only.
- The length of earth rod and the required depth depend on the composition of the soil.

4.3 The Mother Board and Expansion Cards

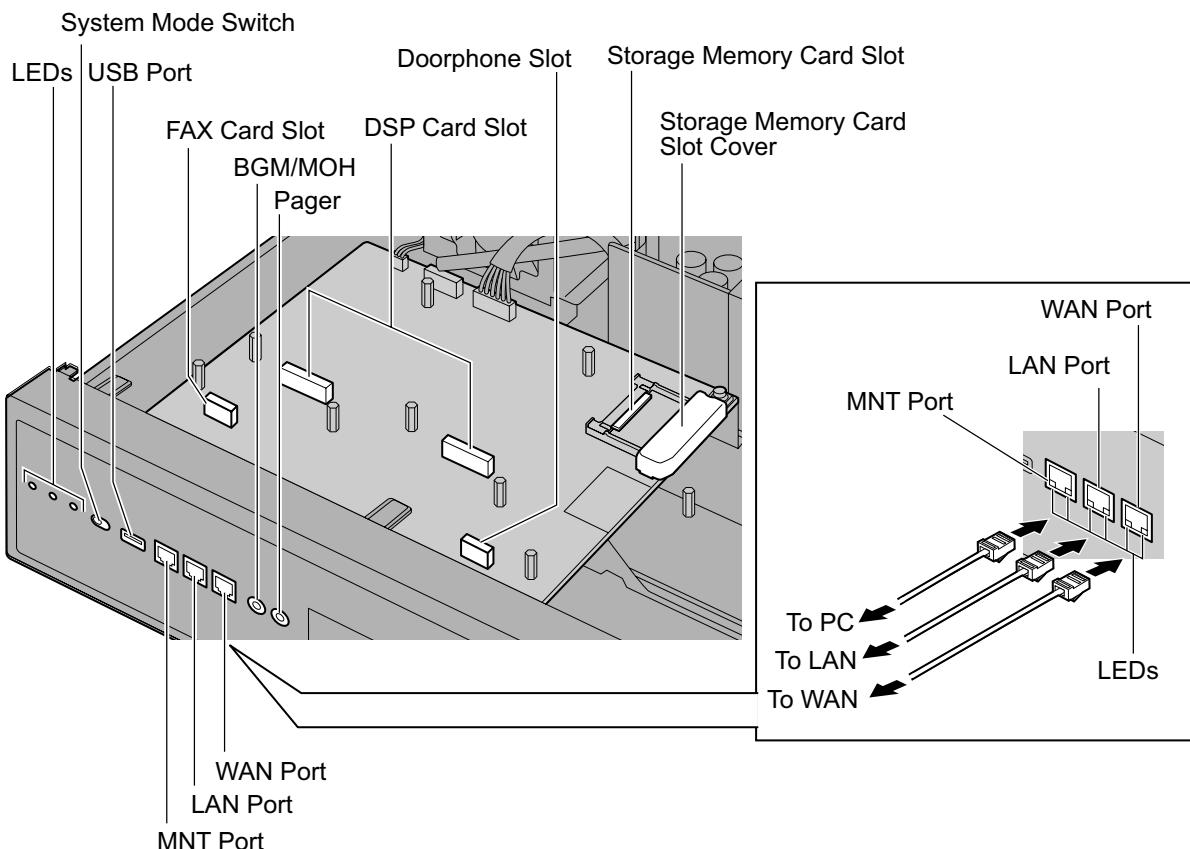
4.3.1 Mother Board

Function

The mother board is the preinstalled processing board with activation keys for CA Basic-Express for 1022 users, use of 8 IP-PT, and 2 Unified Messaging ports. The Virtual Cards (trunk/extension) can be installed in Virtual Slots of the mother board and can be activated with the activation keys. Also, the mother board supports LAN connection so that IP telephones (IP-PTs, IP softphones, SIP phones) and PCs can be connected on a private IP network.

Mountable Cards

- Two of the DSP S, DSP M, or DSP L cards (refer to "4.3.3 DSP S Card (KX-NS0110), DSP M Card (KX-NS0111), DSP L Card (KX-NS0112)")
- Storage Memory Card (refer to "4.3.2 Storage Memory Card (installed by default), Storage Memory S Card (KX-NS0135), Storage Memory M Card (KX-NS0136), Storage Memory L Card (KX-NS0137)")
- FAX card (refer to "4.3.4 FAX Card (KX-NS0106)")
- DOORPHONE card (refer to "4.7.1 DOORPHONE Card (KX-NS0161)")



Note

- Make sure to use the MNT port for PC connection, and the LAN port for LAN connection.

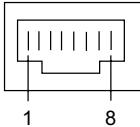
- The maximum length of the CAT 5/CAT 5e cables to be connected to the mother board is 100 m.
- For installing and removing the Storage Memory Card, refer to "4.2.6 Installing/Removing the Storage Memory Card".
- For details about Virtual Slots, refer to "2.3.3 System Capacity".
- If the preinstalled activation keys on the mother board are not enough for the desired configuration, you need to purchase activation key codes. For details about the activation keys, refer to "3.1 Information about the Activation Keys".
- For details about connecting to a LAN, refer to "4.11 LAN Connection".
- For details about connecting peripherals, refer to "4.10 Connection of Peripherals".
- For details about System Mode Switch, refer to "4.13 Starting the KX-NS1000".

WARNING

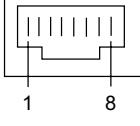
A lithium battery is used in the mother board. There is a risk of explosion if the battery is replaced with the incorrect type. Dispose of used batteries according to the manufacturer's instructions.

Pin Assignments

MNT Port/LAN Port/WAN Port (10BASE-T/100BASE-TX)

	No.	Signal Name	Input (I)/Output (O)	Function
	1	TPO+	O	Transmit data+
	2	TPO-	O	Transmit data-
	3	TPI+	I	Receive data+
	4-5	Reserved	—	—
	6	TPI-	I	Receive data-
	7-8	Reserved	—	—

MNT Port/LAN Port/WAN Port (1000BASE-T)

	No.	Signal Name	Input (I)/Output (O)	Function
	1	TRD0 (+)	I/O	Transmit and receive data 0 (+)
	2	TRD0 (-)	I/O	Transmit and receive data 0 (-)
	3	TRD1 (+)	I/O	Transmit and receive data 1 (+)
	4	TRD2 (+)	I/O	Transmit and receive data 2 (+)
	5	TRD2 (-)	I/O	Transmit and receive data 2 (-)
	6	TRD1 (-)	I/O	Transmit and receive data 1 (-)
	7	TRD3 (+)	I/O	Transmit and receive data 3 (+)
	8	TRD3 (-)	I/O	Transmit and receive data 3 (-)

LED Indications

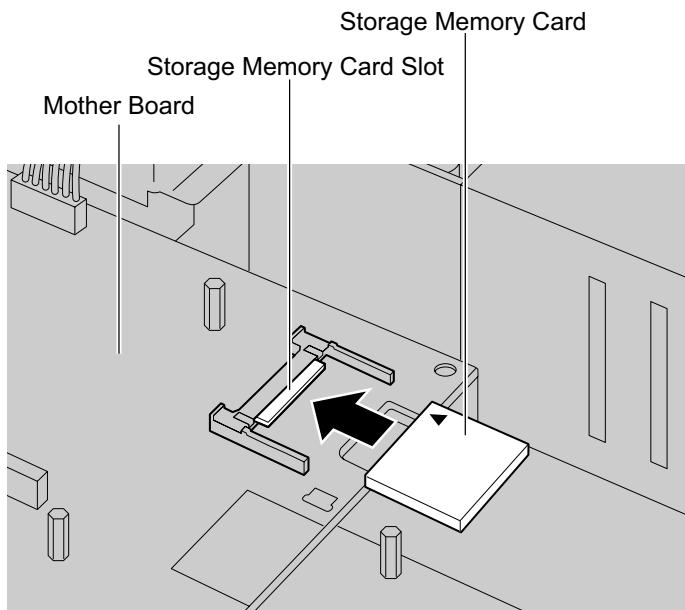
Indication	Colour	Description
STATUS	Green	PBX status indication <ul style="list-style-type: none"> OFF: Power Off ON: Power On and running Flashing: Starting up/Logging in
	Amber	PBX status indication <ul style="list-style-type: none"> ON: Ready to shutdown Flashing: Shutting down
	Red	PBX status indication <ul style="list-style-type: none"> ON: Alarm The cause may be one of the following: <ul style="list-style-type: none"> Power was cut without performing the shutdown procedure. No IP address(es) assigned for the DSP card(s) by the DHCP server. Alarm for an optional service card. Flashing: Initialise failed
BATT ALARM	Red	Alarm indication <ul style="list-style-type: none"> OFF: Normal ON: Alarm
MASTER	Green	Master unit status indication <ul style="list-style-type: none"> ON: Master
		Slave unit status indication <ul style="list-style-type: none"> Flashing: Running as Backup Master unit
	Amber	Master unit status indication <ul style="list-style-type: none"> Flashing: Factory default
		Slave unit status indication <ul style="list-style-type: none"> ON: Slave Flashing: Factory default/Starting up
	Red	Master unit status indication <ul style="list-style-type: none"> ON: Recovered (Waiting to be switched with Backup Master unit)
		Slave unit status indication <ul style="list-style-type: none"> Flashing: Isolated from Master unit

Indication			Colour	Description
10BASE-T/ 100BASE-TX/ 1000BASE-T	MNT	LINK	Green	Link status indication <ul style="list-style-type: none"> OFF: Off-line ON: Linked normally Flashing: In communication
		1000	Green/ Yellow	Data transmission speed indication <ul style="list-style-type: none"> OFF: 10 Mbps Yellow ON: 100 Mbps Green ON: 1000 Mbps
	LAN	LINK	Green	Link status indication <ul style="list-style-type: none"> OFF: Off-line ON: Linked normally Flashing: In communication
		1000	Green/ Yellow	Data transmission speed indication <ul style="list-style-type: none"> OFF: 10 Mbps Yellow ON: 100 Mbps Green ON: 1000 Mbps
	WAN	LINK	Green	Link status indication <ul style="list-style-type: none"> OFF: Off-line ON: Linked normally Flashing: In communication
		1000	Green/ Yellow	Data transmission speed indication <ul style="list-style-type: none"> OFF: 10 Mbps Yellow ON: 100 Mbps Green ON: 1000 Mbps

4.3.2 Storage Memory Card (installed by default), Storage Memory S Card (KX-NS0135), Storage Memory M Card (KX-NS0136), Storage Memory L Card (KX-NS0137)

Function

Storage Memory Card (Installed by default):	Storage Memory with 2 hours Voice Mail recording time. To increase recording time to a maximum of 15 hours, activate REC Time Expansion (KX-NSU001) activation key.
Storage Memory S:	Storage Memory with maximum of 200 hours Voice Mail recording time.
Storage Memory M:	Storage Memory with maximum of 450 hours Voice Mail recording time.
Storage Memory L:	Storage Memory with maximum of 1000 hours Voice Mail recording time.



Accessories and User-supplied Items

Accessories (included): none

User-supplied (not included): none

Note

For installing and removing the Storage Memory Card, refer to "4.2.6 Installing/Removing the Storage Memory Card".

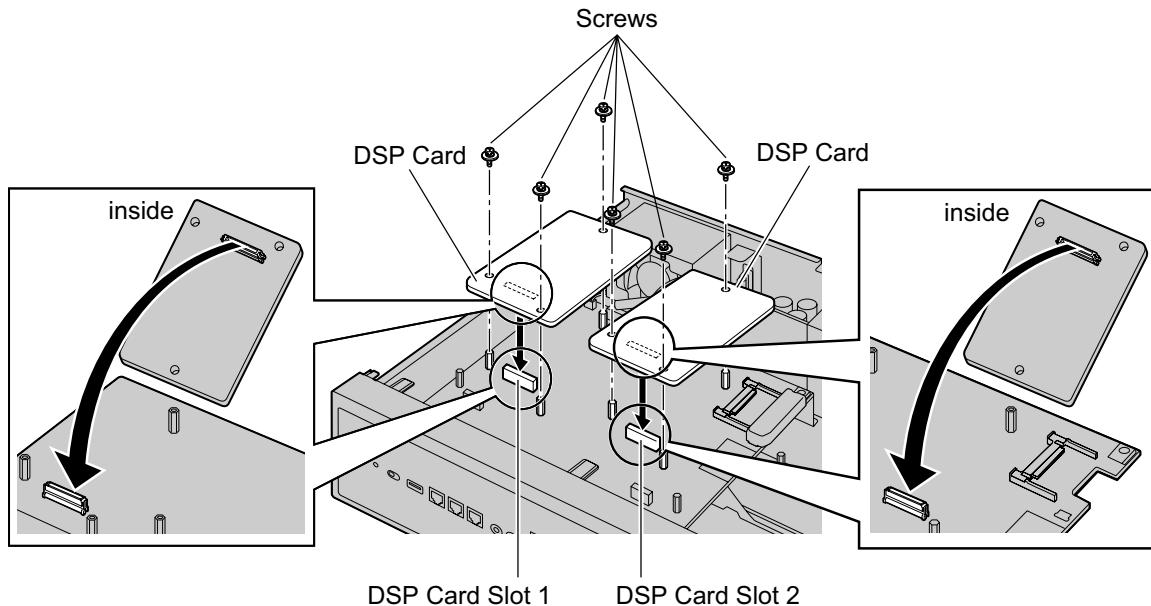
4.3.3 DSP S Card (KX-NS0110), DSP M Card (KX-NS0111), DSP L Card (KX-NS0112)

Function

A DSP card is a digital signal processor card with DSP resources that can be used for VoIP calls, conferences, the Unified Messaging feature, and the DISA/OGM feature. The DSP cards are compliant with ITU-T G.729A and G.711 codec methods.

Depending on the amount of your DSP resource needs, DSP S, DSP M, or DSP L cards can be installed. Up to 2 DSP cards can be installed on the mother board.

To operate the PBX, at least one DSP S, DSP M, or DSP L card must be installed in one of the DSP card slots.



Accessories and User-supplied Items

Accessories (included): Screws × 3

User-supplied (not included): none

CAUTION

When installing or removing the optional service cards, do not put pressure on any parts of the mother board. Doing so may result in damage to the PBX.

Note

The DSP Resource Advisor can be used to calculate DSP resource usage easily. For details, refer to "9.34.1.1 PBX Configuration—[1-5-1] Configuration—DSP Resource—Setting—DSP Resource Advisor" in the PC Programming Manual.

DSP Resource Information

The number of resources provided by each type of DSP card is as follows:

DSP Card Type	Number of Resources
DSP S	63

4.3.3 DSP S Card (KX-NS0110), DSP M Card (KX-NS0111), DSP L Card (KX-NS0112)

DSP Card Type	Number of Resources
DSP M	127
DSP L	254

IP Address Information

Either 1 or 2 IP addresses must be assigned to each DSP card, depending on the type of DSP card. You can assign IP addresses to the DSP cards during Easy Setup Wizard or through system programming.

For details about Easy Setup Wizard, refer to "5.4.1 Easy Setup Wizard".

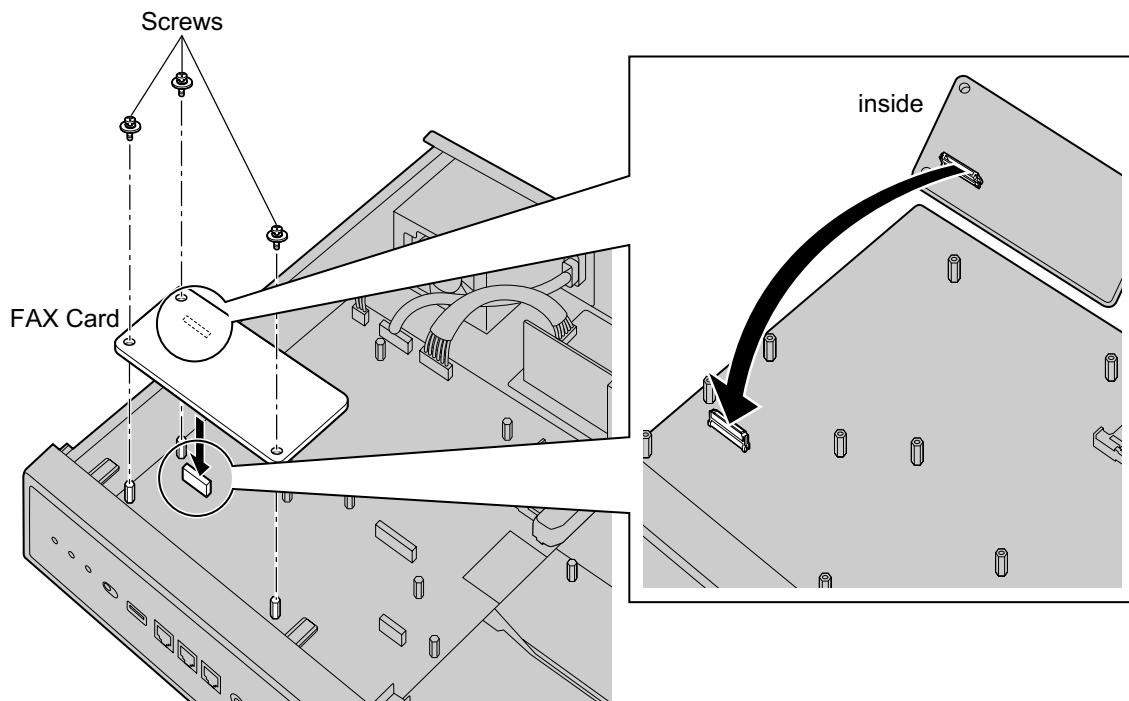
For details about assigning IP addresses through System Programming, refer to "Changing IP Address Settings".

DSP Card Type	Number of IP Addresses
DSP S/DSP M	1
DSP L	2

4.3.4 FAX Card (KX-NS0106)

Function

1-channel fax server. To be mounted on the mother board.



Accessories and User-supplied Items

Accessories (included): Screws × 3

User-supplied (not included): none

Note

When installing or removing the FAX card, do not put pressure on any parts of the mother board. Doing so may result in damage to the PBX.

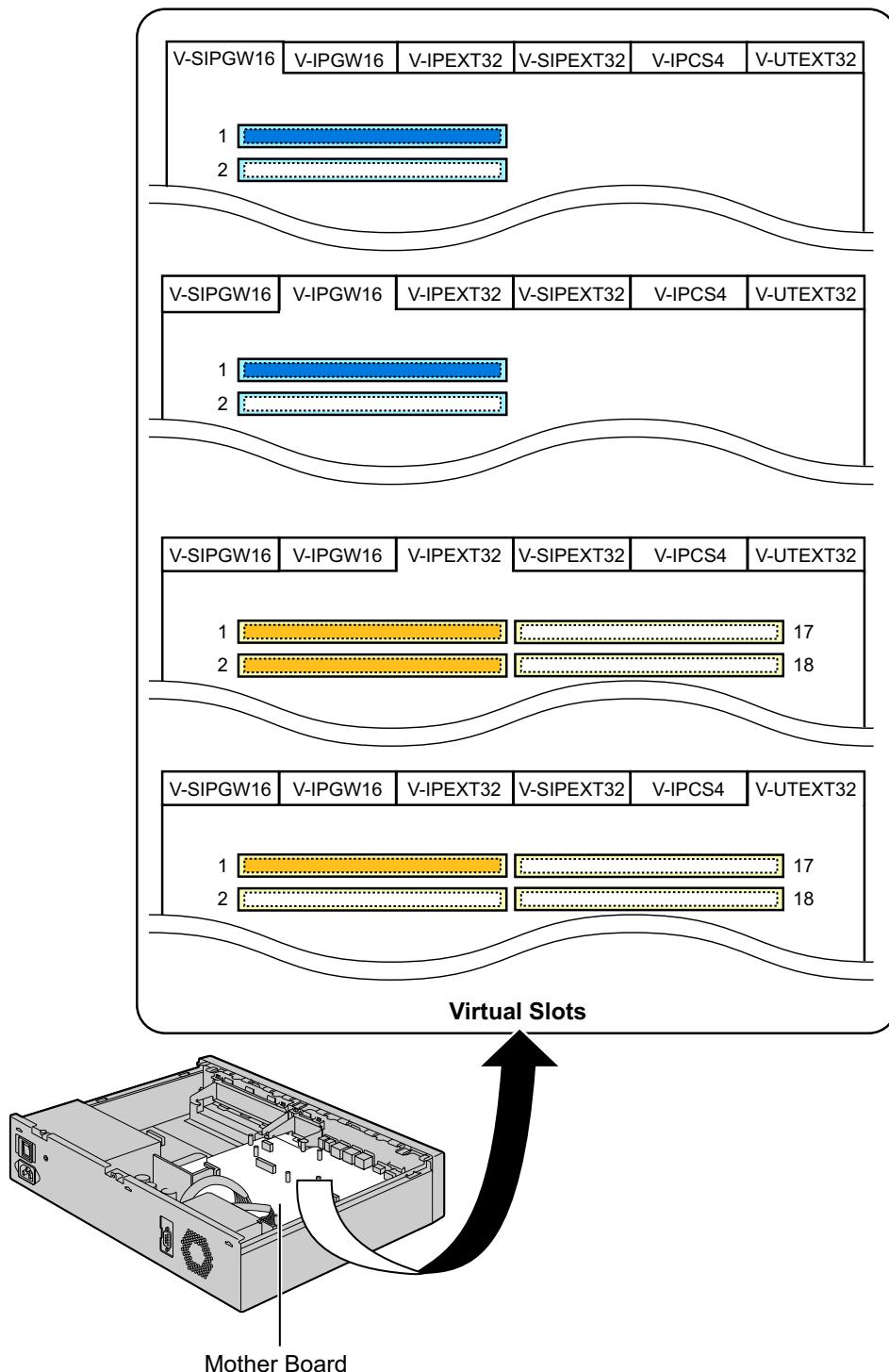
4.4 Virtual Cards

Function

Virtual Cards are programs included with the mother board and that are treated as virtual cards by Web Maintenance Console for convenience. Those programs can be activated with the appropriate activation key (apart from V-IPCS4 cards, which do not require activation keys). By installing Virtual Cards in the Virtual Slots of the mother board using Web Maintenance Console, IP trunks, IP extensions, and IP-CSs can be used via the mother board.

Virtual Card	Description
Virtual 16-Channel SIP Trunk Card (V-SIPGW16)	Virtual Card for 16-channel SIP trunk. Compliant with RFC 3261, 3262, 3264, 3311, 3581, 3960 and 4028 protocols, and ITU-T G.729A and G.711 codec methods. Also supports T.38 protocol.
Virtual 16-Channel VoIP Gateway Card (V-IPGW16)	Virtual Card for 16-channel H.323 trunk. Compliant with VoIP H.323 V.5 protocol, and ITU-T G.729A and G.711 codec methods. Also supports T.38 protocol.
Virtual 32-Channel VoIP Extension Card (V-IPEXT32)	Virtual Card for 32 IP-PTs (KX-NT300 series, KX-NT500 series, and KX-NT265 [software version 2.00 or later only]). Compliant with Panasonic proprietary protocol, and ITU-T G.729A, G.711 and G.722 codec methods.
Virtual 32-Channel SIP Extension Card (V-SIPEXT32)	Virtual Card for 32 third party SIP phones. Compliant with RFC 3261, 3264, 3310, 2327 and 4028 protocols, and ITU-T G.729A, G.711 and G.722 codec methods. Also supports T.38 protocol.
Virtual 4 IP Cell Station Interface Card (V-IPCS4)	Virtual Card for 4 IP-CSs. Compliant with ITU-T G.729A and G.711 codec methods.
Virtual UT Extension Card (V-UTEXT32)	Virtual Card for 32 KX-UT series SIP phones. Compliant with RFC 2327, 3261, 3264, 3310, 3515, 4028 and 4235 protocols, and ITU-T G.729A, G.711 and G.722 codec methods. Also supports WSD, CWMP and HTTP.

Example: Virtual Cards in the Virtual Slots of the PBX



4.5 Physical Trunk and Extension Cards

Note

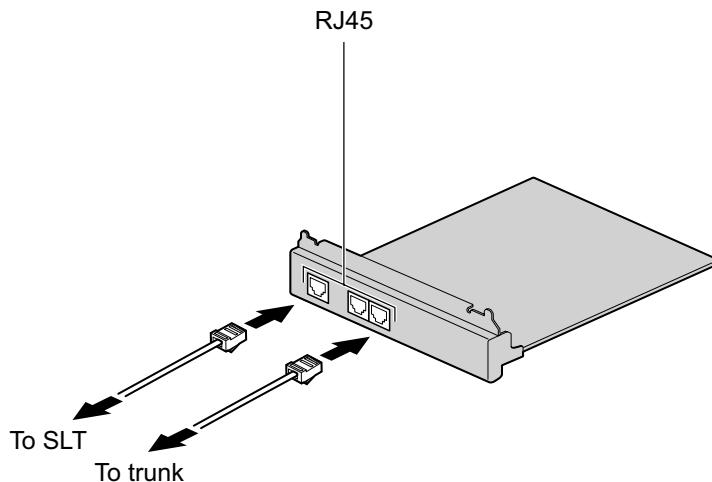
For details about physical trunk and extension cards for legacy gateways, refer to the Installation Manual for the corresponding PBX.

4.5.1 SLC2/LCOT2 Card (KX-NS0180)

Function

A combination card including:

- 2 analogue trunk ports with Caller ID (FSK/FSK with Call Waiting Caller ID [Visual Caller ID]/DTMF). One port is a power failure transfer (PFT) port.
- 2 extension ports with Caller ID (FSK) for SLTs.



Accessories and User-supplied Items

Accessories (included): Screws × 4

User-supplied (not included): RJ45 connector, Twisted pair cable

Note

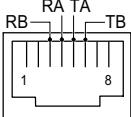
- For details about power failure transfer, refer to "4.12 Power Failure Ports".
- To confirm the trunk connection, refer to "Confirming the Trunk Connection" in "4.13 Starting the KX-NS1000".

Pin Assignments

RJ45 Connector for Trunk Use

	No.	Signal Name	Function
	1-3	Reserved	–
	4	R	Ring
	5	T	Tip
	6-8	Reserved	–

RJ45 Connector for Single Line Telephone Extension Use

	No.	Signal Name	Function
	1-2	Reserved	–
	3	RB	Ring B
	4	RA	Ring A
	5	TA	Tip A
	6	TB	Tip B
	7-8	Reserved	–

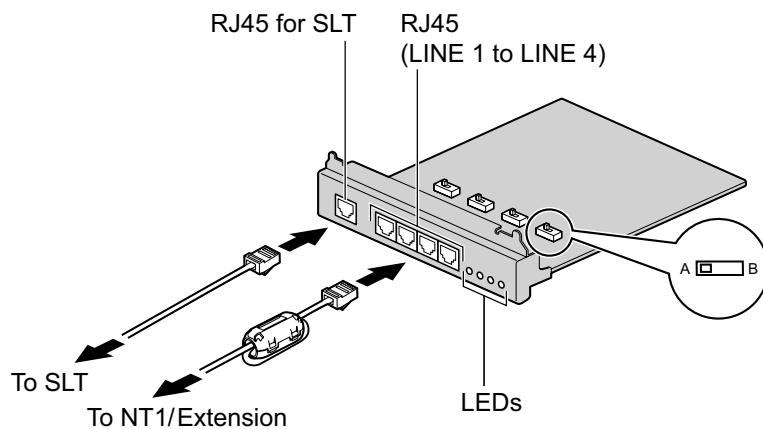
4.5.2 SLC2/BRI4 Card (KX-NS0280)

Function

A combination card including:

- 4 ISDN Basic Rate Interface ports.
- 2 extension ports with Caller ID (FSK) for SLTs.

EURO-ISDN/ETSI compliant.



Accessories and User-supplied Items

Accessories (included): Ferrite core × 2, Screws × 4

User-supplied (not included): RJ45 connector, Twisted pair cable

CAUTION

When connecting this optional service card to the trunk, connect through an NT1; do not connect to the U interface of the trunk directly.

Notice

When connecting the RJ45 connector, attach the included ferrite core. Refer to "4.2.8 Attaching a Ferrite Core".

Note

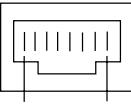
- This optional service card has $100\ \Omega$ of terminal resistance. For use in point to multi-point connection, the card must be placed at the end of the bus.
- This optional service card can be used for either trunk or extension connection, by setting the A/B switch or using the connector with appropriate pin assignments.
- To confirm the trunk connection, refer to "Confirming the Trunk Connection" in "4.13 Starting the KX-NS1000".

Switch Settings

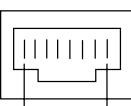
Switch	Type	Usage and Status Definition
A/B	Slide	Select A (default) for trunk or B for extension use.

Pin Assignments

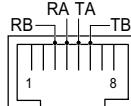
RJ45 Connector for Trunk Use

	No.	Signal Name	Level [V]	Function
	1-2	Reserved	–	–
	3	TX1	(+)	Transmit data 1
	4	RX1	(+)	Receive data 1
	5	RX2	(–)	Receive data 2
	6	TX2	(–)	Transmit data 2
	7-8	Reserved	–	–

RJ45 Connector for Extension Use

	No.	Signal Name	Level [V]	Function
	1-2	Reserved	–	–
	3	RX1	(+)	Receive data 1
	4	TX1	(+)	Transmit data 1
	5	TX2	(–)	Transmit data 2
	6	RX2	(–)	Receive data 2
	7-8	Reserved	–	–

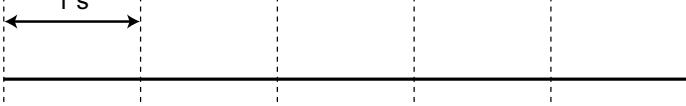
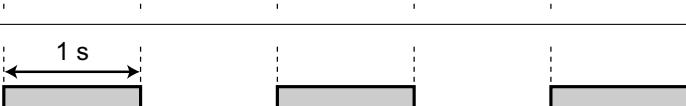
RJ45 Connector for Single Line Telephone Extension Use

	No.	Signal Name	Function
	1-2	Reserved	–
	3	RB	Ring B
	4	RA	Ring A
	5	TA	Tip A
	6	TB	Tip B
	7-8	Reserved	–

LED Indications

Indication	Colour	Description
LINE 4 LINE 3 LINE 2 LINE 1	Green	Line status indication (LINE 1 to LINE 4): Refer to "LINE LED Pattern" below for details.

LINE LED Pattern

Layer 1	Layer 2	Master Clock	LED Pattern
OFF	OFF	OFF	
ON	OFF	OFF	
ON	ON	OFF	
ON	OFF	ON	
ON	ON	ON	

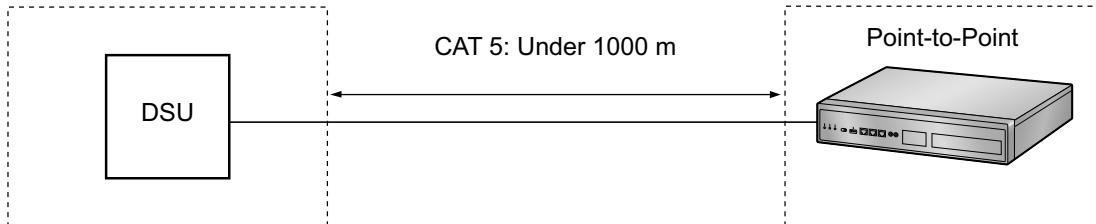
Layer 1: ON (Synchronous)

Layer 2: ON (Link established)/OFF (Link not established)

Master Clock: ON (Master)/OFF (Slave)

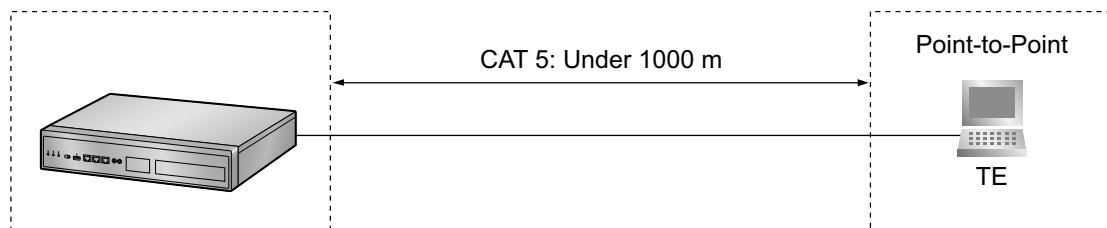
Maximum Cabling Distance of ISDN DSU Connection

The maximum length of the cable that connects the DSU and the PBX is shown below:



Maximum Cabling Distance of ISDN Terminal Equipment (TE) Connection

The maximum length of the extension cable that connects the PBX and the TE is shown below:



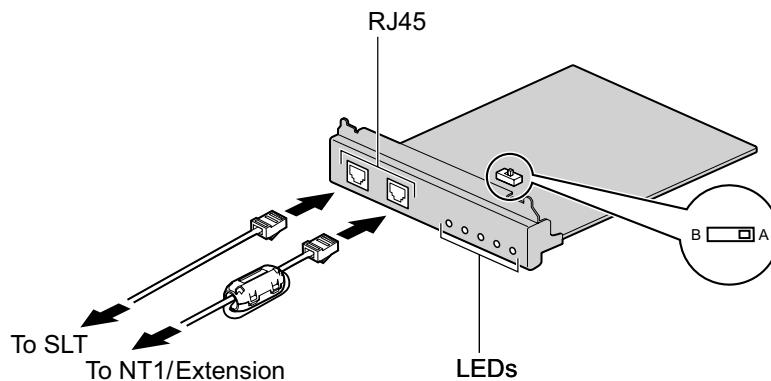
4.5.3 SLC2/PRI30 Card (KX-NS0290CE)

Function

A combination card including:

- 1 ISDN Primary Rate Interface port (30B channels).
- 2 extension ports with Caller ID (FSK) for SLTs.

EURO-ISDN/ETSI compliant.



Accessories and User-supplied Items

Accessories (included): Ferrite core × 1, Screws × 4

User-supplied (not included): RJ45 connector, Twisted pair cable

CAUTION

- When connecting this optional service card to the trunk, connect through an NT1; do not connect to the U interface of the trunk directly.
- PRI ports are SELV ports and should only be connected to SELV services.

Notice

- When connecting the RJ45 connector, attach the included ferrite core. Refer to "4.2.8 Attaching a Ferrite Core".
- The cable to connect to the ISDN Primary Rate Interface port of the SLC2/PRI30 card should be CAT 5 (Category 5) or higher.

Note

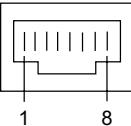
- In some countries/areas, this optional service card must not be connected to the Public Switched Telephone Network.
- This optional service card can be used for either trunk or extension connection, by setting the A/B switch or using the connector with appropriate pin assignments.
- To confirm the trunk connection, refer to "Confirming the Trunk Connection" in "4.13 Starting the KX-NS1000".

Switch Settings

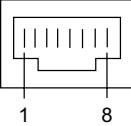
Switch	Type	Usage and Status Definition
A/B	Slide	Select A (default) for trunk or B for extension use.

Pin Assignments

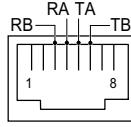
RJ45 Connector for Trunk Use

	No.	Signal Name	Level [V]	Function
	1	RX+	(+)	Receive data (+)
	2	RX-	(-)	Receive data (-)
	3	Reserved	-	-
	4	TX-	(-)	Transmit data (-)
	5	TX+	(+)	Transmit data (+)
	6-8	Reserved	-	-

RJ45 Connector for Extension Use

	No.	Signal Name	Level [V]	Function
	1	TX-	(-)	Transmit data (-)
	2	TX+	(+)	Transmit data (+)
	3	Reserved	-	-
	4	RX+	(+)	Receive data (+)
	5	RX-	(-)	Receive data (-)
	6-8	Reserved	-	-

RJ45 Connector for Single Line Telephone Extension Use

	No.	Signal Name	Function
	1-2	Reserved	-
	3	RB	Ring B
	4	RA	Ring A
	5	TA	Tip A
	6	TB	Tip B
	7-8	Reserved	-

LED Indications

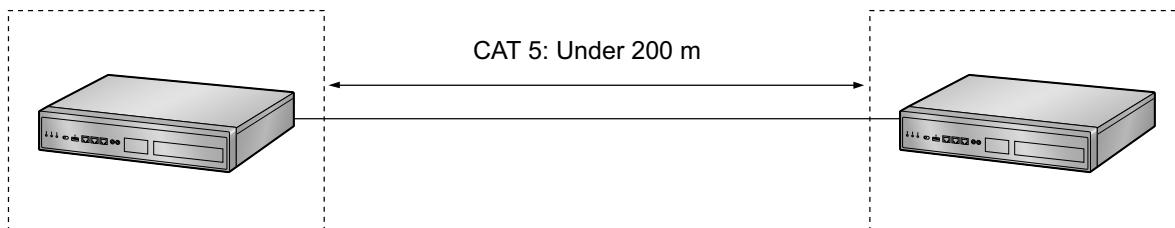
Indication	Colour	Description
SERR	Red	Non-synchronisation status indication <ul style="list-style-type: none"> OFF: Normal ON: Out of synchronisation

4.5.3 SLC2/PRI30 Card (KX-NS0290CE)

Indication	Colour	Description
RAI	Red	RAI signal status indication <ul style="list-style-type: none">• OFF: Normal• ON: Alarm• Flashing (60 times per minute): Alarm (Clock Master)
AIS	Red	AIS status indication <ul style="list-style-type: none">• OFF: Normal• ON: Alarm
SYNC	Green	Synchronisation status indication <ul style="list-style-type: none">• OFF: Not synchronised• ON: Synchronised• Flashing (60 times per minute): Synchronised (External Clock Master)
DLK	Green	Data link status indication <ul style="list-style-type: none">• OFF: Not established• ON: Established

Maximum Cabling Distance of Extension Connection

The maximum length of the extension cable that connects the PRI port is shown below:

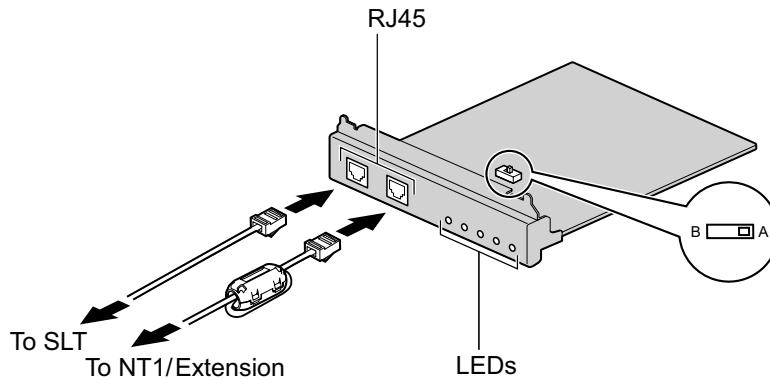


4.5.4 SLC2/PRI23 Card (KX-NS0290)

Function

A combination card including:

- 1 ISDN Primary Rate Interface port (23B channels).
 - 2 extension ports with Caller ID (FSK) for SLTs.
- NI (North American standard ISDN protocol) compliant.



Accessories and User-supplied Items

Accessories (included): Ferrite core × 1, Screws × 4

User-supplied (not included): RJ45 connector, Twisted pair cable

CAUTION

- When connecting this optional service card to the trunk, connect through an NT1; do not connect to the U interface of the trunk directly.
- PRI ports are SELV ports and should only be connected to SELV services.

Notice

- When connecting the RJ45 connector, attach the included ferrite core. Refer to "4.2.8 Attaching a Ferrite Core".
- The cable to connect to the ISDN Primary Rate Interface port of the SLC2/PRI23 card should be CAT 5 (Category 5) or higher.

Note

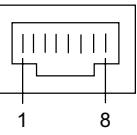
- This optional service card can be used for either trunk or extension connection, by setting the A/B switch or using the connector with appropriate pin assignments.
- To confirm the trunk connection, refer to "Confirming the Trunk Connection" in "4.13 Starting the KX-NS1000".

Switch Settings

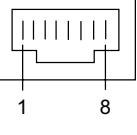
Switch	Type	Usage and Status Definition
A/B	Slide	Select A (default) for trunk or B for extension use.

Pin Assignments

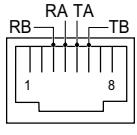
RJ45 Connector for Trunk Use

	No.	Signal Name	Level [V]	Function
	1	RX+	(+)	Receive data (+)
	2	RX-	(-)	Receive data (-)
	3	Reserved	-	-
	4	TX-	(-)	Transmit data (-)
	5	TX+	(+)	Transmit data (+)
	6-8	Reserved	-	-

RJ45 Connector for Extension Use

	No.	Signal Name	Level [V]	Function
	1	TX-	(-)	Transmit data (-)
	2	TX+	(+)	Transmit data (+)
	3	Reserved	-	-
	4	RX+	(+)	Receive data (+)
	5	RX-	(-)	Receive data (-)
	6-8	Reserved	-	-

RJ45 Connector for Single Line Telephone Extension Use

	No.	Signal Name	Function
	1-2	Reserved	-
	3	RB	Ring B
	4	RA	Ring A
	5	TA	Tip A
	6	TB	Tip B
	7-8	Reserved	-

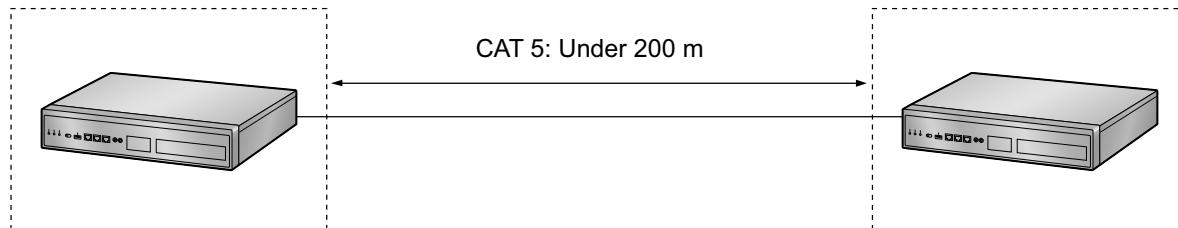
LED Indications

Indication	Colour	Description
SERR	Red	Non-synchronisation status indication <ul style="list-style-type: none"> OFF: Normal ON: Out of synchronisation

Indication	Colour	Description
RAI	Red	RAI signal status indication <ul style="list-style-type: none"> OFF: Normal ON: Alarm (Clock Slave) Flashing (60 times per minute): Alarm (Clock Master)
AIS	Red	AIS status indication <ul style="list-style-type: none"> OFF: Normal ON: Alarm
SYNC	Green	Synchronisation status indication <ul style="list-style-type: none"> OFF: Not synchronised ON: Synchronised Flashing (60 times per minute): Synchronised (External Clock Master)
DLK	Green	Data link status indication <ul style="list-style-type: none"> OFF: Not established ON: Established

Maximum Cabling Distance of Extension Connection

The maximum length of the extension cable that connects the PRI port is shown below:

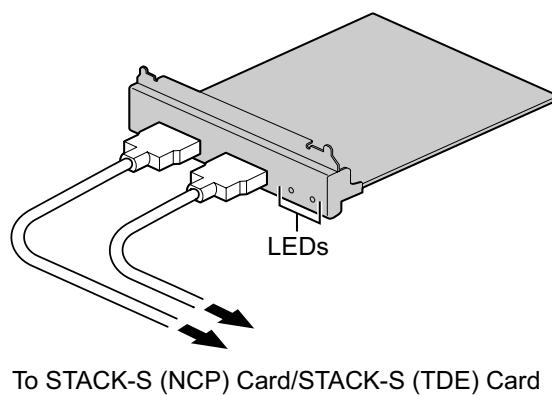


4.6 Stacking Cards

4.6.1 STACK-M Card (KX-NS0130)

Function

A stacking card to be installed in a KX-NS1000. Up to 2 legacy gateways can be connected. This card can be used only with PCMPR Software Version 002.01000 or later.



Accessories and User-supplied Items

Accessories (included): Screws × 4

User-supplied (not included): None¹

¹ The necessary stacking cable to connect the STACK-M card and the STACK-S (NCP) or STACK-S (TDE) card is included with the STACK-S (NCP)/STACK-S (TDE) card.

LED Indications

Indication	Colour	Description
Link 1	Green	Connection status indication for legacy gateway
Link 2	Green	<ul style="list-style-type: none">ON: Normal connectionOFF: Connection error

Conditions for Connecting Legacy Gateways

Up to 2 KX-TDA/KX-TDE/KX-NCP series PBXs, KX-TDA100D PBXs, and KX-NS1020 expansion cabinets can be connected to a KX-NS1000 and used as legacy gateways under the following conditions:

Condition 1

You cannot connect legacy gateways of mixed categories to a KX-NS1000. The following table shows the category number for each type of PBX:

Category	Model
1	KX-NCP500
	KX-NCP1000
	KX-NS1020
2	KX-TDE100
	KX-TDE200
	KX-TDA100
	KX-TDA200
3	KX-TDE600
	KX-TDE620
	KX-TDA600
	KX-TDA620
4	KX-TDA100D

Example:

KX-NCP500 (category 1) and KX-NCP1000 (category 1): OK

KX-NCP500 (category 1) and KX-TDA100 (category 2): Not allowed

Notice

The following PBX models cannot be connected as legacy gateways:

- KX-TDA15
- KX-TDA30

Note

- For details about connecting a KX-NS1020 as legacy gateways to KX-NS1000, refer to your KX-NS1020 Installation Manual.

Condition 2 (KX-TDE100/KX-TDE200/KX-TDA100/KX-TDA200/KX-TDA100D only)

If you install the OPB3 card with an ECHO16 card, they must be installed in SLOT1 of the legacy gateway.

Condition 3 (KX-TDE600/KX-TDE620/KX-TDA600/KX-TDA620 only)

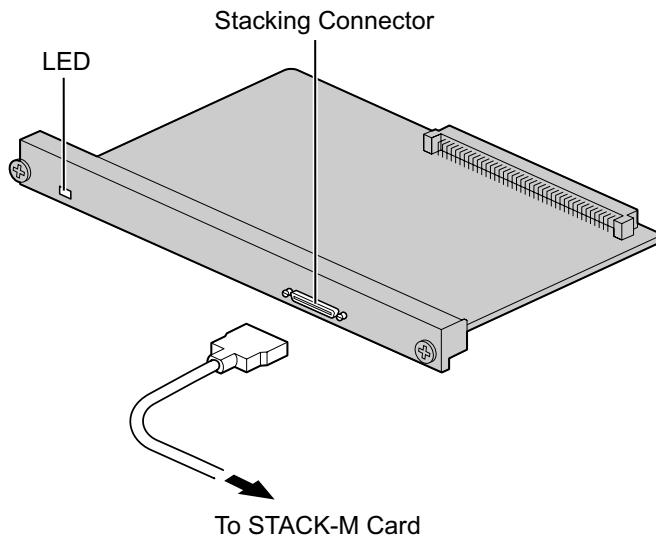
- The KX-TDE600 and KX-TDE620 must be disconnected from each other before connecting to a KX-NS1000.
- The KX-TDA600 and KX-TDA620 must be disconnected from each other before connecting to a KX-NS1000.

4.6.2 STACK-S (NCP) Card (KX-NS0131)

Function

A stacking card to be installed in the MPR card slot of a KX-NCP500 or KX-NCP1000 to be used as a legacy gateway.

This card can be used only with PCMPR Software Version 002.01000 or later.



Accessories and User-supplied Items

Accessories (included): Stacking cable × 1

User-supplied (not included): None

WARNING

A lithium battery is used in the STACK-S (NCP) card. There is a risk of explosion if the battery is replaced with an incorrect type. Dispose of used batteries according to the manufacturer's instructions.

CAUTION

When installing or removing this card, the power switch must be turned off.

Notice

When stacking other PBXs with the KX-NS1000, place them well within reach of the stacking cable (2 m).

LED Indications

STACK-S (NCP) Card

Indication	Colour	Description
CARD STATUS	Green	STACK-S (NCP) card status indication <ul style="list-style-type: none"> ON: INS (In Service)
	Red	STACK-S (NCP) card status indication <ul style="list-style-type: none"> ON: Fault Flashing: OUS (Out of Service)

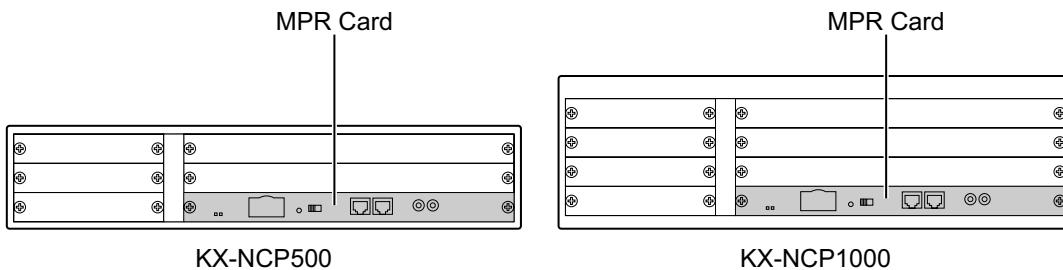
Legacy Gateway

Indication	Colour	Description
RUN	Green	<p>Status indication for legacy gateway</p> <ul style="list-style-type: none"> ON: Normal OFF: Power off Slow Flashing: Starting up Moderate Flashing: STACK-S (NCP) card error <p>Note</p> <p>LED flashing patterns are as follows:</p> <ul style="list-style-type: none"> Slow Flashing: 60 times per minute Moderate Flashing: 120 times per minute
ALARM	Red	<p>Alarm status indication for legacy gateway</p> <ul style="list-style-type: none"> ON: Alarm OFF: Normal

Installing and Removing a STACK-S (NCP) Card**Before Installing the STACK-S (NCP) Card**

Before you install a STACK-S (NCP) card in a PBX that has been used, make a backup of the system data in case you want to use it later, with another PBX, etc. For details about making a backup, refer to the PC Programming Manual of the corresponding PBX.

To use the PBX as a legacy gateway, the MPR card must be replaced with a STACK-S (NCP) card.



Follow the procedure below to install a STACK-S (NCP) card in the PBX.

1. Remove the 2 screws from the MPR card slot, and then remove the MPR card.
2. Insert the STACK-S (NCP) card into the MPR card slot along the guide rails.
3. Reinsert the 2 screws and turn them clockwise to fix the STACK-S (NCP) card in place.

Note

- To remove the STACK-S (NCP) card, reverse the procedure above.
- Make sure the screws are tightened to earth the card securely.

For more details about installing and removing optional service cards, refer to the Installation Manual of the corresponding PBX.

4.6.3 STACK-S (TDE) Card (KX-NS0132)

Function

A stacking card to be installed in the MPR card slot or the BUS-S card slot of the PBX to be used as a legacy gateway.

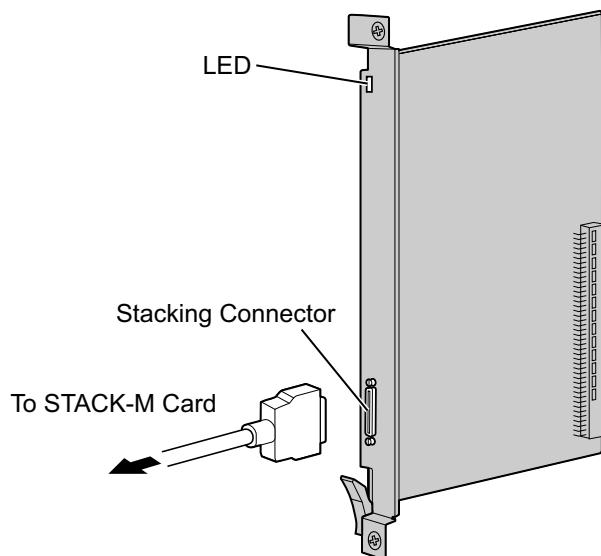
For the following PBXs, this card is installed in the MPR card slot:

KX-TDE100, KX-TDE200,
KX-TDA100, KX-TDA200,
KX-TDE600, KX-TDA600,
KX-TDA100D

For the following PBXs, this card is installed in the BUS-S card slot:

KX-TDE620, KX-TDA620

This card can be used only with PCMPR Software Version 002.03000 or later.



Accessories and User-supplied Items

Accessories (included): Stacking cable × 1

User-supplied (not included): None

WARNING

A lithium battery is used in the STACK-S (TDE) card. There is a risk of explosion if the battery is replaced with an incorrect type. Dispose of used batteries according to the manufacturer's instructions.

CAUTION

When installing or removing this card, the power switch must be turned off.

Notice

When stacking other PBXs with the KX-NS1000, place them well within reach of the stacking cable (2 m).

LED Indications

STACK-S (TDE) Card

Indication	Colour	Description
CARD STATUS	Green	STACK-S (TDE) card status indication <ul style="list-style-type: none"> ON: INS (In Service)
	Red	STACK-S (TDE) card status indication <ul style="list-style-type: none"> ON: Fault Flashing: OUS (Out of Service)

Legacy Gateway

Indication	Colour	Description
RUN	Green	Status indication for legacy gateway <ul style="list-style-type: none"> ON: Normal OFF: Power off Slow Flashing: Starting up Moderate Flashing: STACK-S (TDE) card error <p>Note</p> <p>LED flashing patterns are as follows:</p> <ul style="list-style-type: none"> Slow Flashing: 60 times per minute Moderate Flashing: 120 times per minute
ALARM	Red	Alarm status indication for legacy gateway <ul style="list-style-type: none"> ON: Alarm OFF: Normal

Installing and Removing a STACK-S (TDE) Card

Before Installing the STACK-S (TDE) Card

Before you install a STACK-S (TDE) card in a PBX that has been used, make a backup of the system data in case you want to use it later, with another PBX, etc. For details about making a backup, refer to the PC Programming Manual of the corresponding PBX.

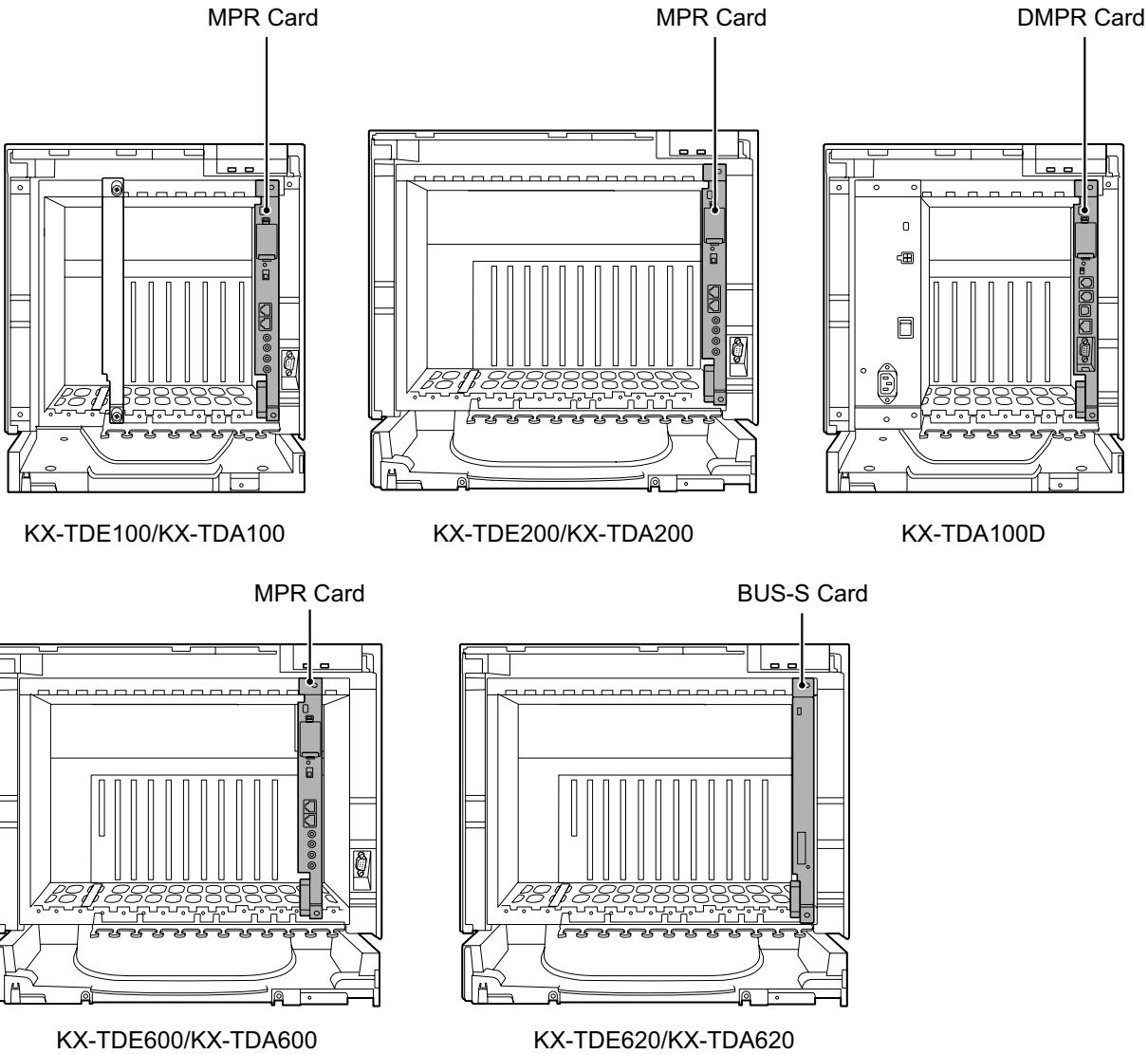
To use the PBX as a legacy gateway, the MPR card must be replaced with a STACK-S (TDE) card.

Note

- For some PBXs, the appearance of the MPR card and BUS-S card may differ from the following illustrations.

4.6.3 STACK-S (TDE) Card (KX-NS0132)

- For KX-TDE620 and KX-TDA620, replace the BUS-S card with a STACK-S (TDE) card.



Follow the procedure below to install a STACK-S (TDE) card in the PBX.

- Remove the front cover as instructed in the Installation Manual for the PBX.
- Remove the 2 screws from the MPR card slot/BUS-S card slot.
- Pull the release lever in the direction of the arrow to disconnect the MPR card/BUS-S card from the back board. Pull the card from the shelf to remove it.

Note

If a BUS-M card is installed in a KX-TDE600/KX-TDA600, remove the BUS-M card in the same way as the MPR card/BUS-S card.

- Insert the STACK-S (TDE) card into the MPR card slot/BUS-S card slot along the guide rails.
- Holding the STACK-S (TDE) card, push the release lever in the direction of the arrow so that the STACK-S (TDE) card engages securely with the connector on the back board.
- Reinsert the 2 screws and turn them clockwise to fix the STACK-S (TDE) card in place.
- Close the front cover as instructed in the Installation Manual for the PBX.

Note

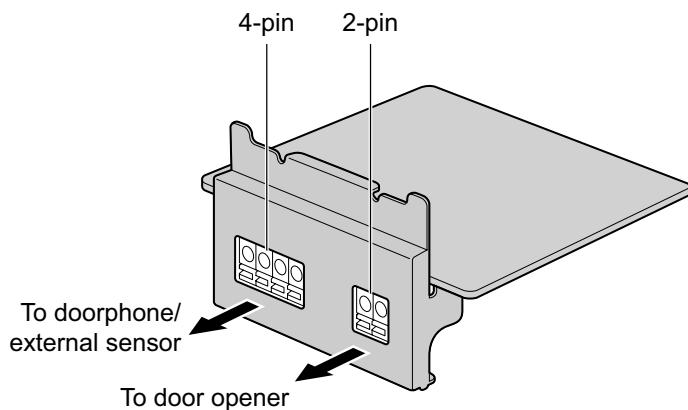
- To remove the STACK-S (TDE) card, reverse the procedure above.
- For more details about installing and removing optional service cards, refer to the Installation Manual of the corresponding PBX.

4.7 The Doorphone Card

4.7.1 DOORPHONE Card (KX-NS0161)

Function

A doorphone card for 1 doorphone, 1 door opener, and 1 external sensor.



Accessories and User-supplied Items

Accessories (included): Screws × 2

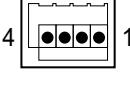
User-supplied (not included): Copper wire

Note

For details about connecting to a doorphone and/or door opener, refer to "4.9 Connecting to a Doorphone, Door Opener, and/or External Sensor".

Pin Assignments

4-pin Terminal Block

	No.	Signal Name	Function
	1	SENS1b	Sensor 1 common
	2	SENS1a	Sensor 1
	3	COM1	Doorphone 1 receive
	4	DP1	Doorphone 1 transmit

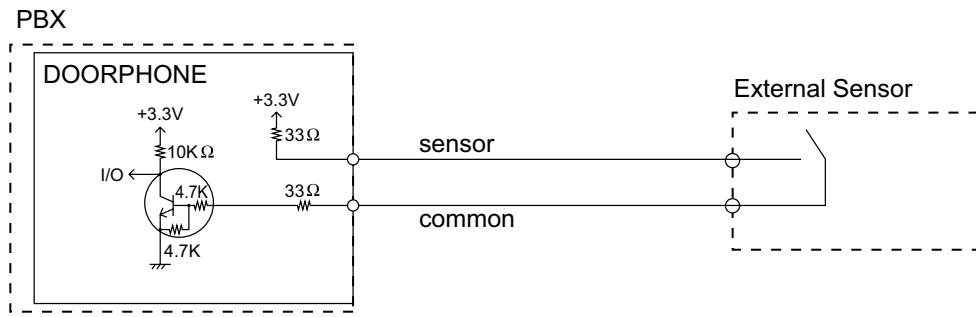
2-pin Terminal Block

	No.	Signal Name	Function
	1	OP1b	Door opener 1 (Relay)
	2	OP1a	Door opener 1 com (Relay com)

External Sensor

Power to the external sensor is provided from the DOORPHONE card and must be grounded through the DOORPHONE card as indicated in the diagram below. A pair of "sensor" and "common" lines are connected to the DOORPHONE card for each external sensor. The PBX detects input from the sensor when the signal is under $100\ \Omega$.

Connection Diagram



Door Opener

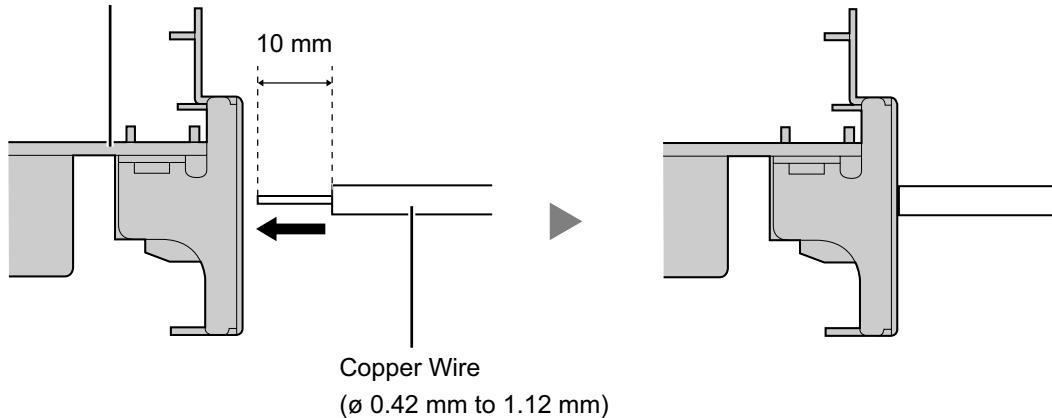
Current Limit: 24 V DC/30 V AC, 1 A maximum

Connecting to the DOORPHONE Card

When connecting a doorphone, door opener, and/or external sensor to the DOORPHONE card, use copper wire with a diameter from 0.42 mm to 1.12 mm. Follow the procedure below to connect a doorphone, door opener, and/or external sensor to the DOORPHONE card.

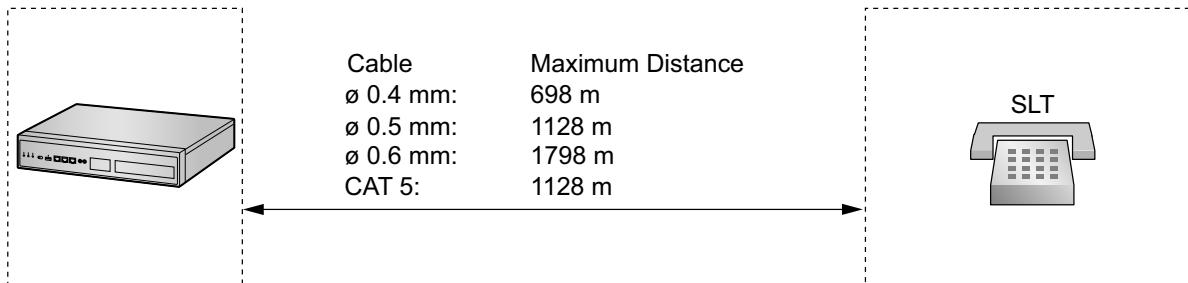
1. Strip off the insulation of the wire about 10 mm from the end.
2. Use a screwdriver to press on the orange tab at the bottom of the terminal block, and insert the wire into the upper hole.
3. Check from side to ensure that no bare copper wire is exposed.

DOORPHONE Card



4.8 Connection of SLTs

4.8.1 Maximum Cabling Distances of the Extension Wiring (Twisted Cable)



Notice

The maximum cabling distance may vary depending on the conditions.

Note

For information about maximum cabling distances for stacked PBXs, refer to the Installation Manual for each PBX.

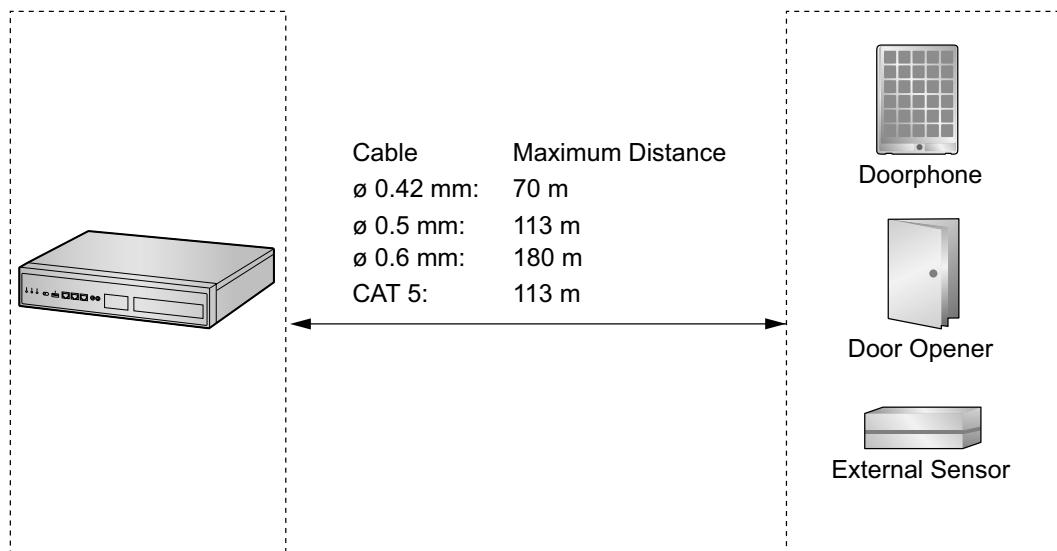
4.9 Connecting to a Doorphone, Door Opener, and/or External Sensor

The PBX supports 1 each of a doorphone, a door opener, and an external sensor.

Note

- Doorphones, door openers, and external sensors are user-supplied.
- For information about maximum cabling distances for stacked PBXs, refer to the Installation Manual for each PBX.

Maximum Cabling Distance

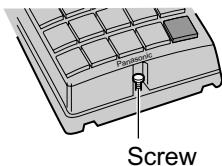


Installing the Doorphone (KX-T30865/KX-T7765)

Note

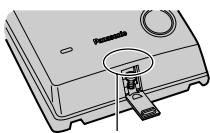
The illustrations shown in the installation procedure are based on the KX-T30865.

1. Loosen the screw to separate the doorphone into 2 halves.



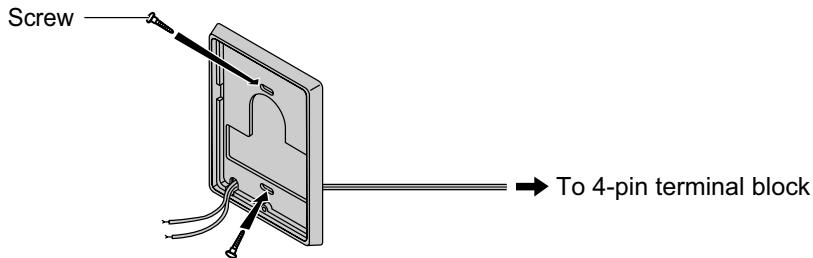
Note for KX-T7765 Users

When loosening/tightening the screw, do not scratch the cabinet wall with the driver shaft.



Cabinet Wall

2. Pass the wires through the hole in the base cover, and attach the base cover to a wall using 2 screws.



Note

Two kinds of screws are included with the doorphone. Please choose the appropriate kind for your wall type.

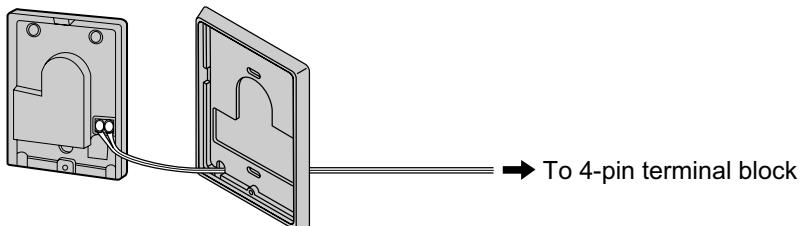


: when a doorphone plate has been fixed to the wall



: when you wish to install the doorphone directly onto the wall

3. Connect the wires to the screws located in the back cover.



4. Re-attach the 2 halves and re-insert the screw.

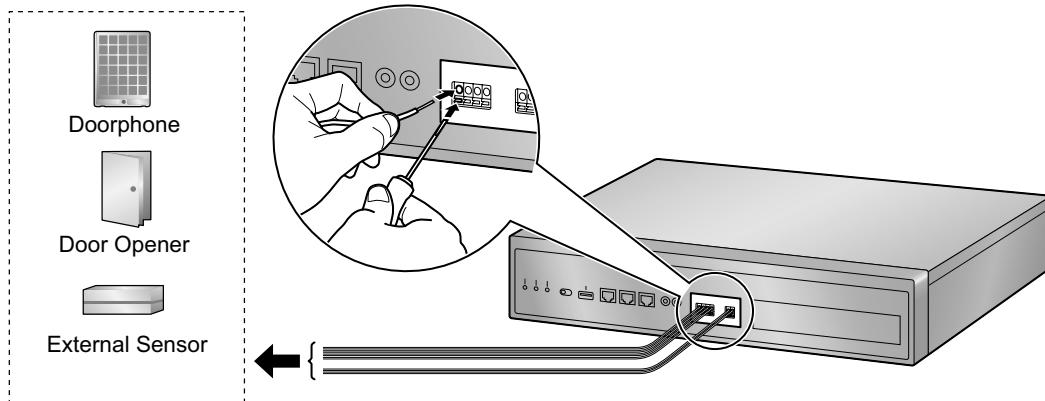
Connection

Use 4-pin and 2-pin terminal blocks (included with the card) for connection.

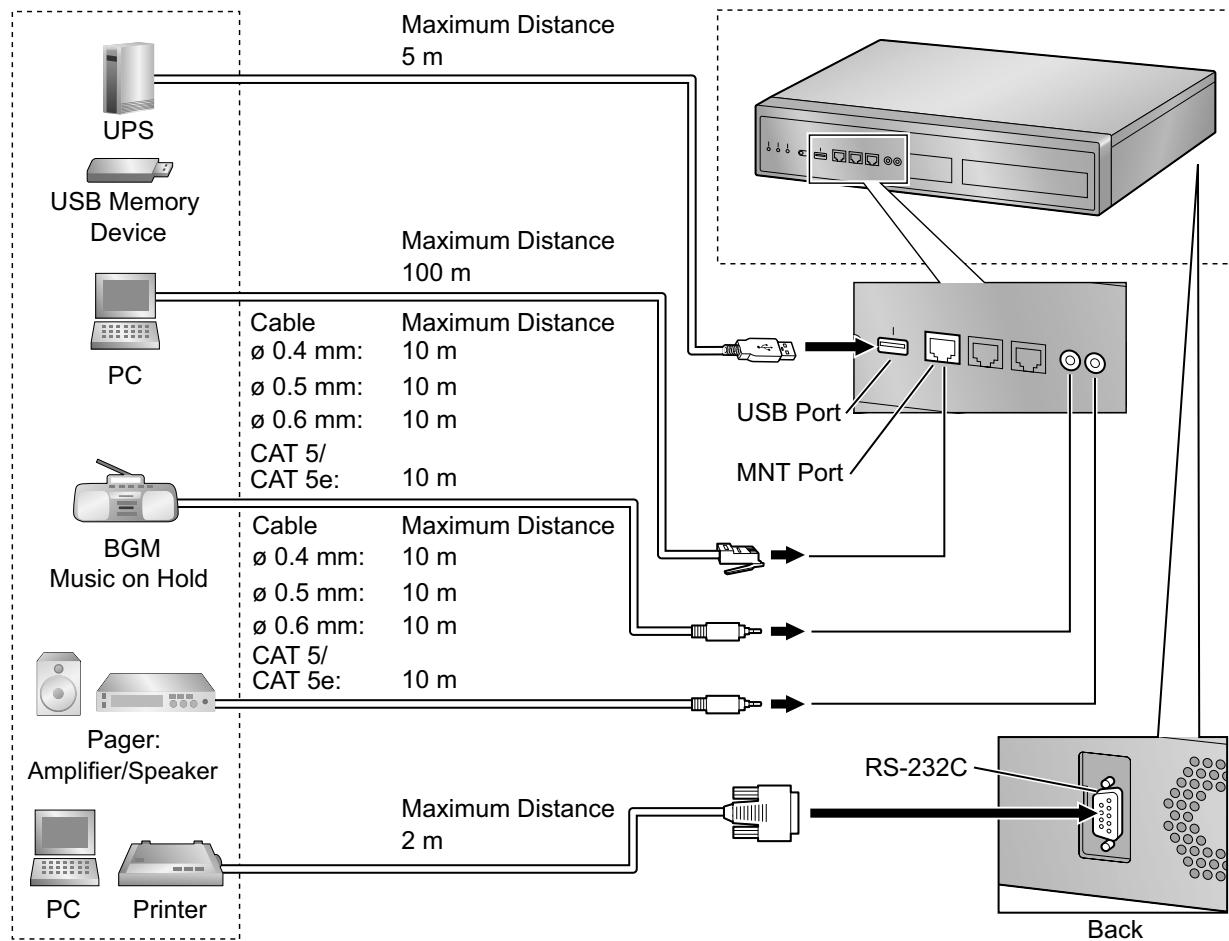
1. While pressing on the orange tab at the bottom of the terminal block using a screwdriver, insert the wire into the upper hole as shown below. Repeat this procedure for each doorphone, door opener, and/or external sensor wire to connect.

Refer to "4.7.1 DOORPHONE Card (KX-NS0161)" for pin assignments.

For information about wiring, refer to "Connecting to the DOORPHONE Card".



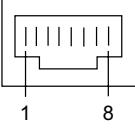
4.10 Connection of Peripherals



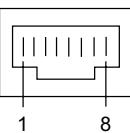
PC (via MNT Port)

A PC can be connected to the PBX via the MNT port of the PBX. It is used for system programming, diagnostics and external system database storage (save/load) functions.

Pin Assignments for 10BASE-T/100BASE-TX

	No.	Signal Name	Input (I)/Output (O)	Function
	1	TPO+	O	Transmit data+
	2	TPO-	O	Transmit data-
	3	TPI+	I	Receive data+
	4-5	Reserved	-	-
	6	TPI-	I	Receive data-
	7-8	Reserved	-	-

Pin Assignments for 1000BASE-T

	No.	Signal Name	Input (I)/Output (O)	Function
	1	TRD0 (+)	I/O	Transmit and receive data 0 (+)
	2	TRD0 (-)	I/O	Transmit and receive data 0 (-)
	3	TRD1 (+)	I/O	Transmit and receive data 1 (+)
	4	TRD2 (+)	I/O	Transmit and receive data 2 (+)
	5	TRD2 (-)	I/O	Transmit and receive data 2 (-)
	6	TRD1 (-)	I/O	Transmit and receive data 1 (-)
	7	TRD3 (+)	I/O	Transmit and receive data 3 (+)
	8	TRD3 (-)	I/O	Transmit and receive data 3 (-)

Note

You can use 1000BASE-T cables for 10BASE-T/100BASE-TX connections.

BGM/MOH

The PBX provides Background Music and Music on Hold. An external music source (e.g., user-supplied radio) can be connected to the PBX.

CAUTION

The MOH port is an SELV port and should only be connected to an approved SELV device, or in Australia, via a Line Isolation Unit with a Telecommunications Compliance Label.

Notice

- Wiring should be done carefully to prevent undue force being exerted on the plug. Otherwise, sound may only be heard intermittently.
- When the PBX and external music source are not connected to the same earth, hum noise may be induced into Background Music and Music on Hold.

Pager

A paging device (user-supplied) can be connected to the PBX.

CAUTION

The Pager port is an SELV port and should only be connected to an approved SELV device, or in Australia, via a Line Isolation Unit with a Telecommunications Compliance Label.

PC/Printer (via RS-232C)

The PBX is equipped with an RS-232C interface. This interface provides communication between the PBX and the user-supplied devices such as PC or line printers. The RS-232C port is used for SMDR, diagnostics and external system database storage (save/load) functions.

CAUTION

To protect the system, keep the following in mind:

1. Make sure that both connector cases (frame ground) of the RS-232C cross cable (shielded cable) are conductive. If they are not conductive, make sure that both connector cases of the cable are firmly connected.
2. If this is not possible, connect the frame of the PBX to the frame of the PC/Printer using an earthing wire in order to prevent difference in the electrical potentials.

Pin Assignments

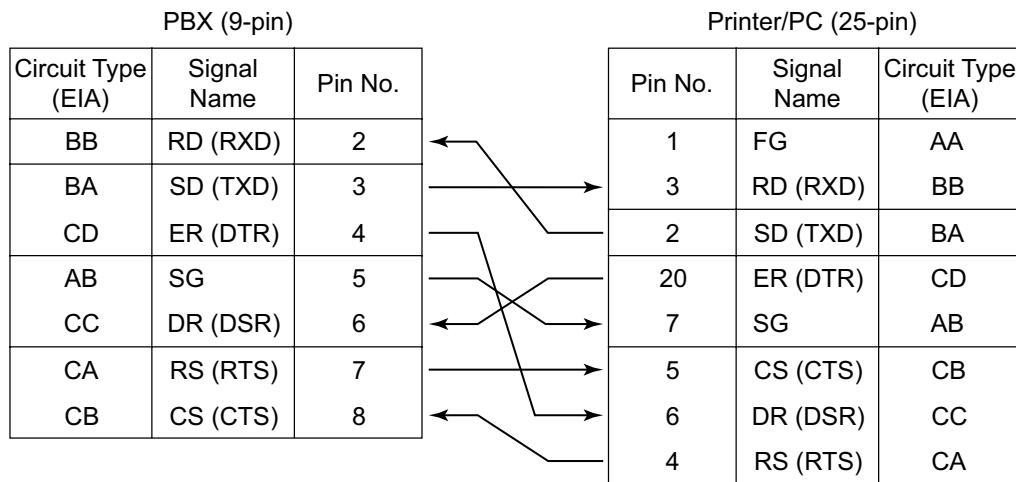
	No.	Signal Name	Function	Circuit Type	
				EIA	CCITT
	2	RD (RXD)	Receive Data	BB	104
	3	SD (TXD)	Transmit Data	BA	103
	4	ER (DTR)	Data Terminal Ready	CD	108.2
	5	SG	Signal Ground	AB	102
	6	DR (DSR)	Data Set Ready	CC	107
	7	RS (RTS)	Request To Send	CA	105
	8	CS (CTS)	Clear To Send	CB	106

Connection Charts

For connecting a printer/PC with a 9-pin RS-232C connector

PBX (9-pin)			Printer/PC (9-pin)		
Circuit Type (EIA)	Signal Name	Pin No.	Pin No.	Signal Name	Circuit Type (EIA)
BB	RD (RXD)	2	2	RD (RXD)	BB
BA	SD (TXD)	3	3	SD (TXD)	BA
CD	ER (DTR)	4	4	ER (DTR)	CD
AB	SG	5	5	SG	AB
CC	DR (DSR)	6	6	DR (DSR)	CC
CA	RS (RTS)	7	7	RS (RTS)	CA
CB	CS (CTS)	8	8	CS (CTS)	CB

For connecting a printer/PC with a 25-pin RS-232C connector



RS-232C Signals

- **Receive Data (RXD):...**(input)
Conveys signals from the printer or the PC.
- **Transmit Data (TXD):...**(output)
Conveys signals from the unit to the printer or the PC. A "Mark" condition is held unless data or BREAK signals are being transmitted.
- **Data Terminal Ready (DTR):...**(output)
This signal line is turned ON by the unit to indicate that it is ON LINE. Circuit ER (DTR) ON does not indicate that communication has been established with the printer or the PC. It is switched OFF when the unit is OFF LINE.
- **Signal Ground (SG)**
Connects to the DC ground of the unit for all interface signals.
- **Data Set Ready (DSR):...**(input)
An ON condition of circuit DR (DSR) indicates the printer or the PC is ready. Circuit DR (DSR) ON does not indicate that communication has been established with the printer or the PC.
- **Request To Send (RTS):...**(output)
This lead is held ON whenever DR (DSR) is ON.
- **Clear To Send (CTS):...**(input)
An ON condition of circuit CS (CTS) indicates that the printer or the PC is ready to receive data from the unit. The unit does not attempt to transfer data or receive data when circuit CS (CTS) is OFF.
- **Frame Ground (FG)**
Connects to the unit frame and the earth ground conductor of the AC power cord.

USB Interface for Uninterruptible Power Supply (UPS) and USB Memory Device

The PBX is equipped with a USB 2.0 interface. This interface provides communication between the PBX and user-supplied devices such as a UPS or USB memory device.

Using a USB memory device

A USB memory device can be used to backup and restore the system data of the PBX.

The PBX supports USB memory devices that meet the following specifications:

- File system: FAT
- Maximum capacity: 32 GB

4.10 Connection of Peripherals

- Maximum current: 500 mA

For details about backing up and restoring using a USB memory device, refer to "6.1.1 Tool—System Data Backup—Backup to USB" in the PC Programming Manual.

Note

Do not use a USB hub when connecting a USB memory device to the PBX.

Using a UPS

A UPS is a device that supplies power for several minutes to a connected device when a power failure occurs. For details about connecting a UPS to the PBX, refer to "Connecting an Uninterruptible Power Supply (UPS)".

Note

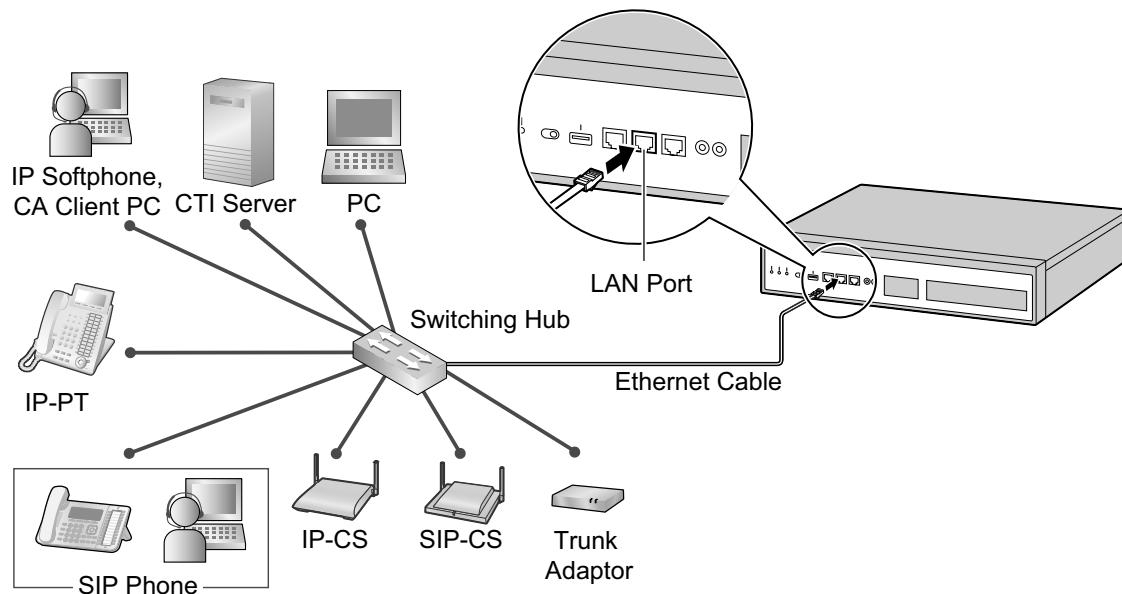
When connecting a UPS, use only the USB cable included with the UPS, and do not use a USB hub.

4.11 LAN Connection

4.11.1 LAN Connection for the Main Unit

Connecting the Main Unit to the LAN

The PBX is equipped with a LAN port for connecting to a LAN so that IP telephones (IP-PTs, IP softphones, SIP phones), IP-CSs, PCs and a CTI Server can be connected on a private IP network. When the PBX is connected to the LAN for the first time, you must assign IP addressing information to the PBX. See "5.4 Programming the PBX" for instructions.



Connection for 10BASE-T/100BASE-TX

Signal Name	Pin No.		Pin No.	Signal Name
TX+	1	→	1	RX+
TX-	2	←	2	RX-
RX+	3	←	3	TX+
RX-	6	→	6	TX-

4.11.1 LAN Connection for the Main Unit

Switching Hub		Connection for 1000BASE-T		PBX (LAN Port)	
Signal Name	Pin No.			Pin No.	Signal Name
TRD0 (+)	1		↔	1	TRD0 (+)
TRD0 (-)	2	↔		2	TRD0 (-)
TRD1 (+)	3	↔		3	TRD1 (+)
TRD2 (+)	4	↔		4	TRD2 (+)
TRD2 (-)	5	↔		5	TRD2 (-)
TRD1 (-)	6	↔		6	TRD1 (-)
TRD3 (+)	7	↔		7	TRD3 (+)
TRD3 (-)	8	↔		8	TRD3 (-)

Note

- Use an Ethernet cable with an RJ45 connector for connection to a switching hub. The cable should be a CAT 5 (Category 5) or higher for 10BASE-T/100BASE-TX, or CAT 5e (Enhanced Category 5) or higher for 1000BASE-T.
- Make sure that all CAT 5/CAT 5e cables in use are not over 100 m in length.
- Make sure to set the port of the switching hub that connects to the card to operate under "Auto Negotiation" mode.
- Make sure to create a spanning tree for LAN connection in order to prevent loops from occurring in a multi-bridged environment. Otherwise, some packets may circulate for long periods of time and eventually PBX performance system may degrade.
- The CTI server can be used for connecting PCs on a LAN to provide third party call control CTI. CTI connection uses the CSTA Phase 3 or TAPI 2.1 protocol. The operating system of the PC or CTI server required for third party call control depends on your CTI application software. For details, refer to the manual for your CTI application software.
- When using the VLAN feature on the network, make sure that the PBX is connected to a layer 2 switch that is IEEE 802.1Q compliant, and that is configured for VLANs. In addition, the port of the switching hub to which the PBX is connected must be set to "Untagged". Consult your network administrator for details.

4.11.2 LAN Connections for IP Telephones

When an IP telephone is connected to the LAN and power is supplied for the first time, you will be prompted to set network parameters. The network parameters must be set for the IP telephone before it can be used. Refer to "5.8 Assigning Networking Information to IP Telephones" for instructions.

Connecting an IP Telephone to a Switching Hub

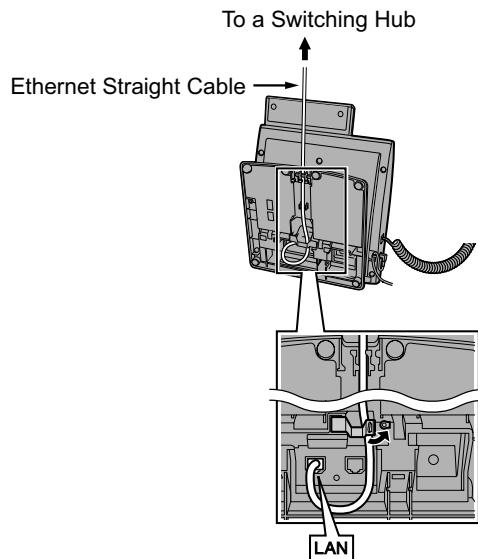
When connecting an IP telephone to the LAN, connect it to a switching hub.

Note

- Use an Ethernet straight cable with an RJ45 connector to connect the IP telephone to a switching hub. The cable should be a CAT 5 (Category 5) or higher for 10BASE-T/100BASE-TX, or CAT 5e (Enhanced Category 5) or higher for 1000BASE-T.
- When using the VLAN feature on the network, make sure that the switching hub to be connected is IEEE 802.1Q compliant and is configured for VLANs. In addition, the port of a switching hub that the IP telephone is connected to must be set to "Trunk" port, to allow VLAN tagging. Consult your network administrator for details.
- Since an IP softphone is installed and operates on a PC, the PC must be connected to the LAN to use the IP softphone on the network.

The diagram below is for connecting an IP-PT to a switching hub. For SIP phones, refer to the documentation of your SIP phone.

Example: KX-NT346



Connecting an AC Adaptor to an IP Telephone

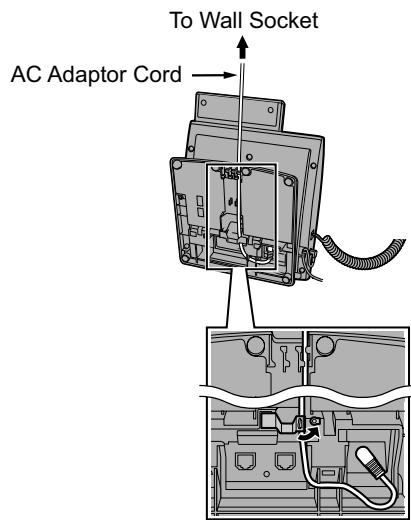
IP-PTs and some SIP phones comply with the IEEE 802.3af Power-over-Ethernet (PoE) standard. If PoE is available on your network, these IP telephones can receive the necessary power supply from the network through the network cable. In this case, no AC adaptor is needed for the IP telephones.

However, if PoE is not available, you will need to connect an AC adaptor to the IP telephone.

Note

Use only the specified type of AC adaptor for each IP telephone. For details, refer to the documentation of your IP telephone.

Example: KX-NT346



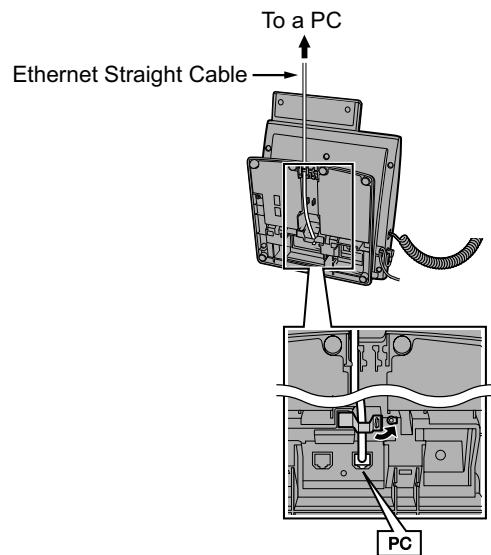
Connecting a PC to an IP Telephone

You can connect a PC to some IP telephones (e.g., KX-NT300 series) using the IP telephone's secondary port. In this case, only a single port from the LAN's network interface (switching hub) is required to connect both the IP telephone and PC to the LAN.

Note

- Use an Ethernet straight cable with an RJ45 connector to connect a PC to the IP telephone. The cable should be a CAT 5 (Category 5) or higher for 10BASE-T/100BASE-TX, or CAT 5e (Enhanced Category 5) or higher for 1000BASE-T.
- Only a PC can be connected to the secondary port of an IP telephone. Other IP telephones, including IP-PTs, or network devices such as routers or switching hubs, cannot be connected.
- The secondary port does not support PoE for connected devices.
- In cases where a PC is connected to the secondary port, if the IP telephone connection to the PBX is disconnected or reset, LAN communication to the PC will also be disrupted.
- Generally, it is recommended that you connect no more than one PC to the secondary port of each IP telephone.

Example: KX-NT346



4.12 Power Failure Ports

When the power supply to the PBX fails, power failure transfer (PFT) will switch from the current connection to the Power Failure Connection. Refer to "5.6.2 Power Failure Transfer" in the Feature Guide for further information.

For information about PFT for stacked PBXs, refer to the Installation Manual for each PBX.

Using SLC2/LCOT2 Card

In the event of a power failure, a specific SLT is automatically supplied power through the PFT port. The PFT ports are the SLC1 port and LCOT1 port on the SLC2/LCOT2 card.

Note

A trunk conversation established during power failure can be maintained even when the power returns and the connection is switched back to the normal configuration from the Power Failure Connection.

4.13 Starting the KX-NS1000

WARNING

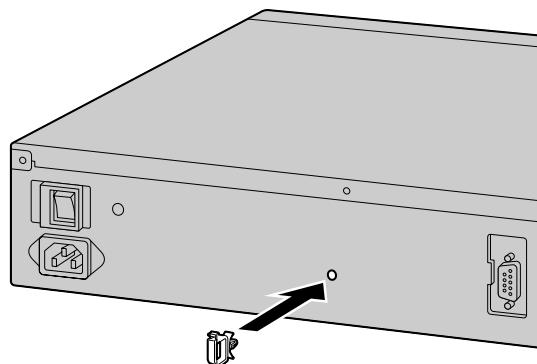
Make sure that the AC outlet is properly earthed, then securely connect the 3-pin AC plug including the earthed pin.

CAUTION

- Use only the AC power cord included with the PBX.
- Before touching the product (PBX, cards, etc.), discharge static electricity by touching ground or wearing an earthing strap. Failure to do so may cause the PBX to malfunction due to static electricity.
- Once you have started the PBX, if you unplug the PBX, do not initialise it again as described in "System Initialisation Procedure". Otherwise, your programmed data will be cleared. To restart the PBX, refer to "7.1.5 Restarting the KX-NS1000".
- The power supply cord is used as the main disconnect device. Ensure that the AC outlet is located near the equipment and is easily accessible.

Installing the Hook Clip for the AC Power Cord

1. Insert the hook clip into the hook clip hole.



Note

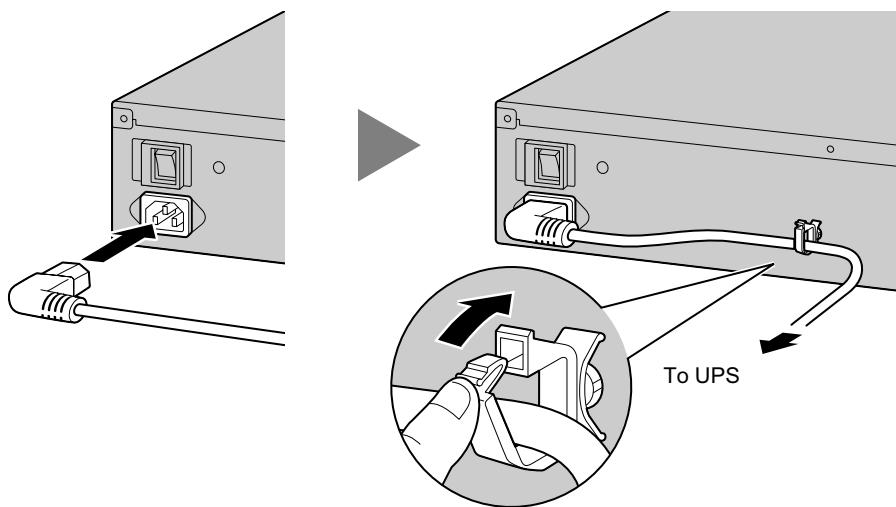
Use only the hook clip included with the PBX.

Connecting the AC Power Cord

1. Plug the AC power cord into the PBX and pass the cord through the hook clip as indicated. Push the hook clip in the direction of the arrow until it clicks.

Note

For safety reasons, do not stretch or pinch the AC power cord.



2. **When not using a UPS:**

Plug the other end of the cord into an AC outlet.

When using a UPS:

Plug the other end of the cord into the outlet of the UPS.

Connecting an Uninterruptible Power Supply (UPS)

A UPS can be connected to the PBX and it provides temporal power to the PBX in the event of a power failure. When using the recommended UPS (with a USB interface), the PBX can perform automatic shutdown when the UPS battery ratio is at a specified rate by sending a warning signal to the PBX through the USB port. Therefore, data loss or serious damage to the PBX caused by a sudden power cut can be prevented. After power is restored, turn off the PBX using the power switch first, and then turn the PBX back on before starting the PBX.

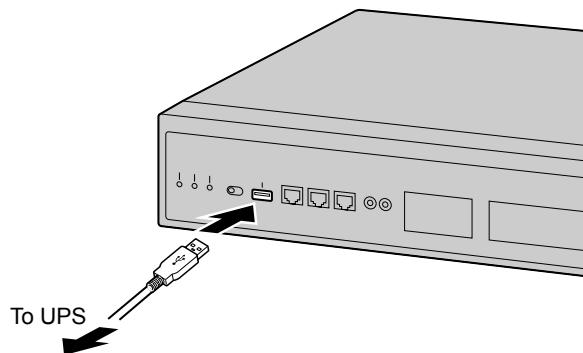
Note

- For details about using Web Maintenance Console to specify the UPS battery ratio to begin automatic shutdown, refer to "4.1.1 Status—Equipment Status—UPS" in the PC Programming Manual.
- For information about the installation of an UPS, refer to the documentation of your UPS.
- For information about the recommended UPS, ask your local Panasonic dealer.

1. Connect the UPS to the USB port of the PBX.

Note

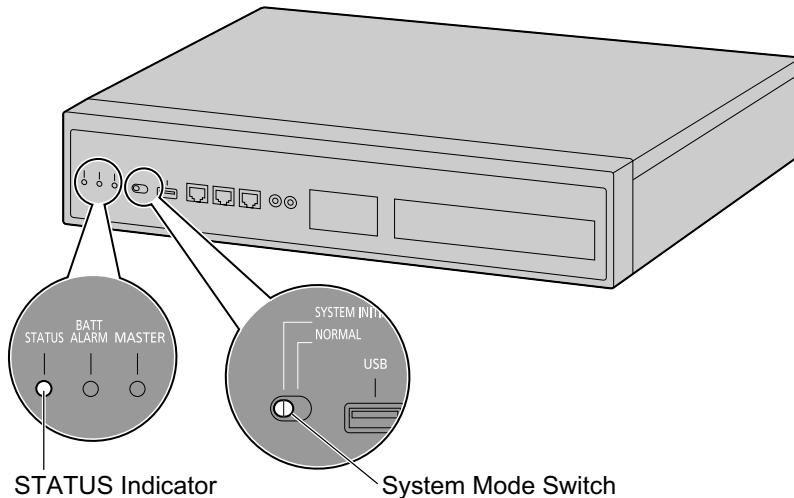
When connecting the UPS, use only the USB cable included with the UPS and do not use USB hubs to connect the UPS and the PBX.



2. Follow the instructions in the documentation of the UPS to setup and start the UPS.

System Initialisation Procedure

1. Slide the System Mode Switch to the "SYSTEM INITIALIZE" position.



2. Turn on the power switch of the PBX. The STATUS indicator will flash green.
3. While the STATUS indicator is flashing green, slide the System Mode Switch back to the "NORMAL" position. Depending on the configuration, initialisation takes about 2.5 minutes. If successfully executed, the STATUS indicator will stop flashing and remain lit up.

Note

When DSP card(s) are installed and a DHCP server is not connected, each installed DSP card cannot acquire an IP address, and the STATUS indicator will turn red.

All data, except for system prompts and activation key files, will be erased. Data that is erased includes Unified Messaging data, call logs, etc. The settings for the PBX as well as all optional service cards will be initialised to their default values.

Note

- After the PBX is initialised, you can restore system data to the PBX that has been backed up earlier. For details about backing up and restoring system data, refer to "6.1 Tool—System Data Backup", "7.2.2 Utility—File—File Transfer PBX to PC" and "7.2.1 Utility—File—File Transfer PC to PBX" in the PC Programming Manual.
- After the PBX is initialised, you must set up the mandatory settings required for both stand-alone PBXs and PBXs in a One-look network with Easy Setup Wizard. For details refer to "Connecting to Web Maintenance Console" and "5.4.1 Easy Setup Wizard".
- When a UPS is connected, make sure it is started as instructed in the documentation for the UPS.

Confirming the Trunk Connection

After the SLC2/LCOT2 card is installed, programme the PBX and connect trunks to the PBX. If SLC2/LCOT2 card is not installed, this confirmation can be skipped.

To confirm that the trunks are successfully connected, dial [×] [3] [7] + trunk number (3 digits) on an IP telephone, or press the IP telephone's S-CO button. You will hear a dial tone if the trunk is available and connected.

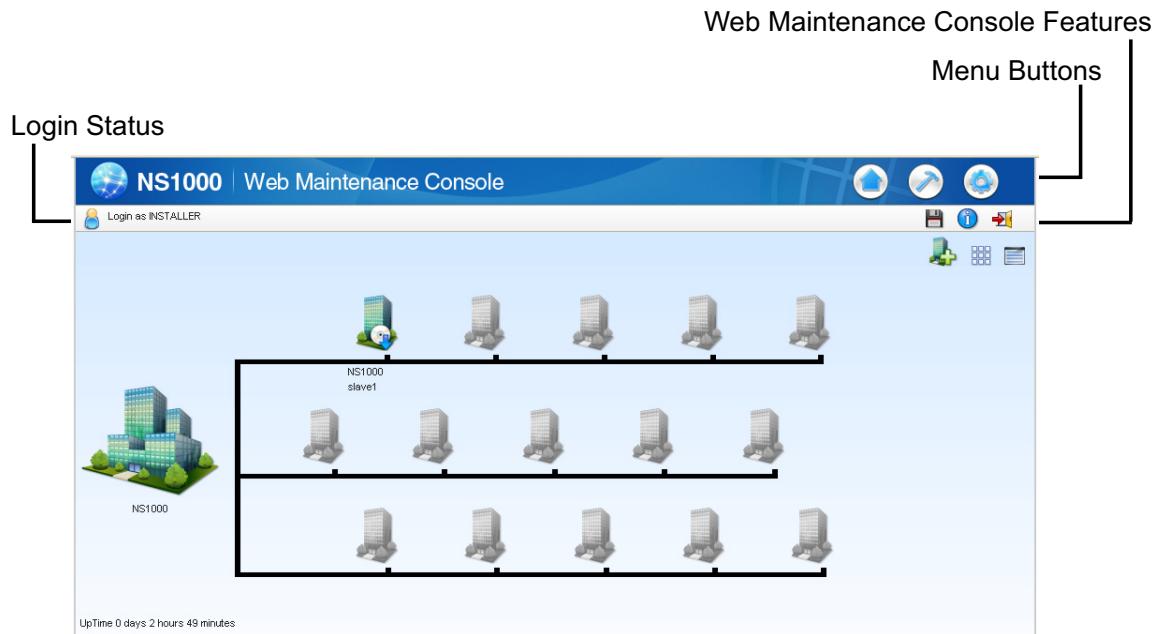
Section 5

Programming Information

This section describes the installation procedure, structure, and functions of the Web Maintenance Console for programming IP telephones and the PBX. Further information on programming the PBX for use with SIP trunks and a VoIP network is included.

5.1 Overview of Web Maintenance Console

Web Maintenance Console is designed to serve as an overall system programming reference for the PBX. You can programme and control the PBX over an IP network using Web Maintenance Console. This section describes programming basic items using Web Maintenance Console.



Note

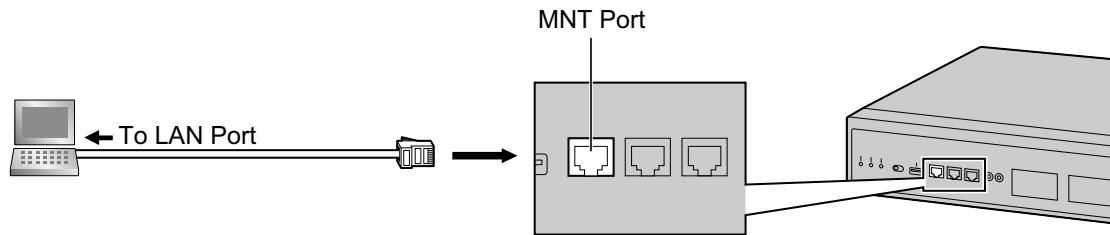
The contents and design of the software are subject to change without notice.

5.2 PC Connection

KX-NS1000 has 3 physical ports for PC and LAN connections. A default IP address is assigned to each port. A PC connect to the PBX either directly or over a LAN using the appropriate method for the port being used.

Port	Default IP Address	Default Subnet Mask
MNT Port	223.0.0.1	
LAN Port	192.168.0.101	255.255.255.0

Direct Connection



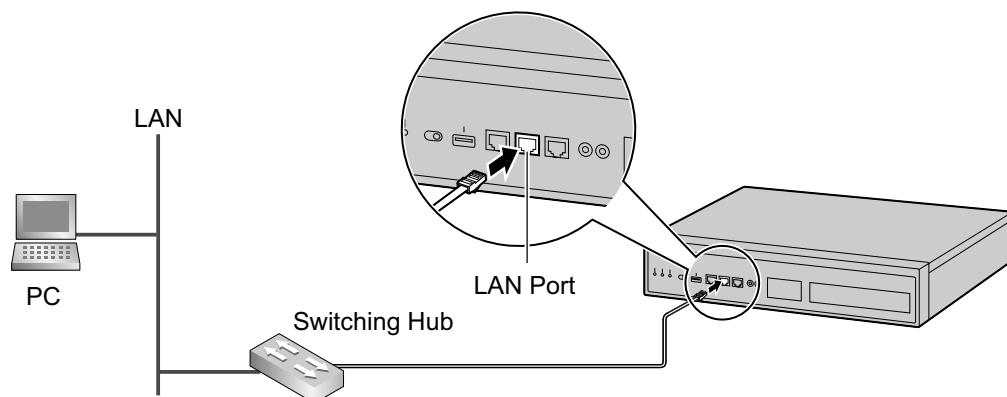
Notice

When connecting the PC to the MNT port, if the PC is set to obtain the IP address automatically, the IP address of the PC will be set to an appropriate IP address to establish a connection to the PBX.

Note

- Use an Ethernet cable with an RJ45 connector to connect a PC to the PBX.
- For pin assignments and maximum cabling distance, refer to "4.10 Connection of Peripherals".

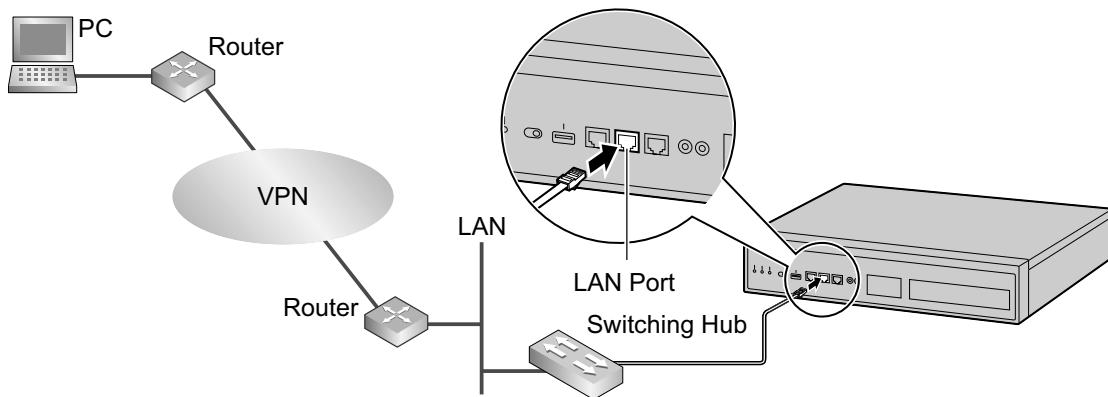
Connection via LAN



Note

For details about connecting a switching hub to the PBX, refer to "4.11.1 LAN Connection for the Main Unit".

Connection via Virtual Private Network (VPN)



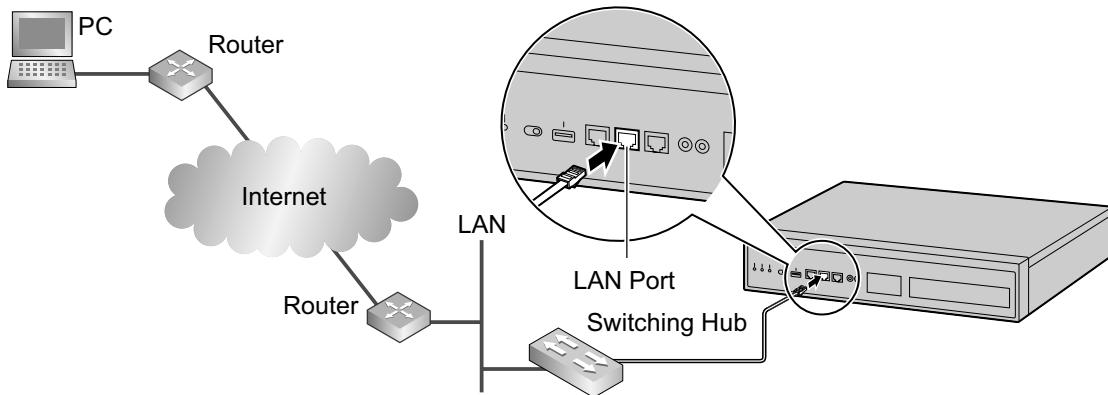
Notice

To access the PBX via VPN, the PC must be in the same VPN.

Note

For details about connecting a switching hub to the PBX, refer to "4.11.1 LAN Connection for the Main Unit".

Connection via Internet



CAUTION

It is strongly recommended to use SSL encrypted communication when the PC is accessing the PBX via the Internet. To use SSL encryption, routers must have a port set up for https communication.

Notice

To access the PBX via the internet, routers must have static NAT/NAPT settings (Port forwarding) enabled.

Note

For details about connecting a switching hub to the PBX, refer to "4.11.1 LAN Connection for the Main Unit".

5.3 Starting Web Maintenance Console

System Requirements

Required Operating System

- Microsoft® Windows® XP, Windows Vista® Business, Windows 7, Windows 8 or Windows 8 Professional operating system

Note

In Windows 8 and Windows 8 Professional, Web Maintenance Console runs only in desktop mode. It is not available from the Windows 8 Start screen.

Recommended Display Settings

- Screen resolution: XGA (1024 × 768)
- DPI setting: Normal size (96 DPI)

Supported Browsers for use with Web Maintenance Console

- Windows Internet Explorer® 8
- Windows Internet Explorer 9
- Windows Internet Explorer 10¹
- Mozilla® Firefox® version 6 or later

¹ 64-bit Enhanced Protected Mode (EPM) is not supported.

Note

Always be sure to apply the latest updates to your Web browser software. For details, refer to your Web browser's documentation. Only the browsers and browser versions listed above are supported for use with Web Maintenance Console.

Copyright for MD5

This software uses the Source Code of RSA Data Security, Inc. described in the RFC1321 (MD5 Message-Digest Algorithm).

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

Licence to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

Licence is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

Password Security

CAUTION

To the Administrator or Installer regarding the system password

1. Please provide all system passwords to the customer.

2. To avoid unauthorised access and possible abuse of the PBX, keep the passwords secret, and inform the customer of the importance of the passwords, and the possible dangers if they become known to others.
3. The PBX has default passwords preset. For security, change these passwords the first time that you programme the PBX.
4. Change the passwords periodically.
5. It is strongly recommended that passwords of 10 numbers or characters be used for maximum protection against unauthorised access. For a list of numbers and characters that can be used in system passwords, refer to "1.1.3 Entering Characters" in the PC Programming Manual.

Connecting to Web Maintenance Console

1. Connect the PC to the PBX:
 - Connect the PBX to a PC with the MNT port and access the PBX directly from the PC. For details, refer to "Direct Connection" in "5.2 PC Connection".
 - Connect the PBX to a network with the LAN port and access the PBX from a PC in your LAN or VPN. For details, refer to "Connection via LAN", "Connection via Virtual Private Network (VPN)" and "4.11.1 LAN Connection for the Main Unit".
 - Connect the PBX to a network with the LAN port and access the PBX from a PC using an Internet connection. For details, refer to "Connection via Internet" and "4.11.1 LAN Connection for the Main Unit".
2. Access Web Maintenance Console:

MNT Port Connection:

Launch your Web browser and in the address bar, enter one of the following addresses exactly as shown:

– **223.0.0.1**

or

– **http://kx-ns1000.**

Note

- If entering "**http://kx-ns1000.**", be sure to include the period at the end as shown.
- When connecting to the MNT port for more than 24 hours, the "Operation Failed" error occurs. In this case, log in to Web Maintenance Console again.
- The default subnet mask for the MNT port is 255.255.255.0.
- If connecting using 223.0.0.1 takes a long time, configure a static IP address for the PC.

LAN or VPN Connection:

Launch your Web browser and input the IP address of the PBX followed by the Web Maintenance Console port number into the address bar. The input method will differ according to the PC's connection to the PBX. The default IP address for the LAN port of the PBX is 192.168.0.101, and the default Web Maintenance Console port number is 80. Accordingly, the address to enter to connect to the PBX for the first time will be as follows (enter the address exactly as shown):

http://192.168.0.101

Note

The default subnet mask for the LAN port is 255.255.255.0.

Internet Connection (SSL Connection):

When the PC is accessing the PBX from a connection over the internet, the use of SSL is strongly recommended. When using an SSL encrypted connection, the default port is 443. The format of the address to enter to connect to the PBX using an SSL encrypted connection will be as follows:

https://xxx.xxx.xxx.xxx:yyy

- "**xxx.xxx.xxx.xxx**" is the IP address of a device that can be accessed from the Internet, such as the IP address of a network router.
- "**yyy**" is a port number. The network router's port forwarding settings must be configured so that traffic arriving at port "yyy" is forwarded to the correct IP address and port of the PBX in the LAN.
- Port forwarding settings must specify the IP address and the port number of the network router ("**xxx.xxx.xxx.xxx:yyy**") to transfer the packets to the PBX in the LAN, so that the packets sent to the global IP address and specified port of the router will be transferred to the IP address and specified port of the PBX in the LAN.
- Note the usage of "https" instead of "http".
- If you connect to Web Maintenance Console using SSL, a security alert window is displayed. Follow the prompts to install a security certificate. The procedure may vary according to your browser.

Note

The IP address and Web Maintenance Console port number for the PBX can be changed from their default values. If settings for the LAN port's IP address or port number has been forgotten, connect using the MNT port connection as described above and confirm the LAN port's IP address in "28.1 Network Service—[1] IP Address/Ports—Basic Settings", and the port in "28.2.3 Network Service—[2-4] Server Feature—HTTP" in the PC Programming Manual.

3. The Web Maintenance Console login screen is displayed. Log in with the Installer level account name and the default Installer level account password to launch the Easy Setup Wizard. For details about the Easy Setup Wizard, see "5.4.1 Easy Setup Wizard".

Using Web Maintenance Console in Off-line Mode

You can connect a PC to the PBX to programme the PBX using Web Maintenance Console (On-line mode), or you can programme the PBX without connecting the PC to the PBX (Off-line mode).

Off-line mode programming is performed using the Off-line version of Web Maintenance Console, which you install on your PC. The changes made during Off-line mode are saved as local data on the PC, and then later uploaded to the PBX.

The following procedures outline how to install the Web Maintenance Console for Off-line mode programming.

Installation

Note

- Be sure to install the latest version of Off-line WEB-Maintenance Console.
- Before beginning the installation of Off-line Web Maintenance Console, the following software must be installed on the PC:
 - Microsoft .NET Framework 2.0
 - Microsoft .NET Framework 4
 This software can be downloaded from Microsoft's online Download Centre.
- To install or uninstall the software on a PC running Windows XP Professional, you must be logged in as a user in either the "Administrators" or "Power Users" group.
- To install or uninstall the software on a PC running Windows Vista Business, Windows 7, Windows 8 or Windows 8 Professional, you must be logged in as a user in the "Administrators" group.

1. Copy the Off-line WEB-Maintenance Console setup file to your PC.
2. Double-click the setup file to run the installer.
3. Follow the on-screen instructions provided by the installation wizard.

Note

For information about programming the PBX in Off-line mode, refer to the PC Programming Manual.

Converting KX-TDE, KX-NCP or KX-TDA100D System Data for Use with the KX-NS1000

System data from a KX-TDE series, KX-NCP series or KX-TDA100D PBX can be converted for use with the KX-NS1000 to ensure a seamless transition to the new system.

1. Connect a PC to a KX-TDE series, KX-NCP series or KX-TDA100D PBX and then start the Unified Maintenance Console.
For details about connecting a PC to a PBX or for details about the Unified Maintenance Console, refer to the appropriate documentation.
2. In the Unified Maintenance Console, save the PBX's system data file (DxSYS¹) to the PC.²
For details about saving the system data file to the PC, refer to the appropriate documentation.
3. Start Web Maintenance Console for the KX-NS1000 in Off-line mode.
4. In the Programme Launcher, click **Database Converter**.
5. Select the appropriate option according to whether a legacy gateway is connected.
6. In **Select Original File Name**, select the system file (DxSYS) you saved in step 2 as the file to convert.
An image of converting the file to the KX-NS1000 is displayed on the screen.
7. Click "Next". The Easy Setup Wizard starts as it would for a normal setup of the KX-NS1000.
8. Specify the following Master site parameters as necessary:
 - Location Setting
 - PBX Setting
 - LAN Setting
 - WAN Setting
 - Registration Setting
 - SNTP / Daylight Saving
 - Maintenance Setting

This tool displays a "stacking style" image on the screen as necessary (e.g. when converting KX-TDE600/KX-TDE620 data to KX-NS1000 data).

The system data will be converted and a system data file for the KX-NS1000 (DCSYS) is created. It will complete within one minute.

9. After conversion is complete, you can click **Save** on the Result of Converting screen and save the results file (ConvertReport.txt) to your PC.
10. On the Save Convert File of System Data screen, save the created DCSYS file.
11. Select **Finish of Database Conversion**, and then click **OK**.
Conversion is complete.
12. Start Web Maintenance Console, and click **Open -Offline Mode** in the Programme Launcher.
13. Select the created DCSYS file, and configure any additional required parameters.
For details about the parameters, refer to the PC Programming Manual.
14. Start the KX-NS1000, and then transfer the system data file (DCSYS) to the PBX.
For details about transferring the file, refer to "1.2.2 PC Programming Using Off-line Mode—Uploading Programmed Settings to the PBX" in the PC Programming Manual.

¹ "DxSYS" refers to the following:

- KX-NCP500/KX-NCP1000: DBSYS
- KX-TDE100/KX-TDE200: DMSYS
- KX-TDA100D: DDSYS
- KX-TDE600: DGSYS

² The software version for KX-TDE series, KX-NCP series or KX-TDA100D PBXs must meet the latest version requirements shown in the Data Converter tool. If the requirements are not met, you must use the Unified Maintenance Console to upgrade the version to the one shown in the table below, and then save the DxSYS file.

Notice

- Activation keys are not brought over during data conversion. You must supply the necessary activation keys for the KX-NS1000 separately.

- The following numbering plan settings are brought over during data conversion: Feature Numbers, Other PBX Number, Extension Number, Quick Dial Number
- Data conversion does not support system data from KX-TDA series PBXs. To convert KX-TDA data, first convert it to KX-TDE data using the PBX Replacement of Unified Maintenance Console and then convert that data to KX-NS1000 data.
- Data for cards that are supported in legacy gateways connected to the KX-NS1000 can be converted from KX-TDE series and KX-NCP series PBXs.
- Data for IP-EXT16 cards in a KX-TDE series or KX-NCP series PBX will be converted for use with a V-IPEXT32 card in the KX-NS1000. IP-PTs that had been connected to the IP-EXT16 card must be registered again to the V-IPEXT32 card in the KX-NS1000.
- PBX voice data (e.g., ESVM, SVM, OGM) is not converted.
- Data conversion for a SLC/LCOT/BRI card in the KX-NS1000 is not supported; the number of ports in these cards is too small.
- After conversion, if CSs are connected to both Slave units and the Master unit, you must change the settings so that all CSs are connected to the Master Unit.
- Data that is not supported by the data conversion is shown in the following table.

Unsupported Item	Default Setting
Time Mode	
Current time mode	Location setting default
Time mode switching time (manual mode)	Not Stored
Wired/Wireless extensions	
Timed Reminder	Not set
Station Lock	Unlocked
Remote Station Lock	Unlocked
Extension Call Charge Total	Total cleared
Not Ready/Ready (Wrap-up)	Wrap-up status cleared
LCS On/Off	Location setting default
Room Status (Check In/Check out/Not Ready/ Cleaned Up)	Location setting default
Auto Answer	Location setting default
Absent Message Status	Not set
Saved Number Redial	Number cleared
ICD Group Login Status (Login/Logout)	Location setting default
Message Waiting	Cancelled
Incoming Log	Cleared
Outgoing Log	Cleared
TAM Log	Cleared
Personal Absent Message	Message cleared

Unsupported Item	Default Setting
FWD/DND setting status (intercom/outside calls)	Setting Cancelled
Monitor PBX ID	Cleared
Trunk	
Call Charge Total	Total cleared
Traffic Data	Cleared
Incoming Call Group	
Message Waiting	Cancelled
Incoming Log	Cleared
FWD/DND setting status (FWD/DND set or not)	Setting cancelled
Traffic Data	Cleared
Verification Code Information	
Verification Code Password, Lock Status	Unlocked
Verification Code Password, Lock Counter	Counter cleared
Call Charge Total	Total cleared
Cabinet Information	
Incoming Log	Cleared
Outgoing Log	Cleared
Line Error Log	Cleared
MPR-LPR Call Data Log	Cleared
System Information	
Password, Lock Counter for Remote Programming	Counter cleared
Major/Minor Error	Cleared
Timed Reminder (Wake-up Call)	Cancelled

Converting System Component Type

When starting the KX-NS1000, you can specify **System Capacity Selection** in Easy Setup. (For details about Easy Setup, refer to "5.4.1 Easy Setup Wizard".)

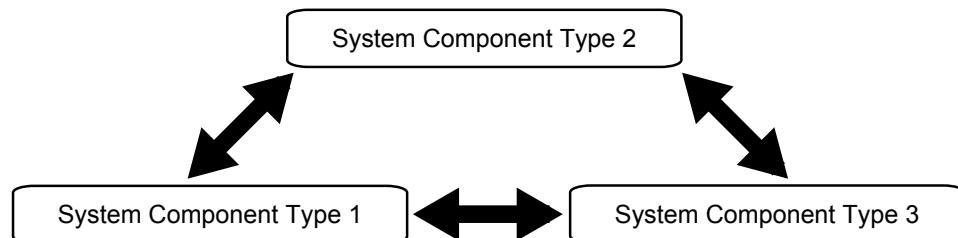
The system capacity changes according to the value you select for **System Capacity Selection**. (For details about system capacity, refer to "2.3.3 System Capacity".)

In this manual, we define the "system component type" in relation to **System Capacity Selection** as follows.

System Component Type	System Capacity Selection
Type 1	Standard Type
Type 2	IP-Extension Type
Type 3	System Resource Type

System data can be converted between different system component types using Web Maintenance Console (off-line mode).

This procedure is applicable to both minor software updates (e.g., 003.00000 → 003.10000) and major software updates (e.g., 002.30000 → 003.00000). When upgrading from a version prior to 003.00000, you must select **Standard Type** for **System Capacity Selection**.



However, there are certain conditions regarding data conversion, since system capacity differs between the component types.

For details about the conditions, refer to "Conditions" in this section.

Parts of the system data are inherited, increased, or discarded under the regulations.

To convert between system component types

1. Start Web Maintenance Console (Off-line mode).
2. Click **Open -Offline Mode**.
3. Click **Browse** to select the system data file.
4. Select one of the following options for **Select the System Capacity Type**.
 - **Standard Type**
 - **IP-Extension Type**
 - **System Resource Type**

Click **OK**. The system data will be converted.

Note

This step is available only when **System Capacity Selection** setting is enabled.

5. Save the system data file to the local PC.
6. Slide the System Mode Switch to the "SYSTEM INITIALIZE" position.
7. Restart the KX-NS1000. For details about restarting the PBX, refer to "7.1.5 Restarting the KX-NS1000".
8. In Easy Setup, select a value for **Select the System Capacity Type** under **System Capacity Selection**.

Note

The system component type selected in this step will be over-written with the following steps.

9. After Easy Setup is complete, click **Utility** → **File** → **File Transfer PC to PBX**.
10. Select the local file that you saved in step 5, and then click **Execute**.
11. Click **System Control** → **System Reset**.

12. Click **Skip**.

13. Click **OK**.

14. Click **OK**.

Conditions

[Rules for data conversion]

The following table shows the rules for converting system data to a different type.

Condition	Rule
Components will increase	Copy information for inherited components. Set default value for added components.
Components will decrease	Copy information for inherited components. Delete information for discarded components.
Components are same	Copy information for all the components.
Parameters in components will increase	Copy information for inherited parameters. Set default value for added parameters.
Parameters in components will decrease	Copy information for inherited parameters. Delete information for discarded parameters.
Parameters in components are same	Copy information for all the parameters.

"Components" refers to the PBX's physical cards, virtual cards, etc. If the system component type is different from before the conversion, the number of components will be increased, decreased or inherited.

The following table gives an example:

Component	Maximum Cards in 1 Unit			Change in components after conversion					
				Type 1 →		Type 2 →		Type 3 →	
	Type 1	Type 2	Type 3	Type 2	Type 3	Type 1	Type 3	Type 1	Type 2
V-SIPGW16	16	16	10	Same	Decrease	Same	Decrease	Increase	Increase
V-IPGW16	3	3	6	Same	Increase	Same	Increase	Decrease	Decrease
V-IPEXT32	8	20	8	Increase	Same	Decrease	Decrease	Same	Increase
V-SIPEXT32	20	8	12	Decrease	Decrease	Increase	Increase	Increase	Decrease
V-UTEXT32	20	8	12	Decrease	Decrease	Increase	Increase	Increase	Decrease

[Exchanging cards]

- During system data conversion, if the number of optional physical service cards exceeds the maximum number of allowed by the selected system components type, information for the cards exceeding the limit (including extension numbers and trunk numbers) is discarded.

At this time, any data related to the discarded card is processed in the same way as when an optional card is deleted using the normal procedure (e.g., if the extension number is registered as a member of an incoming call group, the extension number will not be deleted from the group).

- Converting virtual card information from data (Type 1) to Type 2 or 3 is processed according to the following order of priority:
 - V-IPEXT32 → V-SIPEXT32 → V-UTEXT32
- You can decide whether to replace a discarded extension card with an alternate extension card during the conversion. If you use an alternate extension card, you can also specify the card type.
- The alternate extension card can inherit the information of each extension registered to the discarded card. However, data specific to the discarded card's type (e.g., port settings for the discarded card) cannot be inherited.

[Data related to Tenant Numbers]

- During system data conversion from system component type 3 to system component type 1 or 2, information for the following data is deleted, due to a decrease in the number of tenants.
 - Time Service Mode¹
 - Music On Hold¹
 - Operator (Extension Number)¹
 - ARS Mode¹
 - Authorisation Code for Tenant²

¹ Refer to "14.6 PBX Configuration—[6-6] Feature—Tenant" in the PC Programming Manual.

² Refer to "16.5 PBX Configuration—[8-5] ARS—Carrier—Authorisation Code for Tenant" in the PC Programming Manual.

[Conversion of System Speed Dialling]

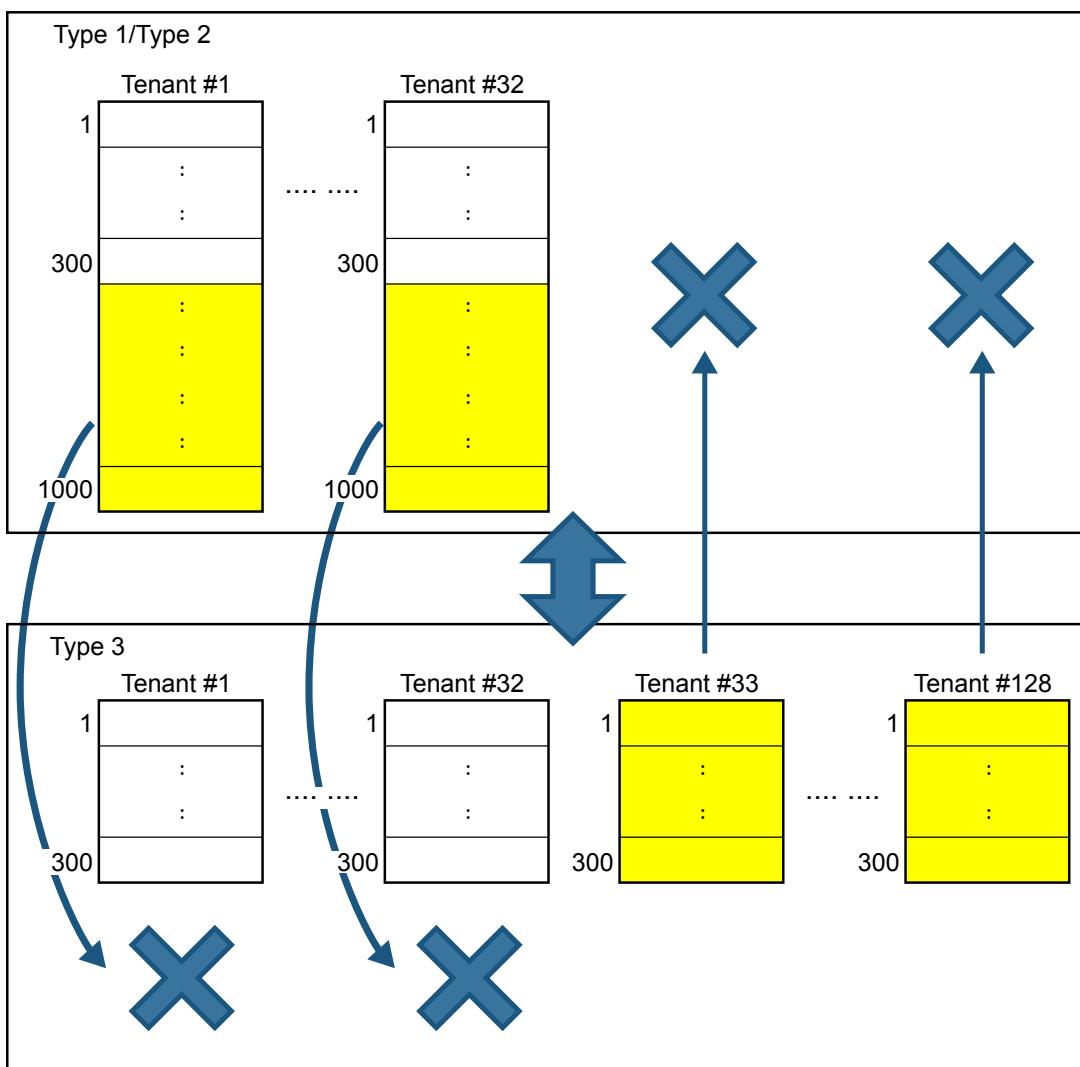
- During system data conversion from system component type 1 or 2 to system component type 3, the number of tenants increases, but some system data is deleted.

Therefore, data conversion proceeds as follows:

- 1. Basic Memory** for systems is inherited regardless of the change to the system component type.
- System data for each tenant is converted according to the following table.

System Component Type 1/ System Component Type 2	System Component Type 3
Tenant 1–32: System speed dial entries 1–300	Tenant 1–32: System speed dial entries 1–300
Tenant 1–32: System speed dial entries 301–600	None
Tenant 1–32: System speed dial entries 601–900	None
Tenant 1–32: System speed dial entries 901–1000	None
None	Tenant 33–128: System speed dial entries 1–300

System data for system speed dial entries 301–1000 of tenants 1–32 is deleted when system component type 1 or 2 data is converted to system component type 3.



KX-TVM System Prompt and Mailbox Data Import

Voice data recorded by users in a KX-TVM series VPS can be converted and used as voice data in the KX-NS1000's Unified Messaging system. System prompts, mailbox prompts, and mailbox messages can be converted.

Condition:

- The required software versions are as follows:
 - KX-TVM series: version 1.0 or later
 - KX-NS1000: version 2.1 or later

Notice

- Only data recorded by users can be imported; the preinstalled guidance data will not be imported.
- The language set for the KX-TVM series VPS must be set as the language for the Unified Message system where the voice data will be imported. If the language is different, the data cannot be imported.

- The following content of KX-TVM mailbox's audio data is not restored as the Unified Messaging system Mailbox data.
 - Receive message: Mailbox number of Recorder
 - Transfer message: Mailbox number of Recorder/Sender
 - Confirmation of hearing a message: Mailbox number of the responder
In this case, the message is treated as if it were recorded by a non-subscriber.
 - Mailbox number of Recorder/Sender/Responder is not announced in restored audio data.
 - When IMAP integration is used, "Unknown Caller" is shown in the "From" field.
- Connect a PC to the KX-TVM series VPS, and then start the KX-TVM Maintenance Console.
For details about connecting a PC to the VPS or about the Maintenance Console, refer to the appropriate documentation.
 - In Maintenance Console, back up the voice data on the KX-TVM series VPS to the PC.
For details about backing up KX-TVM VPS voice data, refer to the documentation of the corresponding VPS.
 - Start the KX-NS1000, and then start Web Maintenance Console.
 - Navigate to Maintenance → Tool → 10. UM data restore, and then select the types of voice data you want to restore. You can select the following types of data:
 - System prompts
 - For batch restore
Under System Prompts, select the System Prompts check box.
Condition:
The Unified Messaging system has only 8 system prompts, which is less than the number on KX-TVM VPSs. If you restore system prompts, Prompt 9 and Prompt 10 on the KX-TVM VPS will not be restored. To import Prompt 9 and Prompt 10 to the Unified Messaging system, they must be restored individually.
 - For individual restore
You can select the voice data to restore one at a time as necessary.
 - Installed Prompts – Prompt 1 to 8
 - Custom Service Menu
 - Company Name
 - Company Greeting
 - System Mailbox Group Voice Label
 - System Caller Name
 - Prompt Selection
 - Hold Announce Menu
 - Mailbox Prompts and Mailbox Messages
 - For batch restore
Under Mailbox Prompts, select the Mailbox Prompts check box, and then select the Mailbox Messages check box.
 - For individual restore
You can select the voice data to restore one at a time as necessary.
 - Owner Name
 - Personal Greetings
 - Personal Caller ID Name
 - Interview
 - Personal Group List Name
 - EMD List Member Name
 - Mailbox Messages
 - Select a file from **Local PC, USB Flash Drive (Main Unit)**, or **NAS** to restore, and the folder selection menu becomes active.
Specify the folder where the backup data is saved, and then click **OK**.
The selected voice data will be imported.

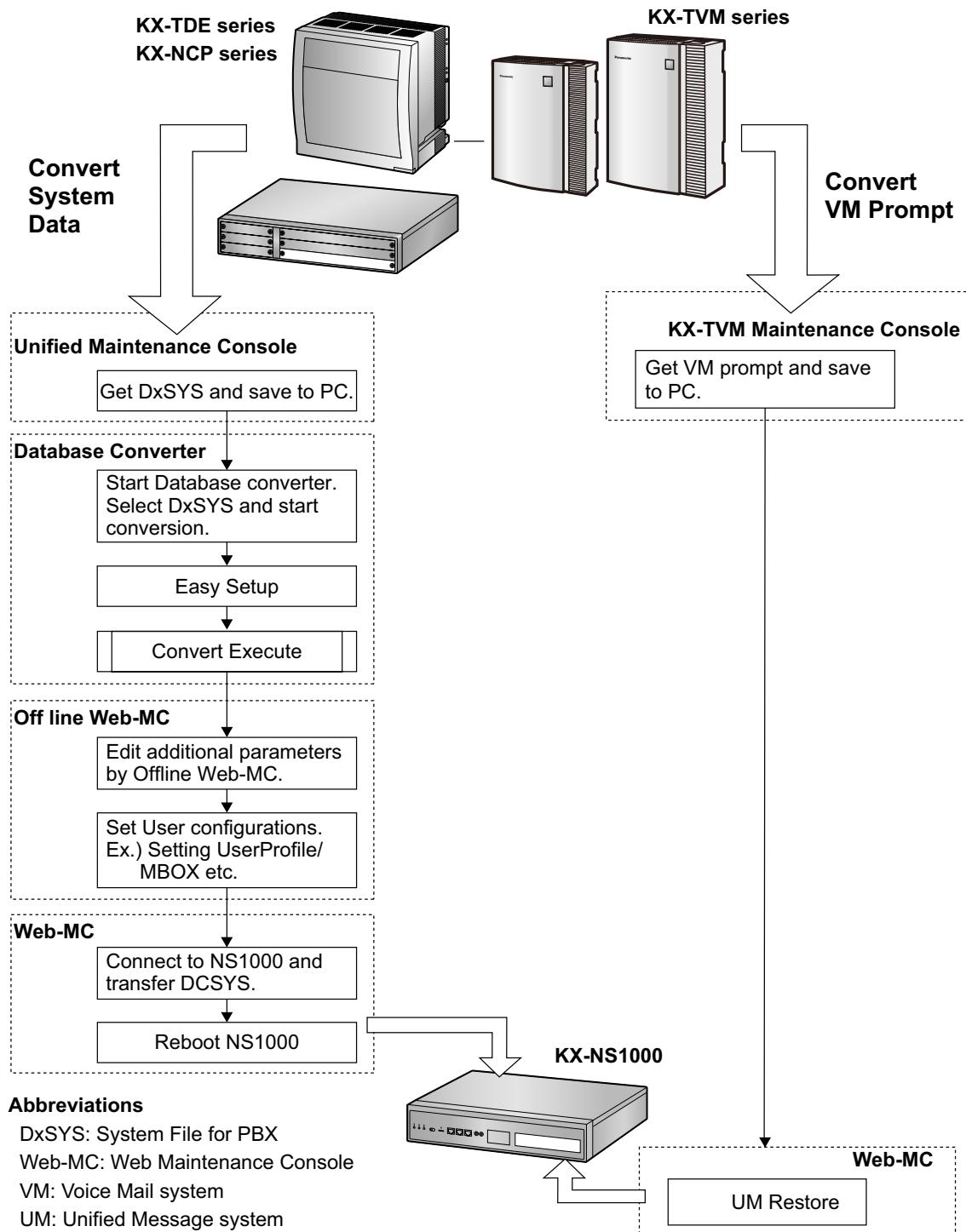
Note

- When using a NAS, ensure that you have sufficient network bandwidth.

6. The import results will be saved in a file called "UM_data_restore_result.txt".

Notice

- It is possible that passwords are set on KX-TVM and Unified Messaging mailboxes. If the passwords for KX-TVM mailboxes are different from the Unified Messaging mailbox passwords, and data is being restored (imported) individually, you will be prompted for the password of the Unified Messaging mailbox. If password authentication fails 3 times, the voice data for that mailbox will not be imported.
- If you are not prompted for mailbox passwords during the restore, the password set for the mailbox in the Unified Messaging system will be used. When **Default Password for New Mailboxes** is enabled, the default password will be set for each mailbox. When **Default Password for New Mailboxes** is disabled, the default "1111" will be set for each mailbox.



5.4 Programming the PBX

5.4.1 Easy Setup Wizard

In the Easy Setup Wizard, you will set up the mandatory settings required for the PBX.

When you log in to Web Maintenance Console for a PBX that is in its initialised, factory default state, the Easy Setup Wizard for that PBX will launch automatically. You must log in using the Installer level account name and password.

- The Installer level account name is "INSTALLER".
- The default Installer level account password is "1234".

1. After Easy Setup Wizard launches, select a language, and then click **Install**.

2. In **Location Setting**:

a. Select a **PBX Type**:

- **Master**: Select for a PBX that will be registered as the Master unit of One-look network. Also select for a stand-alone PBX that will not be used in a One-look network.
- **Slave**: Select for a PBX that will be registered as a Slave unit of a One-look network. If **Slave** is selected, go to step **2-d** below.

Note

If the Master unit is located on a different LAN than the Slave unit being registered, the Slave unit will not be able to automatically detect the Master unit for registration. The IP address of the Master unit must be specified. Enter the IP address of the Master unit in **If located on different network from Master PBX**.

b. Select a **Suffix Code**¹ from the drop-down list if **Master** is selected for **PBX Type**.

c. Select an **Area**¹ from the drop-down list if **Master** is selected for **PBX Type**.

d. Click **Next**.

Note

If **Suffix Code** is changed from its default value, a notice about restarting the PBX is displayed. Click **OK** to restart the PBX. After the PBX restarts, start Web Maintenance Console again (refer to "Connecting to Web Maintenance Console" in "5.3 Starting Web Maintenance Console"). When you start the Easy Setup Wizard again, you will start from step **3**, below.

¹ For information about Suffix Codes and Areas to select, refer to "9.1 PBX Region Suffix Codes and Areas".

3. In **PBX Setting**:

a. Specify a **Site name** if **Master** was selected for **PBX Type** in step **2**.

b. Select a **Time Zone** from the drop-down list.

c. Click the **Local Time** box and select the date and time from the menu.

d. Select one of the following options for Default value of Numbering Plan:

- 3 digits Extension Number (This type is recommended for under 8 sites)
- 4 digits Extension Number
- 3 digits Extension, 4 digits DISA & UM channel

Note

Depending on the value selected above, the numbering plan of the PBX will vary as follows. Be aware that the default values for floating extension numbers and the number of available UM groups are different.

	3 digits Extension Number	4 digits Extension Number	3 digits Extension, 4 digits DISA & UM channel
Number of UM Group	8	16	9
Extension Number	101-xxx	1001-xxxx	101-xxx
Floating Extension Number			
UM Group	500-507	5000-5015	500-508
DISA (1-64)	536-599	5801-5864	5801-5864
TAFAS (Pager)	600	6000	600
ICD Group (1-64)	601-664	6001-6064	601-664
UM Channel (1-2)	508, 509	5101, 5102	5101, 5102
FAX Channel	510	5103	5103

- e. Select one of the following options for **System Capacity Selection**.
 - **Standard Type**
 - **IP-Extension Type**
 - **System Resource Type**
- f. Click the **IP Extension Setting** button on the Master site to configure an IP extension. For details, refer to the following instructions.

Note

- You cannot configure IP extensions for Slave units.
 - The following items can be configured. Click **OK** when you have finished.
- <IP Extension Setting>**
Specify a number for each category in **Number of IP Extensions**
- **IP-PT for V-IPEXT32**
 - **UT/UDT for V-UTEXT32**
 - **SIP-Phone for V-SIPEXT32**

- g. Click the **SIP Trunk Setting** button on the master site to configure a SIP Trunk. For details, refer to the following instructions.

Note

- You cannot configure SIP trunks for Slave units.
 - The following items can be configured. Click **OK** when you have finished.
- <SIP Trunk Setting>**
Configure the following items for **1st Account Setting / 2nd Account Setting**
- **Number of SIP Trunk**
 - **User Name (64 characters)**
 - **Authentication ID (64 characters)**
 - **Authentication Password (32 characters)**
 - **SIP Server Name / Outbound Proxy Name (Max.100 characters)**
 - **SIP Server IP Address**
 - **SIP Server Domain / Proxy Domain (Max.100 characters)**

h. Click **Next**.

Note

- The value you select for **Default value of Numbering Plan** affects the default values for certain settings, such as floating extension numbers, and has a large effect on the system. Select this value with care. For details about the default values that are affected, refer to step 3 in this procedure.
- The value you select for **System Capacity Selection** determines the maximum numbers of virtual trunk slots and virtual extension slots, and has a large effect on the system. Select this value with care. For details about the number of virtual trunk slots and virtual extension slots, refer to "2.3.3 System Capacity".

4. In **LAN Setting**, the IP addresses for the PBX, DNS server, and DSP cards can be assigned automatically through a DHCP server or entered manually.

When using a DHCP server:

- a. Select **Obtain an IP address automatically**.
- b. Select **Obtain DNS server address automatically**.
- c. Select **Obtain DSP IP address automatically**.

Notice

The boxes will turn grey and the IP address information will be assigned automatically.
Write down the address information assigned to the PBX for future reference.

d. Click **Next**.

When not using a DHCP server:

- a. Select **Use the following IP address**.
- b. Enter an IP address¹, Subnet Mask², and Default Gateway¹. (The default gateway may not need to be specified depending on your network configuration.)
- c. Select **Use the following DNS server address**.
- d. Enter the preferred and alternative DNS IP addresses¹.
- e. Select **Use the following DSP IP address**.
- f. Enter up to 2 IP addresses¹ for each installed DSP card.
- g. Click **Next**.

¹ Valid IP address range: "1.0.0.0" to "223.255.255.255"

² Valid subnet mask address range: "0–255.0–255.0–255.0–255" (except "0.0.0.0" and "255.255.255.255")

5. In **WAN Setting**, you can select whether to use the built-in router and an IPsec (VPN) connection for inter-site communication. If you use the built-in router, additional settings such as IP addresses are required.

For details about the built-in router, refer to "8.6 Built-in Router".

When using the built-in router and IPsec (VPN) connection:

- a. In **Built-in Router**, select **Active (Trial Activation Key)**.

Note

- The built-in router will operate until the trial activation key expires. To continue using the built-in router feature, the built-in router activation key (KX-NSN101) is required.
- b. In **Connection Mode**, select a connection type, and then specify the necessary additional settings.

Connection Mode setting	Additional settings
Static IP	<ul style="list-style-type: none"> • WAN IP Address¹ • Subnet Mask² • Gateway¹ • Preferred DNS IP Address¹ • Alternative DNS IP Address¹
DHCP	<ul style="list-style-type: none"> • If you select Obtain From DHCP in DNS Setting, address information is obtained from the DHCP server. • If you select Static in DNS Setting specify the following settings: <ul style="list-style-type: none"> – Preferred DNS IP Address¹ – Alternative DNS IP Address¹
PPPoE	Refer to "PPPoE Additional Settings".
Disable	The built-in router does not operate

PPPoE Additional Settings

Specify the following settings:

Settings	Address Conf. Mode		
	Dynamic IP	Unnumbered	Static IP
User Name ³	✓	✓	✓
Password ³	✓	✓	✓
Service Name ⁴	✓	✓	✓
WAN IP Address ¹		✓	✓
Subnet Mask ²			✓
Gateway ¹			
Preferred DNS IP Address ¹			✓
Alternative DNS IP Address ¹			✓

Note

- For details about configuring the parameters, refer to "27.2.1 Router Configuration—Setup—[1-2-1] WAN—Connection Settings" in the PC Programming Manual.
- For details about the values to set for the parameters, consult the network administrator.

c. In **IPSec (VPN) Connection (Trial Activation Key)**, select **Simple Configuration –VPSS**.

Note

- The IPSec feature will operate until the trial activation key expires. To continue using the IPSec feature, the activation key (KX-NSN216) is required.
- For details about manually changing parameters related to inter-site connections via IPSec established by VPSS, refer to "27.9 Router Configuration—VPN—[3-1] VPSS" in the PC Programming Manual.

d. <At the Master Unit>

Click **Export** to export the setting file.

The setting file created by the Master unit PBX is required to add a Slave unit to the network.

Note

The **Export** button will also be available when adding a Slave unit.

<At a Slave Unit>

Click **Import** to import the setting file exported from the Master unit.

Note

- The settings become active after restarting the Slave unit.
- In the imported data, if the VPSS's **Master Site IP Address (WAN)** cannot be resolved, a window for setting the **Master Site IP Address (WAN)** is displayed. Set the **Master Site IP Address (WAN)**. This setting can also be set later.
For details, refer to "27.9 Router Configuration—VPN—[3-1] VPSS" in the PC Programming Manual.

e. Click **Next**.

When not using the built-in router:

- a. In **Built-in Router—Connection Mode**, select **Disable**.
- b. Click **Next**.

^{*1} Valid IP address range: "1.0.0.1" to "223.255.255.254"

^{*2} Valid subnet mask address range: "0–255.0–255.0–255.0–255" (except "0.0.0.0" and "255.255.255.255")

^{*3} Up to 64 characters.

^{*4} Up to 24 characters.

6. In **Registration Setting**, the **IP Terminal Registration Mode** and the **One Look Networking (Trial Activation Key)** can be set.

a. Select the **IP Terminal Registration Mode**:

- **Manual**: Select this mode to manually register IP terminal information.
- **Full Automatic**: Select this mode to automatically register IP terminal information.
- **Extension Number Input**: Select this mode to automatically register IP terminal information except its extension number. The extension number can then be registered from the IP telephone manually.

Note

- Full Automatic and Extension Number Input registration methods may not be available for certain types of IP terminals. In such cases, select the Manual registration method.
- For more information about the IP terminal registration modes, refer to "5.9.1 Registering IP Telephones".

b. For **One Look Networking (Trial Activation Key)**, specify whether to activate the 60-day One-look Networking Trial Activation Key.

- If **Active** is selected, the 60-day trial will begin when the Easy Setup Wizard is completed.
- If **Non Active** is selected, you will have to activate the trial manually in order to use One-look Networking Features on a trial basis.

c. Click **Next**.

If **Slave** has been selected in step 2, the Easy Setup Wizard will finish at this step. If LAN settings have been changed from their default values in step 4, you will be prompted to restart the PBX. Click **OK** to restart the PBX.

To add the PBX as a Slave unit PBX to the One-look network, use the Add Site Wizard from the Master unit PBX's Home Screen.

7. In **SNTP / Daylight Saving**, enter information for **Automatic Time Adjustment** and **Daylight Saving**, and then click **Next**.
8. In **Maintenance Setting**, the **Installer password**, information for **SNMP Setting** and **SNMP Manager** can be entered.
 - a. Enter a password for the Installer level account in **Installer password**. Confirm your input in **Re-enter**.
 - b. Specify settings for **SNMP Setting** and **SNMP Manager** if necessary. If you are unsure of your network's SNMP settings, contact your network's administrator.
 - c. Click **Finish**.
9. Follow the prompts of the Easy Setup Wizard. After the Easy Setup Wizard is completed, if LAN settings have been changed from their default values in step 4, you will be prompted to restart the PBX. Click **OK** to restart the PBX. Otherwise, the login screen will be displayed.
10. Log in with the Installer level account using the password entered during Easy Setup Wizard. The Home Screen is displayed. You may now begin programming the PBX.

Notice

If an external DHCP server is in use, it must be able to use a "client identifier" option specified by RFC 2131.

Changing IP Address Settings

IP addressing information for the PBX can also be changed from Web Maintenance Console after the Easy Setup Wizard has been completed.

1. Click **Setup** → **Network Service** → **IP Address/Ports**.
2. Click the **Basic Settings** tab.
3. **When using a DHCP server:**
 - a. Select **Obtain an IP address automatically**.
 - b. Select **Obtain DNS server address automatically**.
 - c. Select **Obtain DSP IP address automatically**.

Notice

The boxes will turn grey and the IP address information will be assigned automatically.
Write down the address information assigned to the PBX for future reference.

When not using a DHCP server:

- a. Select **Use the following IP address**.
- b. Enter an IP address¹, Subnet Mask², and Default Gateway¹.
(The default gateway may not need to be specified depending on your network configuration.)
- c. Select **Use the following DNS server address**.
- d. Enter the preferred and alternative DNS IP addresses¹.
- e. Select **Use the following DSP IP address**.
- f. Enter up to 2 IP addresses¹ for each installed DSP card.
4. Click **OK**.
 - a. A screen will appear stating that any changes made in step 3 will be activated after the PBX is restarted.
 - b. Click **OK**.
5. Restart the PBX.
 - a. Click **Maintenance** → **System Control** → **System Reset**.
 - b. On the System Reset screen, click **Backup**.

¹ Valid IP address range: "1.0.0.0" to "223.255.255.255"

² Valid subnet mask address range: "0–255.0–255.0–255" (except "0.0.0.0" and "255.255.255.255")

Notice

- Do not change the IP address of the PBX once IP telephones are registered to the PBX using the set IP address. The IP telephones will not operate properly if the IP address of the PBX is changed. When an external DHCP server is used to automatically assign IP addresses, it must be configured to always allocate the same IP address to the PBX. For details, consult your network administrator.
- If an external DHCP server is in use, it must be able to use a "client identifier" option specified by RFC 2131.
- If an external DHCP server is in use, the KX-NS1000 DHCP Server feature must be disabled.
- The PBX will not start properly if IP addresses cannot be assigned automatically by the DHCP server when the PBX has been set to obtain IP addresses automatically. In this case, you need to consult your network administrator because the DHCP server in your network may not be running or a network failure may have occurred. If the DHCP server is not available, enter IP addresses manually, then restart the PBX. If the PBX cannot be accessed over the network, connect the PC directly to the PBX with an Ethernet cable and access Web Maintenance Console using a direct connection.

For details about connecting the PC directly to the PBX, refer to "Direct Connection" in "5.2 PC Connection".

- During a long programming session, it is highly recommended that you periodically save the system data to the Storage Memory Card. If the PBX undergoes a sudden power failure or if the system is reset for some reason, all the system data in RAM will be lost. However, if system data has been saved to the Storage Memory Card, it can be easily reloaded.

To save the system data to the Storage Memory Card while programming, click the disk button ()

→ **Yes** → **OK**. Be sure to save the system data to the Storage Memory Card before restarting the PBX, or any changes may be lost.

- When no operations are performed for more than 60 minutes (default), you will be automatically logged out from Web Maintenance Console and unsaved data will be lost.

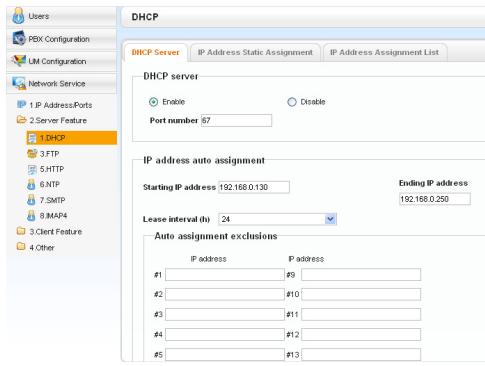
Changing the Display Language

The language used for Web Maintenance Console can be changed after the Easy Setup Wizard has completed.

1. Click **Setup** → **Users** → **User Profiles**.
2. Select the check box for the Installer level account.
3. Click . The **Edit User** screen will be displayed.
4. Select the preferred language in **Change Language**.
5. Click **OK**. The screen will redisplay in the selected language immediately.

5.4.2 Enabling the DHCP Server Feature

This PBX is equipped with a DHCP Server feature. When the feature is enabled, it allows you to centrally manage and automate the assignment of IP addresses for the devices located in same LAN using Web Maintenance Console.



1. Click **Setup** → **Network Service** → **Server Feature** → **DHCP**.
2. On the **DHCP Server** tab, select **Enable** for **DHCP Server**.
3. Enter valid settings for the **IP address auto assignment**.

Note

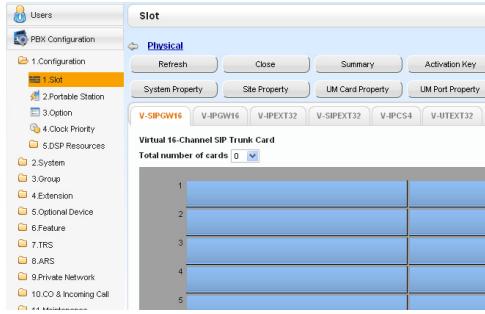
For details about **IP address auto assignment** settings, refer to "28.2.1 Network Service—[2-1] Server Feature—DHCP" in the PC Programming Manual.

4. Click **OK**.

Note

If an external DHCP server is in use, do not enable the DHCP Server feature. Doing so may allocate inappropriate IP addressing information to the devices.

5.4.3 Installing the Virtual IP Cards to the PBX



1. a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
b. Click **Virtual**.
2. a. Click on the name of the desired virtual card tab.
b. From the **Total number of cards** drop-down list, select the desired number of cards.
3. A confirmation message will be displayed. Click **OK**.

5.4.4 Installing Additional Activation Keys

The corresponding number of IP trunks, IP telephones or enhanced features can be activated by installing the downloaded activation key file(s) using Web Maintenance Console.

Installing the Activation Key Files

Be sure to connect the PC to the PBX in advance. For details about Web Maintenance Console, refer to "5.3 Starting Web Maintenance Console".

1. Log in to Web Maintenance Console using the Installer level account.
2. Click **Maintenance** → **Utility** → **Activation Key Installation**.
Activation Key Installation window will be displayed.
3. Click **Browse** and specify the directory where the activation key files are stored, and click **Open**.
4. A list of activation key files stored in the specified directory is displayed. Check the boxes next to the activation keys to install to the PBX, and click **Install**.

5.4.5 Configuration of the Activation Keys

5. The activation keys will be copied to the Master unit, and then the activation keys that Slave units require will be copied to the Slave units of the One-look network. When installation is complete, the message, "The activation key has been installed and activated successfully!" is displayed.
6. Click **OK**.

Notice

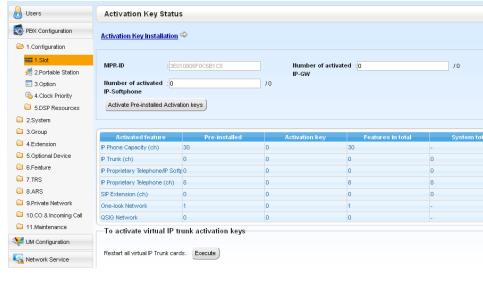
The activation key file can only be installed in the PBX with the MPR ID number entered when the activation key file was downloaded. The activation key file cannot be reissued unless the mother board crashes.

Note

- You can click the provided link to directly access activation key information and programme the number of activated IP trunks and IP softphones.
- For information about programming activation keys using Web Maintenance Console, refer to "9.3 PBX Configuration—[1-1] Configuration—Slot—Activation Key Status" in the PC Programming Manual.

5.4.5 Configuration of the Activation Keys

Depending on your configuration, it may be necessary to programme the number of provided IP Trunk channels to be used for H.323 trunks. By default, all of the provided IP Trunk channels will be used for SIP trunks. Similarly, you can programme how many IP softphone(s) can be used through the IP Softphone/IP Proprietary Telephone activation key. By default, only IP softphone(s) can be used through the IP Softphone/IP Proprietary Telephone activation key.



1. a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
b. Click **Activation Key**.
2. a. In **Number of activated IP-GW**, type the number of IP Trunk channels to be used for H.323 trunks.

Note

If you have changed the value for **Number of activated IP-GW**, you must click **Execute** to restart the V-IPGW16 cards for the change to take effect.

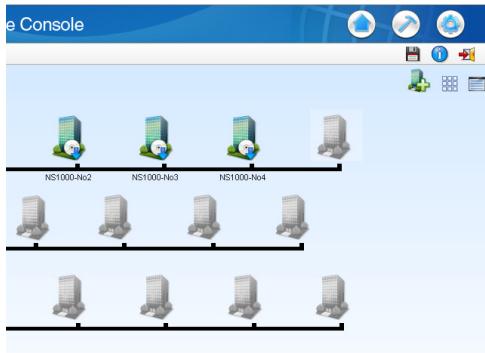
2. b. In **Number of activated IP-Softphone**, type the number of IP softphones to be used through the IP Softphone/IP Proprietary Telephone activation key.
3. Click **OK**.

5.5 Programming a One-look Network

The Add Site Wizard, which is run from the Home Screen of the Master unit, will add other KX-NS1000 PBXs connected to the private IP network to your One-look network as Slave units.

Note

The PBX to be added must have been configured as a Slave unit using the Easy Setup Wizard. For details about Easy Setup Wizard, see "5.4.1 Easy Setup Wizard".



1. To start the Add Site Wizard, click the Add Slave button (Add Slave) on the Home screen.
2. Follow the prompts of the Add Site Wizard to complete following settings:
 - PBX Setting
 - WAN Setting
 - Registration Setting
 - SNTP / Daylight Saving
 - Maintenance Setting

Note

- The parameters which appear in the settings above are described in "5.4.1 Easy Setup Wizard".
- If 2 or more sites will be added to the One-look network, repeat steps **1** to **2** for each site.

Site ID	Site Name	Location(MIB)
1	NS1000	
2	NS1000-N61	
3	NS1000-N62	
4	NS1000-N63	

3. After the Add Site Wizard is completed, click (List View) on the Home screen, and then click **Registration** on the List View.



4. A list of KX-NS1000 PBXs set up as Slave units will be displayed under **Available Site**. Select PBXs by their assigned site names and click the right arrow to move them to **Selected Site for Registration**. Click **Next** to start the registration process.
5. On the **Registration** screen, the status of PBXs being registered is displayed.
6. On the **Registration** screen, the result of the registration process is shown. Click **Close** to continue.

Registered Slave PBXs can now be viewed and selected on the Home Screen for programming.

MASTER LED Transition

When adding Slave units, the MASTER LED of each unit changes as shown in the following table:

5.5 Programming a One-look Network

Master		Slave (When Slave unit power is turned on before Master unit)		Slave (When Slave unit power is turned on after Master unit)	
Operation	MASTER LED	Operation	MASTER LED	Operation	MASTER LED
		Power On	Amber (Flashing)		
		Log in	Amber		
Power On	Amber (Flashing)				
Log in	Green				
Add Site Wizard	Green				
Add Site Wizard is Completed	Green	Being Registered	Amber (Flashing)		
		Registration is Completed	Amber	Power On	Amber (Flashing)
				Log in	Amber
				Being Registered	Amber (Flashing)
				Registration is Completed	Amber

5.6 Programming an H.323 QSIG Network

There are 2 methods to programme the Virtual 16-Channel VoIP Gateway Card (V-IPGW16 card) to establish VoIP communications between PBXs at different locations, as follows:

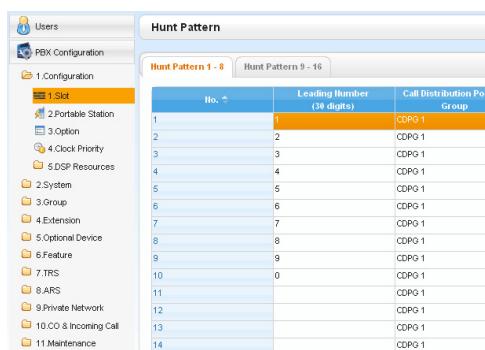
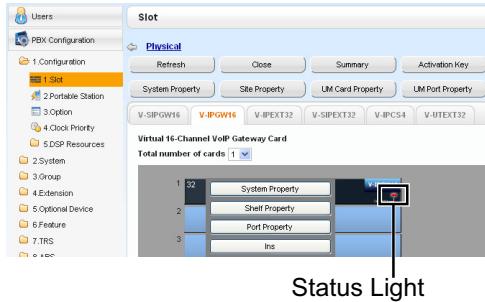
PBX code method	The caller dials the unique PBX code of the PBX to which the called party is connected, in addition to the destination number.
Extension number method	The caller dials only the destination number of the called party to call through PBXs at different locations (hence there are fewer digits to dial than with the PBX code method).

Note

- For a detailed explanation about each method, refer to "4.3 Private Network Features" in the Feature Guide.
- Portions of this software are © 1996–2006 RADVISION Ltd. All intellectual property rights in such portions of the Software and documentation are owned by RADVISION and are protected by United States copyright laws, other applicable copyright laws and international treaty provisions. RADVISION and its suppliers retain all rights not expressly granted.

5.6.1 Assigning the Hunt Pattern

The hunt pattern determines how to route incoming calls through virtual IP trunks to the PBX. The procedure below demonstrates the process of programming the hunt pattern of the local PBX. After the hunt pattern at the local PBX has been fully assigned, repeat the procedure for the hunt pattern at the remote PBX with the appropriate setting values.



- Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
 - Click **Virtual** → **V-IPGW16**.
 - If the V-IPGW16 card's status light is green, move the mouse pointer over the card, select **Ous** from the menu that appears, and then click **OK** on the dialogue box. The status light will turn red.
 - Move the mouse pointer over the installed V-IPGW16 card. A menu will be shown under the mouse pointer.
 - Click **Shelf Property**.
 - Click **Hunt Pattern**.

a. When using the PBX code method:

In the **Leading Number** cell, type the local PBX code and extension starting digit.

When using the extension number method:

In the **Leading Number** cell, type the local extension starting digit.

- Click **OK** to return to the Shelf Property screen.

5.6.2 Programming the Address Translation Table

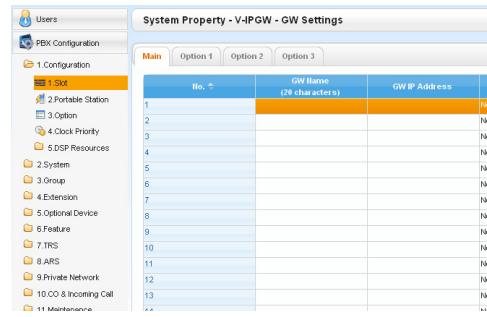
Note

For more details about hunt pattern assignment, refer to "9.12.2 PBX Configuration—[1-1] Configuration—Slot—Shelf Property - Virtual IP Gateway—Hunt Pattern" in the PC Programming Manual.

5.6.2 Programming the Address Translation Table

The function of an address translation table in a VoIP network is to provide 2-way translation of telephone numbers and IP addresses^{*1}. Therefore, a caller can reach the destination by dialling the number without knowing the destination IP address.

The procedure below demonstrates the process of programming the address translation table at the local PBX. After the address translation table at the local PBX has been fully programmed, repeat the procedure for the address translation table at the remote PBX with the appropriate setting values.



1.
 - a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
 - b. Click **System Property**.
 - c. Click the **V-IPGW** tab.
 - d. Click **GW Settings**.
 2. In the **Main** tab, do the following to configure the gateway entry for the remote PBX:
 - a. In the **GW Name** cell, type a unique identifier of the destination in the VoIP network.
 - b. In the **GW IP Address** cell, type the IP address of the destination gateway device.
 - c. In the **GW Group** cell, select **None**.
- Note**
- Having the value **None** for **GW Group** means that the destination gateway device does not belong to any gateway group. Grouping is useful when installing multiple gateway devices at one location. For details, refer to "9.4 PBX Configuration—[1-1] Configuration—Slot—System Property—◆ GW Group" in the PC Programming Manual.
- d. Click **OK** to return to the System Property screen.

^{*1} IP address-to-telephone number translation can also be handled by using an H.323 Gatekeeper device. To configure Gatekeeper devices, refer to the manufacturer's documentation. This manual focuses on the method using the V-IPGW16 card's internal address translation capabilities.

System Property - V-IPGW - DN2IP				
No.	Leading Number (0-9 digits)	Remaining Number of Digits	GW No./GW Group Selection	GW Group
1	0	0	GW No.	1
2	1	0	GW No.	1
3	2	0	GW No.	1
4	3	0	GW No.	1
5	4	0	GW No.	1
6	5	0	GW No.	1
7	6	0	GW No.	1
8	7	0	GW No.	1
9	8	0	GW No.	1
10	9	0	GW No.	1
11	0	0	GW No.	1
12	1	0	GW No.	1
13	2	0	GW No.	1

3.
 - a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
 - b. Click **System Property**.
 - c. Click the **V-IPGW** tab.
 - d. Click **DN2IP**.
 - e. When using the **PBX code method**:
In the **Leading Number** cell, type the remote PBX code and starting digit of destination extension.

When using the extension number method:

In the **Leading Number** cell, type the remote PBX code and starting digit of destination extension.

- f. In the **Remaining Number of Digits** cell, type a number of digits to dial following the leading number.
- g. In **GW No./GW Group Selection**, select **GW No.**.
- h. In the **GW No.** cell, select 1 (the gateway entry for the destination gateway device at the remote PBX).
- i. Click **OK**.

Note

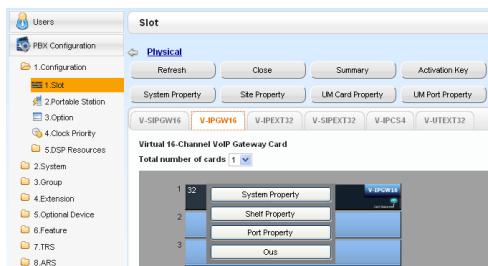
For more details about gateway settings, refer to "9.4 PBX Configuration—[1-1] Configuration—Slot—System Property—GW Settings—Main" in the PC Programming Manual.

5.6.3 Programming the Network Settings

For successful operation of a VoIP network using the V-IPGW16 card, network settings for the PBX at each location must be programmed appropriately. For a detailed discussion of related features, refer to the Feature Guide.

This section details the procedure to programme the network settings for the local PBX. After the programming for the local PBX has been done, repeat the procedure for the remote PBX with the appropriate setting values. The following procedures describe the process of programming the network settings for each numbering method.

Programming for the PBX Code Method



1. a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
- b. Click **Virtual** → **V-IPGW16**.
- c. Move the mouse pointer over the installed V-IPGW16 card to display the menu of options, and click **Ous** (out of service) to set the card to out of service.
- d. Repeat step c for each installed V-IPGW16 card until all V-IPGW16 cards are OUS.
- e. Move the mouse pointer over the installed V-IPGW16 card to display the menu of options, and click **Port Property**.

Confirm that all V-IPGW16 cards are OUS.

Note

When a V-IPGW16 card is installed, 8 ports are available for the card (a port has 2 channels).

Port Property			
Shelf	Slot	Port	Connection
Virtual	32	1	OUS
Virtual	32	2	OUS
Virtual	32	3	OUS
Virtual	32	4	OUS
Virtual	32	5	OUS
Virtual	32	6	OUS
Virtual	32	7	OUS
Virtual	32	8	OUS

2. a. Click **Setup** → **PBX Configuration** → **CO & Incoming Call**.
- b. Click **CO Line Settings**.
- c. Type the **CO Name** and assign an unused **Trunk Group Number** to be used for all IP trunks.
- d. Click **OK**.

CO Line Settings		
	Slot	Port
31	1	
31	2	
31	3	
31	4	
31	5	
31	6	
31	7	
31	8	
31	9	
31	10	
31	11	

The first screenshot shows the 'Main' tab of the 'Features' section. It lists various PBX features with their corresponding dialing numbers. The 'TIE Line Access' feature is highlighted with a yellow background and the number '7' in the 'Dial (4 digits)' column.

No.	Feature	Dial (4 digits)
1	Operator Call	9
2	Idle Line Access (Local Access)	0
3	Trunk Group Access	8
4	TIE Line Access	7
5	Redial	#
6	System Speed Dialing / Persons**	
7	Personal Speed Dialing - Program	*39
8	DOORPHONE Call	*51
9	Group Paging	*33
10	External BGM On/Off	*35
11	OGM Record / Clear / Playback	*36
12	Single CO Line Access	*37
13	Parallel Telephone (Ring) Mode	*39
14	Group Call Pickup	*40
15	Directed Call Pickup	*41
16	TAFAS Answer	*42

The second screenshot shows the 'TIE Table' tab. It lists 'Priority 1' through 'Priority 6' and 'Leading Number (3 digits)' for trunk groups 1 through 13. Trunk group 1 is highlighted with a yellow background and has a value of '0' in the 'Priority 1 - Remote Number of Digits' column.

ID	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Leading Number (3 digits)	Priority 1 - Remote Number of Digits
1							0	0
2							2	0
3							3	0
4							4	0
5							5	0
6							6	0
7							7	0
8							8	0
9							9	0
10							0	0
11								0
12								0
13								0

The third screenshot shows the 'Slot' tab. It lists installed cards: V-SIPGW16, V-IPGW16, V-IPEXT32, V-SIPEXT32, V-IPCS4, and V-UTEXT32. The V-IPGW16 card is highlighted with a yellow background. A context menu is open over the card, showing options: System Property, Shelf Property, Port Property, and Ins (in service). The 'Ins' option is highlighted with a yellow background.

3. Note

Before changing Numbering Plan settings, when a V-SIPEXT32 card or V-UTEXT32 card is installed, change the status of the card(s) to OUS.

- Click **Setup** → **PBX Configuration** → **System**.
- Click **Numbering Plan**.
- Click **Main**.
- Click the **Features** tab.
- In the **TIE Line Access** cell, type the dialling number.
- Click **OK**.
- Click **Setup** → **PBX Configuration** → **Private Network**.
- Click **TIE Table**.
- In the **Own PBX Code** cell, type the PBX code of the local PBX in the network.
- In the first unused **Leading Number** cell, type the PBX code of the remote PBX in the network.
- In the corresponding **Trunk Group** list, select the number of the trunk group to be used when making calls.
- If it is necessary to add number(s) to the input number, enter the number(s) to be added in the desired **Added Number** cell.
- If it is necessary to delete number(s) from the input number, enter the number(s) to be deleted in the desired **Removed Number of Digits** cell.
- Click **OK**.
- Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
- Click **Virtual** → **V-IPGW16**.
- Move the mouse pointer over the installed V-IPGW16 card to display the menu of options, and click **Ins** (in service).
- Repeat step **c** for each installed V-IPGW16 card until all V-IPGW16 cards are INS.

Programming for the Extension Number Method

The first screenshot shows the 'Slot' tab with the 'Physical' tab selected. It lists installed cards: V-SIPGW16, V-IPGW16, V-IPEXT32, V-SIPEXT32, V-IPCS4, and V-UTEXT32. The V-IPGW16 card is highlighted with a yellow background. A context menu is open over the card, showing options: System Property, Shelf Property, Port Property, and Ous (out of service). The 'Ous' option is highlighted with a yellow background.

The second screenshot shows the 'Slot' tab with the 'Virtual' tab selected. It lists the same installed cards. The V-IPGW16 card is highlighted with a yellow background. A context menu is open over the card, showing options: System Property, Shelf Property, Port Property, and Port Property. The 'Port Property' option is highlighted with a yellow background.

- Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
- Click **Virtual** → **V-IPGW16**.
- Move the mouse pointer over the installed V-IPGW16 card to display the menu of options, and click **Ous** (out of service) to set the card to out of service.
- Repeat step **c** for each installed V-IPGW16 card until all V-IPGW16 cards are OUS.
- Click **Port Property**.

5.6.3 Programming the Network Settings

Port Property				
	Shelf	Slot	Port	Connection
Virtual	32	1		OUS
Virtual	32	2		OUS
Virtual	32	3		OUS
Virtual	32	4		OUS
Virtual	32	5		OUS
Virtual	32	6		OUS
Virtual	32	7		OUS
Virtual	32	8		OUS

Confirm that all V-IPGW16 cards are set to OUS.

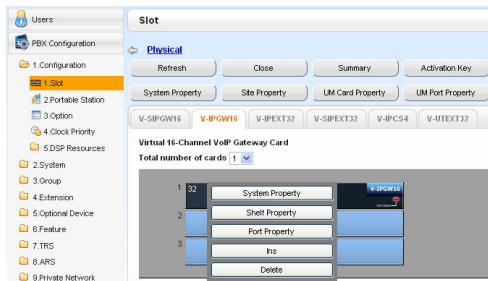
Note

When a V-IPGW16 card is installed, 8 ports are available for the card.

2.
 - a. Click **Setup** → **PBX Configuration** → **CO & Incoming Call**.
 - b. Click **CO Line Settings**.
 - c. Type the **CO Name** and assign an unused **Trunk Group Number** to be used for all IP trunks.
 - d. Click **OK**.

3. **Note**
Before changing Numbering Plan settings, when a V-SIPEXT32 card or V-UTEXT32 card is installed, change the status of the card(s) to OUS.
 - a. Click **Setup** → **PBX Configuration** → **System**.
 - b. Click **Numbering Plan**.
 - c. Click **Main**.
 - d. Click the **Other PBX Extension** tab.
 - e. In the **Dial (3 digits)** cell, type a starting digit of destination extension.
 - f. Click **OK**.

4.
 - a. Click **Setup** → **PBX Configuration** → **Private Network**.
 - b. Click **TIE Table**.
 - c. In the **Leading Number** cell, type the starting digit of destination extension.
 - d. Click **OK**.



5. a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
- b. Click **Virtual** → **V-IPGW16**.
- c. Move the mouse pointer over the installed V-IPGW16 card to display the menu of options, and click **Ins**.
- d. Repeat step c for each installed V-IPGW16 card until all V-IPGW16 cards are INS.

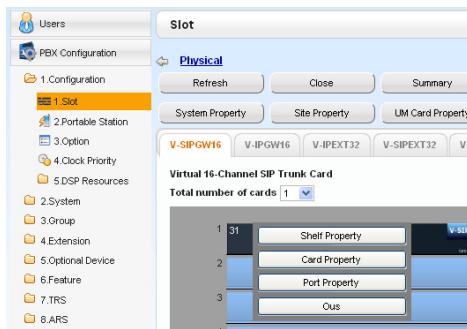
Note

For details about network parameter settings, refer to the relevant sections of the PC Programming Manual.

5.7 Programming SIP Trunks

The Virtual 16-Channel SIP Trunk Card (V-SIPGW16) is a virtual trunk card which is designed to be easily integrated into an Internet Telephony Service provided by an ITSP (Internet Telephony Service Provider). Various settings can be programmed for each virtual SIP gateway port.

Accessing Port Properties



1. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
2. Click **Virtual**.
3. Move the mouse pointer over the V-SIPGW16 card to display the menu of options, and then click **Ous**.
4. Move the mouse pointer over the V-SIPGW16 card to display the menu of options again, and then click **Port Property**.

Programming Port Properties

Automatic Programming

Some of the parameters can be automatically programmed by selecting the desired SIP provider for each virtual SIP gateway port. Available SIP providers can be selected, and a different SIP provider can be assigned to each virtual SIP gateway port.

Note

It is necessary to import a SIP provider list file (comma-separated value [CSV] file) in advance to use the automatic programming feature.

Follow the steps below to configure a SIP provider.

1. Click **Select Provider**.

A dialogue box will appear. Available virtual SIP gateway port numbers are displayed in the list.

2. From the **Provider** menu, select the desired SIP provider.

Note

If the desired SIP provider is not shown in the drop-down list, it is necessary to programme the desired parameters manually. For information about the manual programming procedure, refer to "Manual Programming" below.

3. Highlight the desired port numbers or click **Select All** to select all the virtual SIP gateway port numbers to be assigned to the SIP provider selected in step 2.
4. Click **Execute**.

Appropriate setting values designated by the SIP provider will be set in the parameters for the virtual SIP gateway ports.

Manual Programming

Follow the steps below to programme the parameters which are not automatically programmed by selecting a provider.

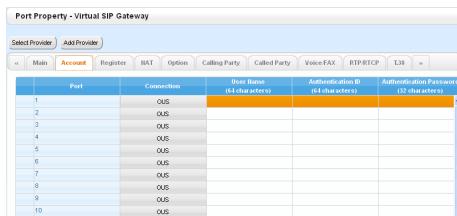
1. Click the desired tab.
2. Enter information or select settings from the drop-down list for each parameter.

Parameters that Require Manual Programming

Manual programming is compulsory for the following parameters:

- **User Name:** Specifies the user name (SIP Account) provided by the SIP provider. (Max. 64 characters)
- **Authentication ID:** Specifies the authentication ID required for registration with the SIP server. (Max. 64 characters)
- **Authentication Password:** Specifies the authentication password used for registration with the SIP provider. (Max. 32 characters)

Follow the steps below to programme these 3 parameters.



1. Click an **Account** tab.
2. In the **User Name** column, enter the user name provided by the SIP provider.
3. In the **Authentication ID** column, enter the authentication ID required for registration with the SIP server.
4. In the **Authentication Password** column, the authentication password used for registration with the SIP provider.
5. Click **OK**.

Adding Settings to Provider Profiles

Follow the steps below to add the settings to provider profiles.



1. Click **Add Provider**. A dialogue box will appear. Available virtual SIP gateway port numbers are displayed in the list.
2. Highlight the desired port numbers or click **Select All** to select all the virtual SIP gateway port numbers to add the settings to provider profiles.
3. Click **Execute**.

Note

For more details about SIP gateway port settings, refer to the PC Programming Manual.

5.8 Assigning Networking Information to IP Telephones

5.8.1 Assigning IP Addressing Information

The IP telephone's IP address, subnet mask address and default gateway address, and the PBX's IP address must be assigned to the IP telephone before it can be used on the network. This IP addressing information can be assigned in the following ways:

For IP-PTs

- **Using a DHCP server (DHCP Server feature or an external DHCP server) when the IP-PT is on the same LAN as the PBX**

The DHCP server automatically assigns the IP address of the IP-PT, the subnet mask address, and the default gateway address to the IP-PT.

The PBX's IP address can also be assigned automatically to the IP-PT in the process of being registered to the PBX. For details about registering the IP-PT, refer to "5.9.1 Registering IP Telephones".

Note

For information about the DHCP Server feature, refer to "8.1.2 DHCP (Dynamic Host Configuration Protocol) Server".

- **Using a DHCP server (DHCP Server feature or an external DHCP server) when the IP-PT is on a remote office LAN**

While the DHCP server automatically assigns the IP address of the IP-PT, the subnet mask address, and the default gateway address to the IP-PT, the PBX's IP address must be assigned manually.

Follow the procedure below to assign the PBX's IP address.

If you need to set VLAN parameters, follow the procedure described in "5.8.2 Setting VLAN Parameters" after assigning the IP addresses, without ending programming.

Note

- By assigning the PBX's IP address to one IP-PT, it is possible to assign the PBX's IP address to other IP-PTs or IP-CSs on the same LAN through system programming. For details, refer to "9.15 PBX Configuration—[1-1] Configuration—Slot—V-IPEXT32—Port Property—Option—◆ Announce Mode" in the PC Programming Manual.
- IP-PTs can only receive IP addressing information from a DHCP server on its own LAN. Therefore, when IP-PTs are located on several LANs, a DHCP server is required on each LAN.
- Since the default setting of the DHCP client function is enabled for IP-PTs, simply connect the IP-PTs to the LAN to use the DHCP server.

KX-NT300 series (except KX-NT321) and KX-NT500 series (except KX-NT551)**To start programming**Supply power to the IP-PT. ►  ►

Press "SETUP" when it is displayed.

To enter the IP address of the PBX

For KX-NT300 series: Software version 2.00 or later only
For KX-NT500 series: Software version 1.00 or later only



To enter the IP address of the Secondary PBX
 (optional for KX-NT300 series [Software version 2.00 or later only] and KX-NT500 series [Software version 1.00 or later only])

**To set VLAN parameters**

► To the VLAN settings

OR**To end programming**

►  ►  ►

Return to the Menu screen. Press "STORE".

The IP-PT will reboot and can then be registered to the PBX.

Note

The illustrations may differ from the buttons on your telephone.

5.8.1 Assigning IP Addressing Information

KX-NT321/KX-NT551

To start programming

Supply power to the IP-PT. ►  ►
Press PROGRAM while "Searching" is displayed.

To enter the IP address of the PBX

►►  ►  ►  ►  ►  ►►
Select "PBX". Press SP-PHONE. Select "PBX IP Address". Press SP-PHONE. Select "Primary PBX".
►►  ►  ►  ►►
Press SP-PHONE. Press SP-PHONE.

To enter the IP address of the Secondary PBX (if required)

►►  ►  ►  ►  ►►
Select "Secondary PBX". Press SP-PHONE. Press SP-PHONE.

►►  ►►

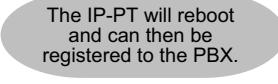
Press HOLD twice to return to the Menu screen.

To set VLAN parameters

►► To the VLAN settings

OR

To end programming

►►  ►  
Press STORE.

The IP-PT will reboot and can then be registered to the PBX.

Note

To confirm the connection to the secondary PBX after assigning IP addressing information, (1) turn the IP-PT's power off, and (2) hold the STORE button and **2** key while turning the power on.

KX-NT265 (Software version 2.00 or later only)

To start programming

Supply power to the IP-PT. ►  ►
Press PROGRAM while "Searching" is displayed.

To enter the IP address of the PBX

►►  ►►  ►►  ►►  ►►  ►►
Press VOLUME to select "PBX". Press SP-PHONE twice. Press SP-PHONE. Press HOLD to return to the Menu screen.

To set VLAN parameters

►► To the VLAN settings

OR

To end programming

►►  ►► The IP-PT will reboot and can then be registered to the PBX.
Press STORE.

5.8.1 Assigning IP Addressing Information

- **Not using a DHCP server (DHCP Server feature or an external DHCP server) when the IP-PT is on the same LAN as the PBX**

Only the PBX's IP address can be assigned automatically to the IP-PT in the process of being registered to the PBX. For details about registering the IP-PT, refer to "5.9.1 Registering IP Telephones".

Follow the procedure below to assign the IP address of the IP-PT, the subnet mask address, and the default gateway address manually.

If you need to set VLAN parameters, follow the procedure described in "5.8.2 Setting VLAN Parameters" after assigning the IP addresses, without ending programming.

KX-NT300 series (except KX-NT321) and KX-NT500 series (except KX-NT551)

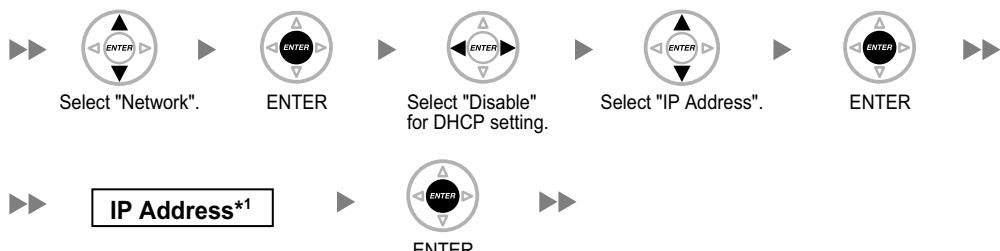
To start programming

Supply power to the IP-PT.

SETUP

Press "SETUP" when it is displayed.

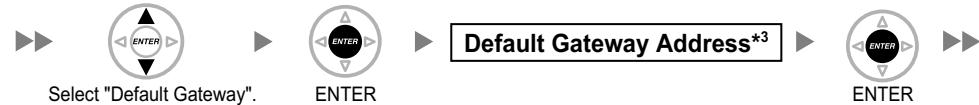
To set the IP address of the IP-PT



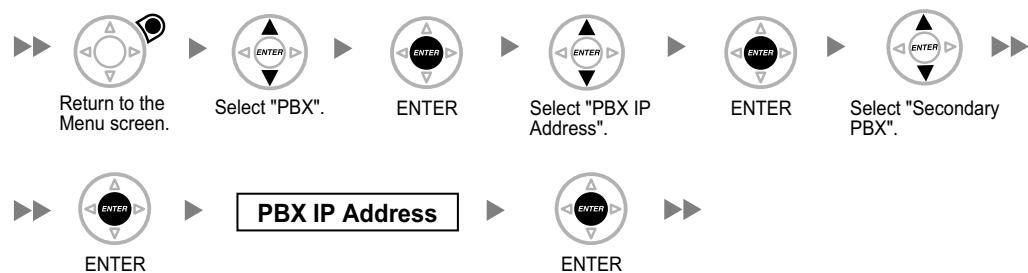
To set the subnet mask address



To set the default gateway address (if required)



To enter the IP address of the Secondary PBX (optional for KX-NT300 series [Software version 2.00 or later only] and KX-NT500 series [Software version 1.00 or later only])



►► Continued on next page

Continued from previous page ►►

To set VLAN parameters



Return to the
Menu screen.

OR

To end programming



Return to the
Menu screen.

STORE

The IP-PT will reboot
and can then be
registered to the PBX.

¹ Valid IP address range: "1.0.0.0" to "223.255.255.255"

² Valid subnet mask address range: "0–255.0–255.0–255" (except "0.0.0.0" and "255.255.255.255")

³ Valid IP address range: "1.0.0.0" to "223.255.255.255"

Note

The illustrations may differ from the buttons on your telephone.

5.8.1 Assigning IP Addressing Information

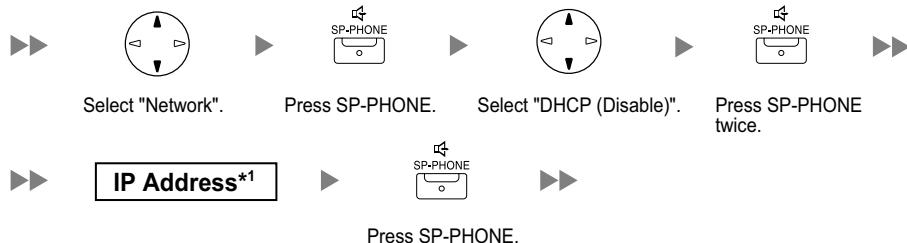
KX-NT321/KX-NT551

To start programming

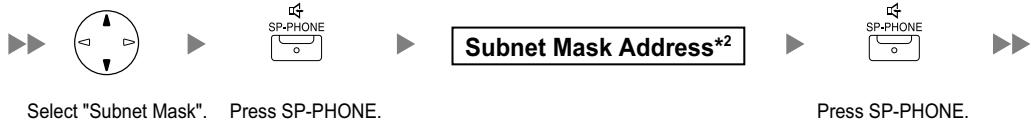
Supply power to the IP-PT. ► 

Press PROGRAM while "Searching" is displayed.

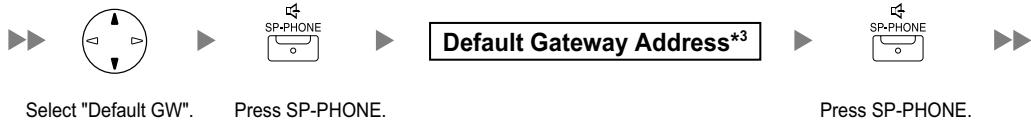
To set the IP address of the IP-PT



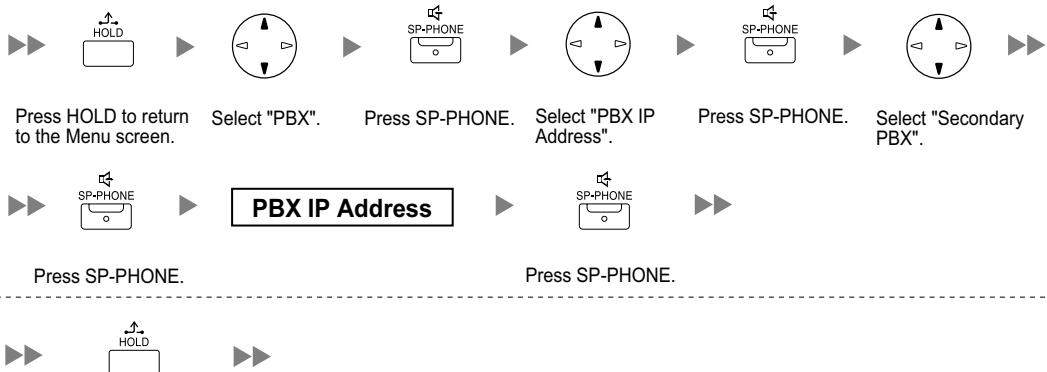
To set the subnet mask address



To set the default gateway address (if required)



To enter the IP address of the Secondary PBX (if required)



►► Continued on next page

Continued from previous page ►►

To set VLAN parameters

►► To the VLAN settings

OR

To end programming

►► 

Press STORE.

The IP-PT will reboot
and can then be
registered to the PBX.

¹ Valid IP address range: "1.0.0.0" to "223.255.255.255"

² Valid subnet mask address range: "0–255.0–255.0–255.0–255" (except "0.0.0.0" and "255.255.255.255")

³ Valid IP address range: "1.0.0.0" to "223.255.255.255"

Note

To confirm the connection to the secondary PBX after assigning IP addressing information, (1) turn the IP-PT's power off, and (2) hold the STORE button and **2** key while turning the power on.

5.8.1 Assigning IP Addressing Information

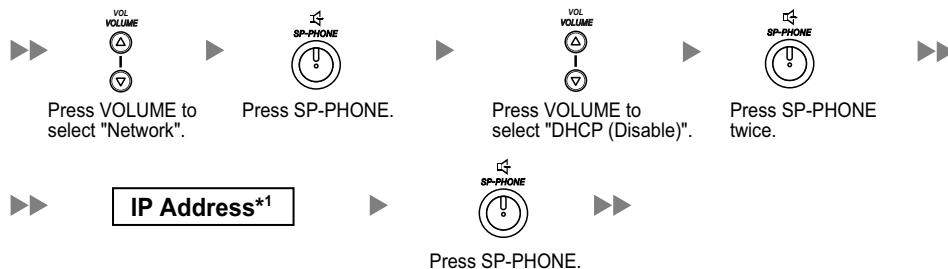
KX-NT265 (Software version 2.00 or later only)

To start programming

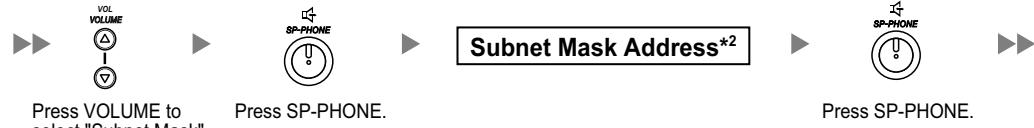
Supply power to the IP-PT. ► 

Press PROGRAM while "Searching" is displayed.

To set the IP address of the IP-PT



To set the subnet mask address



To set the default gateway address (if required)



To set VLAN parameters

►  To the VLAN settings
Press HOLD to return to the Menu screen.

OR

To end programming

►  Press STORE. The IP-PT will reboot and can then be registered to the PBX.
Press HOLD to return to the Menu screen.

*¹ Valid IP address range: "1.0.0.0" to "223.255.255.255"

*² Valid subnet mask address range: "0–255.0–255.0–255" (except "0.0.0.0" and "255.255.255.255")

*³ Valid IP address range: "1.0.0.0" to "223.255.255.255"

- **Not using a DHCP server (DHCP Server feature or an external DHCP server) when the IP-PT is on a remote office LAN**

All of the IP addressing information must be assigned manually.

Follow the procedure below to assign the IP addressing information.

If you need to set VLAN parameters, follow the procedure described in "5.8.2 Setting VLAN Parameters" after assigning the IP addresses, without ending programming.

Note

By assigning the PBX's IP address to one IP-PT, it is possible to assign the PBX's IP address to other IP-PTs or IP-CSs on the same LAN through system programming. For details, refer to "9.15 PBX Configuration—[1-1] Configuration—Slot—V-IPEXT32—Port Property—Option—◆ Announce Mode" in the PC Programming Manual.

5.8.1 Assigning IP Addressing Information

KX-NT300 series (except KX-NT321) and KX-NT500 series (except KX-NT551)

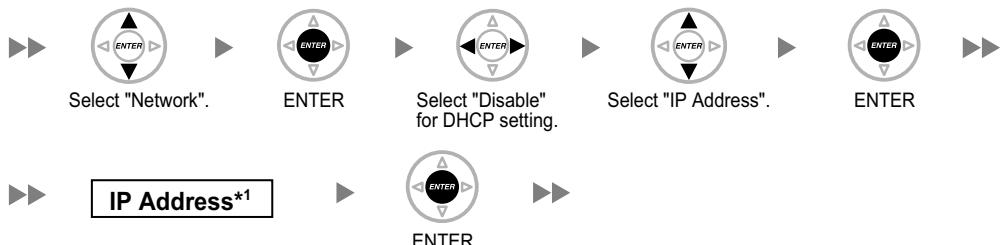
To start programming

Supply power to the IP-PT.

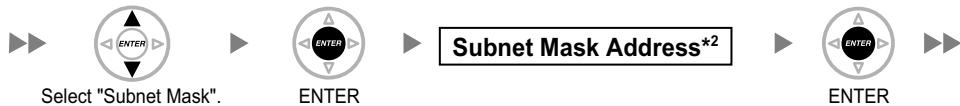
SETUP

Press "SETUP" when it is displayed.

To set the IP address of the IP-PT



To set the subnet mask address



To set the default gateway address



To enter the IP address of the PBX

For KX-NT300 series: Software version 2.00 or later only
For KX-NT500 series: Software version 1.00 or later only



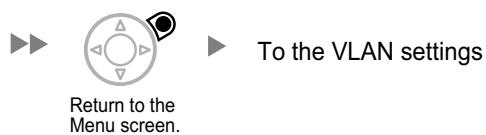
►► **Continued on next page**

Continued from previous page ►►

To enter the IP address of the Secondary PBX (optional for KX-NT300 series [Software version 2.00 or later only] and KX-NT500 series [Software version 1.00 or later only])



To set VLAN parameters



OR

To end programming



¹ Valid IP address range: "1.0.0.0" to "223.255.255.255"

² Valid subnet mask address range: "0–255.0–255.0–255.0–255" (except "0.0.0.0" and "255.255.255.255")

³ Valid IP address range: "1.0.0.0" to "223.255.255.255"

Note

The illustrations may differ from the buttons on your telephone.

5.8.1 Assigning IP Addressing Information

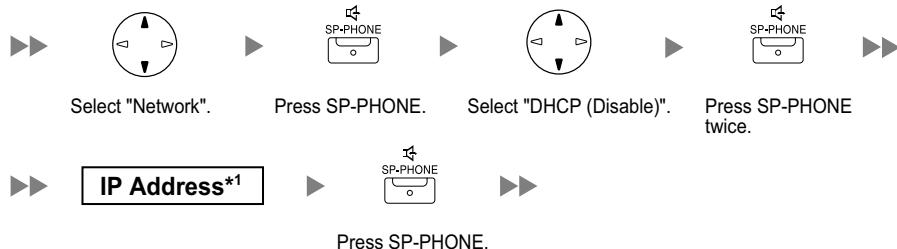
KX-NT321/KX-NT551

To start programming

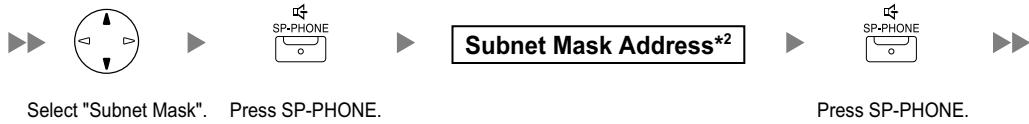
Supply power to the IP-PT. ►  ►►

Press PROGRAM while "Searching" is displayed.

To set the IP address of the IP-PT



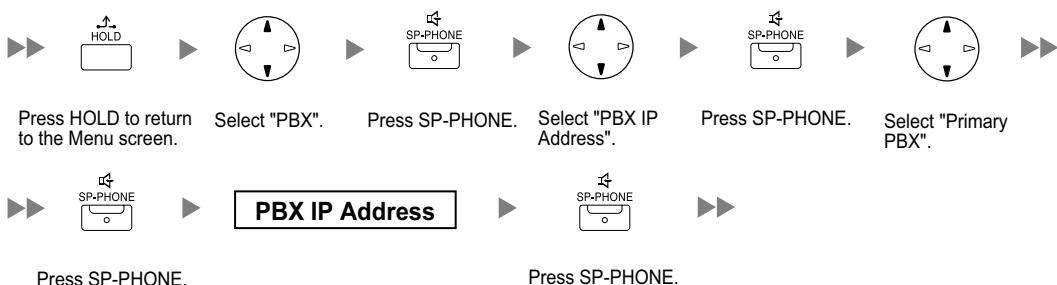
To set the subnet mask address



To set the default gateway address



To enter the IP address of the PBX

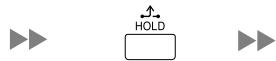


To enter the IP address of the Secondary PBX (if required)



►► **Continued on next page**

Continued from previous page ►►



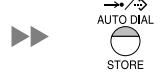
Press HOLD twice to return to the Menu screen.

To set VLAN parameters

►► To the VLAN settings

OR

To end programming



Press STORE.

The IP-PT will reboot and can then be registered to the PBX.

¹ Valid IP address range: "1.0.0.0" to "223.255.255.255"

² Valid subnet mask address range: "0–255.0–255.0–255.0–255" (except "0.0.0.0" and "255.255.255.255")

³ Valid IP address range: "1.0.0.0" to "223.255.255.255"

Note

To confirm the connection to the secondary PBX after assigning IP addressing information, (1) turn the IP-PT's power off, and (2) hold the STORE button and **2** key while turning the power on.

5.8.1 Assigning IP Addressing Information

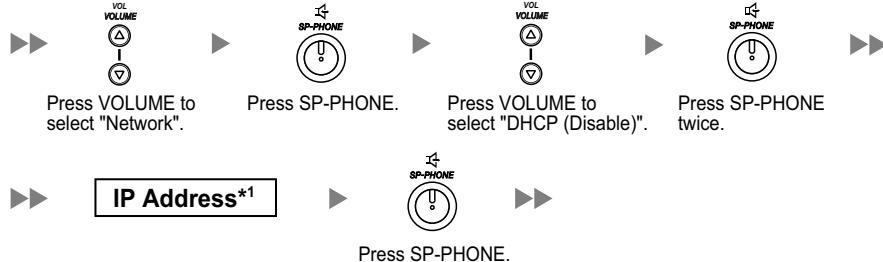
KX-NT265 (Software version 2.00 or later only)

To start programming

Supply power to the IP-PT. ► 

Press PROGRAM while "Searching" is displayed. ►►

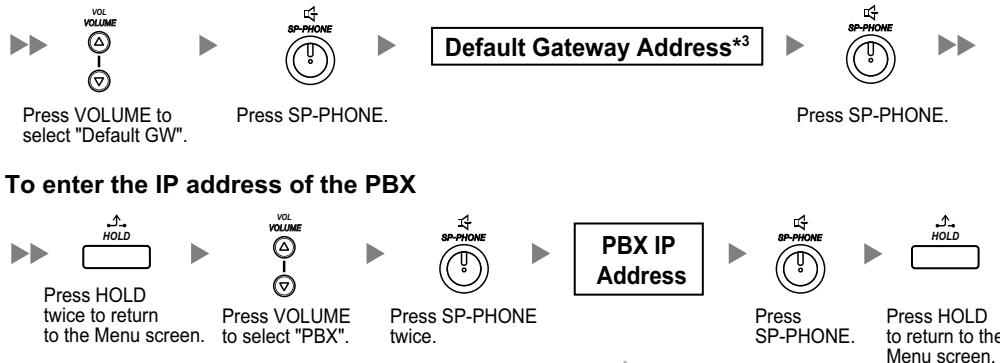
To set the IP address of the IP-PT



To set the subnet mask address



To set the default gateway address



To enter the IP address of the PBX



To set VLAN parameters

► To the VLAN settings

OR

To end programming

► 

Press STORE.

The IP-PT will reboot and can then be registered to the PBX.

*1 Valid IP address range: "1.0.0.0" to "223.255.255.255"

*2 Valid subnet mask address range: "0–255.0–255.0–255.0–255" (except "0.0.0.0" and "255.255.255.255")

*3 Valid IP address range: "1.0.0.0" to "223.255.255.255"

For KX-UT Series SIP Phones

Notice

When you want to use a KX-UT series SIP phone that has already been used with another PBX, or that has had its settings programmed, you must reset the SIP phone to its factory default before assigning new IP address information as detailed in the following procedure.

For details, refer to the documentation for the KX-UT series SIP phone.

Assigning the IP addressing information to the SIP phone

- **Using a DHCP server (DHCP Server feature or an external DHCP server) to automate the assignment of IP addressing information**

The DHCP server automatically assigns the IP address of the SIP phone, the subnet mask address, and the default gateway address to the SIP phone.

The PBX's IP address can also be assigned automatically to the SIP phone in the process of being registered to the PBX. For details about registering the SIP phone, refer to "5.9.1 Registering IP Telephones".

Note

For information about the DHCP Server feature, refer to "8.1.2 DHCP (Dynamic Host Configuration Protocol) Server".

- **Not using a DHCP server (DHCP Server feature or an external DHCP server) when assigning IP addressing information**

Only the PBX's IP address can be assigned automatically to the SIP phone in the process of being registered to the PBX. For details about registering the SIP phone, refer to "5.9.1 Registering IP Telephones". The IP address of the SIP phone, the subnet mask address, and the default gateway address must be assigned manually. For instructions, refer to the documentation of the SIP phone.

Note

- When the PBX is not in the same network as the SIP phone, the IP address of the PBX must be assigned manually. For instructions for manually setting PBX network information, refer to "Assigning the IP address of the PBX to a SIP phone".
- When assigning IP addressing information to the SIP phone, do not use the phone's Web user interface programming.

Assigning the IP address of the PBX to a SIP phone

The IP address of the PBX is automatically assigned to a SIP phone when the SIP phone is in the same LAN as the PBX. However, when the SIP phone is in a different LAN from the PBX, the following procedure is required to assign the IP address of the PBX manually using the Web user interface.

Notice

Do not perform any other operation rather than following procedure with the Web user interface. Otherwise the SIP phone may not work properly. In that case, contact an authorised Panasonic Factory Service Centre.

1. Prepare a configuration file to specify the IP address of the PBX.

When the SIP Phones are in a segment that uses NAT traversal

- a. Open a text editor on a PC, and then write exactly same as the following:

5.8.1 Assigning IP Addressing Information

For standard connection

```
# PCC Standard Format File # DO NOT CHANGE THIS LINE!  
  
### Management Server Settings #####  
ACS_URL="http://xxx.xxx.xxx.xxx:yyy/cwmp/cwmpAction.cgi"
```

For secure connection

```
# PCC Standard Format File # DO NOT CHANGE THIS LINE!  
### Management Server Settings #####  
ACS_URL="http://xxx.xxx.xxx.xxx:yyy/cwmp/cwmpAction.cgi"  
CFG_INT_CERTIFICATE_PATH=http://xxx.xxx.xxx:zzz/utdownload/KX-NS1000
```

Notice

- For "xxx.xxx.xxx.xxx:yyy", enter the IP address and port number of the network router which is in a same LAN with the PBX.
The router accessed by the SIP phone must have static NAT/NAPT settings enabled so that the packets sent to xxx.xxx.xxx.xxx:yyy to be transferred to the PBX. For details, refer to "Connection via Internet" in "5.2 PC Connection" and "Internet Connection (SSL Connection):" in "5.3 Starting Web Maintenance Console".
 - Configuration files must end with an empty line.
- b.** Save the text file as "UT_ACS.cfg".

When the SIP Phones are in a different segments of the same LAN

- a.** Log in to the Web Maintenance Console of the site where the SIP phones will be registered.
For details about logging in to a Slave unit via the Master unit, refer to "3.1 Home Screen" in the PC Programming Manual.
- b.** Click **Utility** → **File** → **File Transfer PBX to PC**.
- c.** Select the config file (UT_ACS_xxxyyy.cfg), and then download it to your PC.
For more details about downloading files from a PBX to a PC, refer to "7.2.2 Utility—File—File Transfer PBX to PC" in the PC Programming Manual.

Note

xx: Site ID (2 digits)

yyy: Site name¹ (Up to 32 characters)²

¹ Spaces as well as the following characters in site names will be replaced with underscores.

/, :, *, ?, ", <, >, | (vertical bar), &, +

² In some cases, the full site name may not be included in the file name even if it is less than 32 characters.

When the SIP Phones are in a different LAN (Remote site installation)

- a.** Log in to the Web Maintenance Console of the site where the SIP phones will be registered.
For details about logging in to a Slave unit via the Master unit, refer to "3.1 Home Screen" in the PC Programming Manual.
- b.** Click **Utility** → **File** → **File Transfer PBX to PC**.
- c.** Select the config file (UT_ACS_HTTPS_xxxyyy.cfg), and then download it to your PC.
For more details about downloading files from a PBX to a PC, refer to "7.2.2 Utility—File—File Transfer PBX to PC" in the PC Programming Manual.

Note

- xx: Site ID (2 digits)

yyyy: Site name¹ (Up to 32 characters²)

¹ Spaces as well as the following characters in site names will be replaced with underscores.

/, :, *, ?, ", <, >, | (vertical bar), &, +

² In some cases, the full site name may not be included in the file name even if it is less than 32 characters.

- When SIP phones use the internet to communicate with the PBX, KX-NS1000 uses the HTTPS protocol for security.

2. Confirm the IP address of the SIP phone.

For non-KX-UT670 telephones

- Press **Setting** or **Setup** (soft button) on the SIP phone.

- Select "Information Display", then press **[ENTER]**.

- Select "IP address".

The IP address of the SIP phone will be displayed.

- Press **[CANCEL]**.

For KX-UT670 telephones

- Tap the status bar.

For details about the status bar, refer to the documentation of the KX-UT670.

- Tap Phone status.

The IP address of the SIP phone will be displayed.

- Tap OK.

3. Open the port of the SIP phone, which is used by the PCs to access the Web user interface.

For non-KX-UT670 telephones

- Press **Setting** or **Setup** (soft button) on the SIP phone.

- Press **[#][5][3][4]**.

- Select "On" for "Embedded web", then press **[ENTER]**.

Note

If no operation are made for 30 minutes, the port will be closed again automatically.

For KX-UT670 telephones

- On the Home screen, press **☰ Menu**.

- Tap Settings.

- Tap About Phone.

- Touch and hold **☰ Menu**.

- Press **[#][5][3][4]**, and then press Enter.

- Select On for Embedded web.

Note

If no operation are made for 30 minutes, the port will be closed again automatically.

4. Access the Web user interface from the PC.

Note

If a KX-UT670 with software version 01.200 or lower is used with the KX-NS1000, the KX-UT670 must be reset to its factory default before you perform the following procedure. For details about resetting the KX-UT670, refer to the documentation of the KX-UT670.

- Open your Web browser, and then enter "http://" followed by the SIP phone's IP address into the address field of your browser.

- For authentication, enter your ID and password, and then click **OK**.

The Installer Level ID and Password are as follows.

ID: instoperatoruserid

Password: instpass

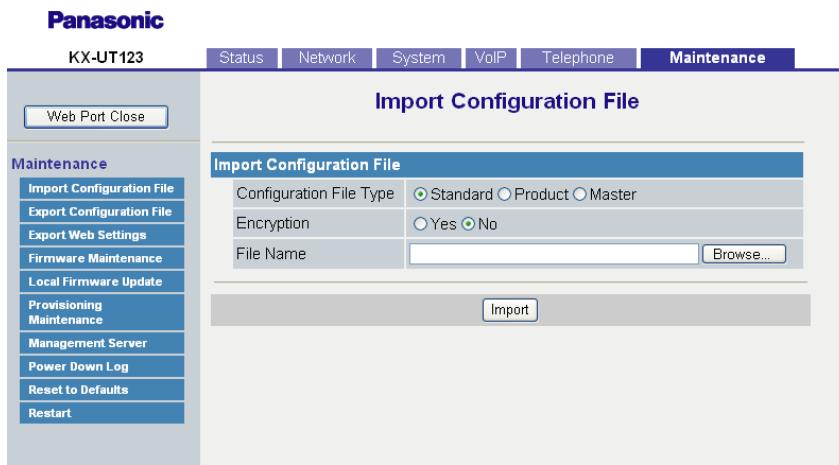
- Select **Maintenance** → **Import Configuration File**.

- Click **Browse...**, and then select the UT_ACS configuration file. (UT_ACS.cfg or UT_ACS_xxxyyy.cfg)

5.8.1 Assigning IP Addressing Information

e. Click **Import**.

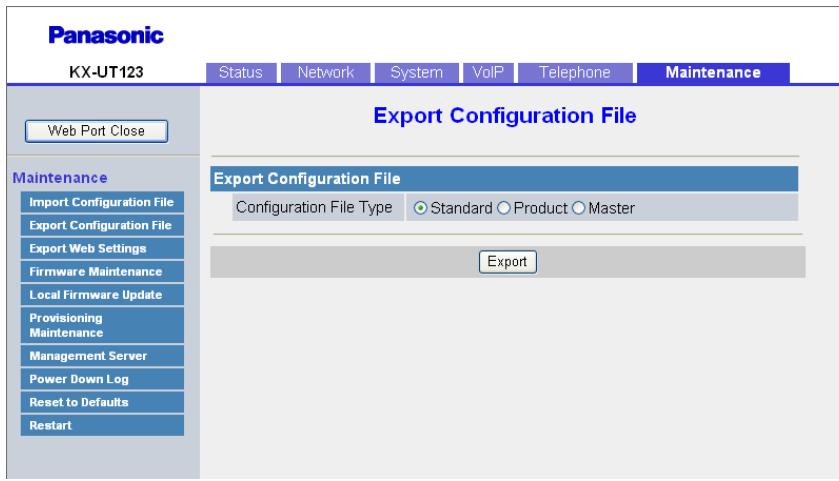
When the configuration file is successfully imported, the SIP phone starts to access the PBX automatically.



5. Confirm if the configuration file was successfully loaded.

a. Select **Maintenance** → **Export Configuration File**.

b. Click **Export** to download the configuration file being used currently on the SIP phone.



c. Compare the UT_ACS configuration file and the downloaded file. If the UT_ACS configuration file was successfully loaded, the contents of those 2 files will be exactly the same.

Notice

When the 2 UT_ACS configuration files do not match, and if the SIP phone does not work properly, contact an authorised Panasonic Factory Service Centre.

For Non-KX-UT Series SIP Phones

Using a DHCP server (DHCP Server feature or an external DHCP server) to automate the assignment of IP addressing information

The IP address of the SIP phone, the subnet mask address, and the default gateway address can be assigned to the SIP phone automatically by the DHCP server.

The PBX's IP address must be assigned manually on the SIP phone side.
For instructions, refer to the documentation of the SIP phone.

Not using a DHCP server (DHCP Server feature or an external DHCP server) when assigning IP addressing information

All of the IP addressing information must be assigned manually.
For instructions, refer to the documentation of the SIP phone.

Note

- A SIP phone can only receive IP addressing information from a DHCP server on its own LAN. Therefore, when SIP phones are located on several LANs, a DHCP server is required on each LAN.
- When the DHCP client function is enabled for SIP phones, simply connect them to the LAN to use the DHCP server. For details about the DHCP client function setting, refer to the documentation of the SIP phone.

5.8.2 Setting VLAN Parameters

To establish voice communications between IP telephones, the primary ports of the IP telephones and the connected PBX must belong to the same VLAN. Consult your network administrator and obtain the appropriate VLAN ID.

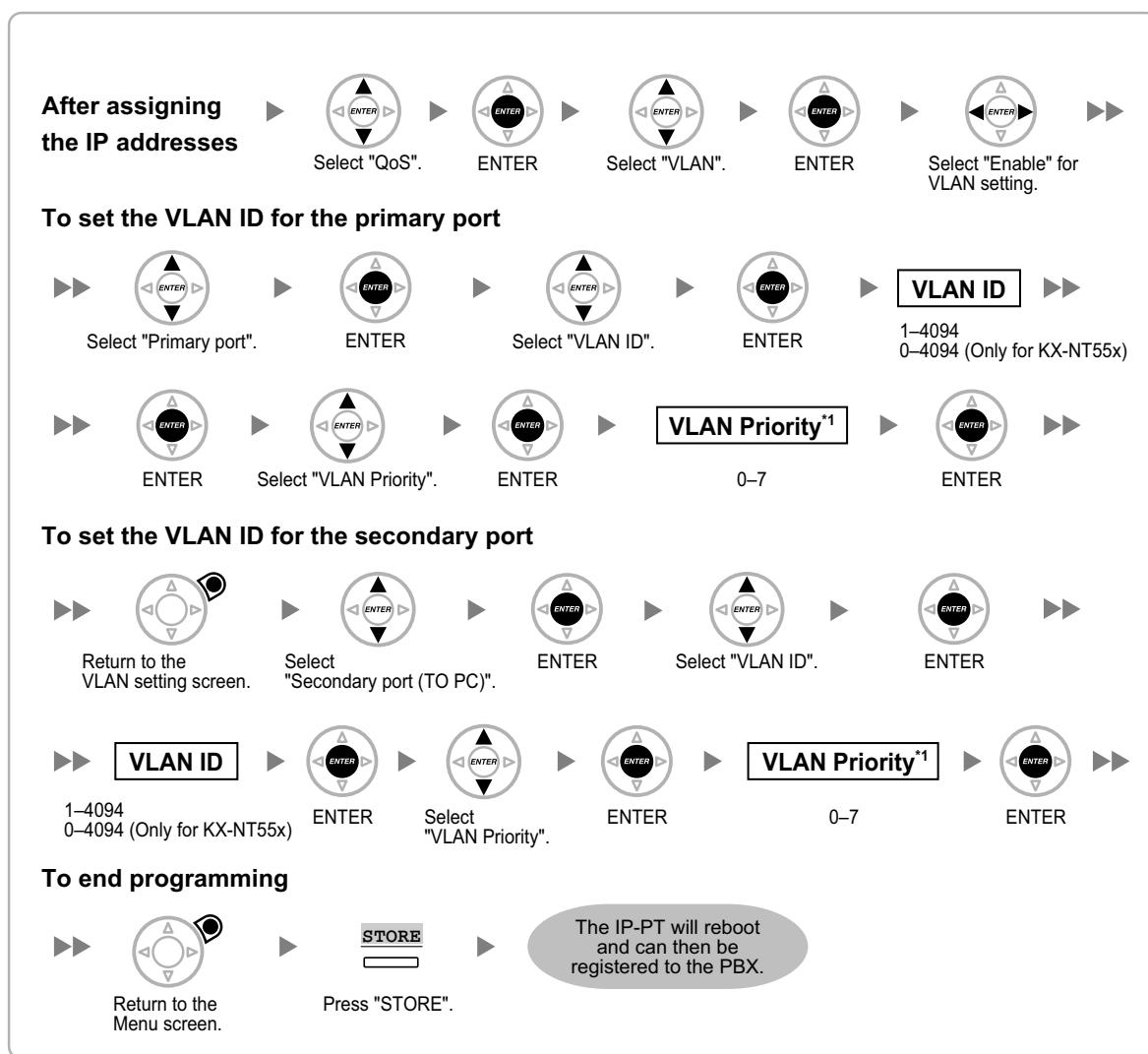
If you are using an IP telephone equipped with two ports, it is possible to place primary and secondary ports of the IP telephone on different VLANs by assigning separate VLAN IDs to each port.

Follow the procedure below for all IP-PTs on the network, using appropriate VLAN IDs.

Note

The procedure for SIP phones may vary depending on the type of the SIP phone being used. Refer to the documentation of your SIP phone for instructions.

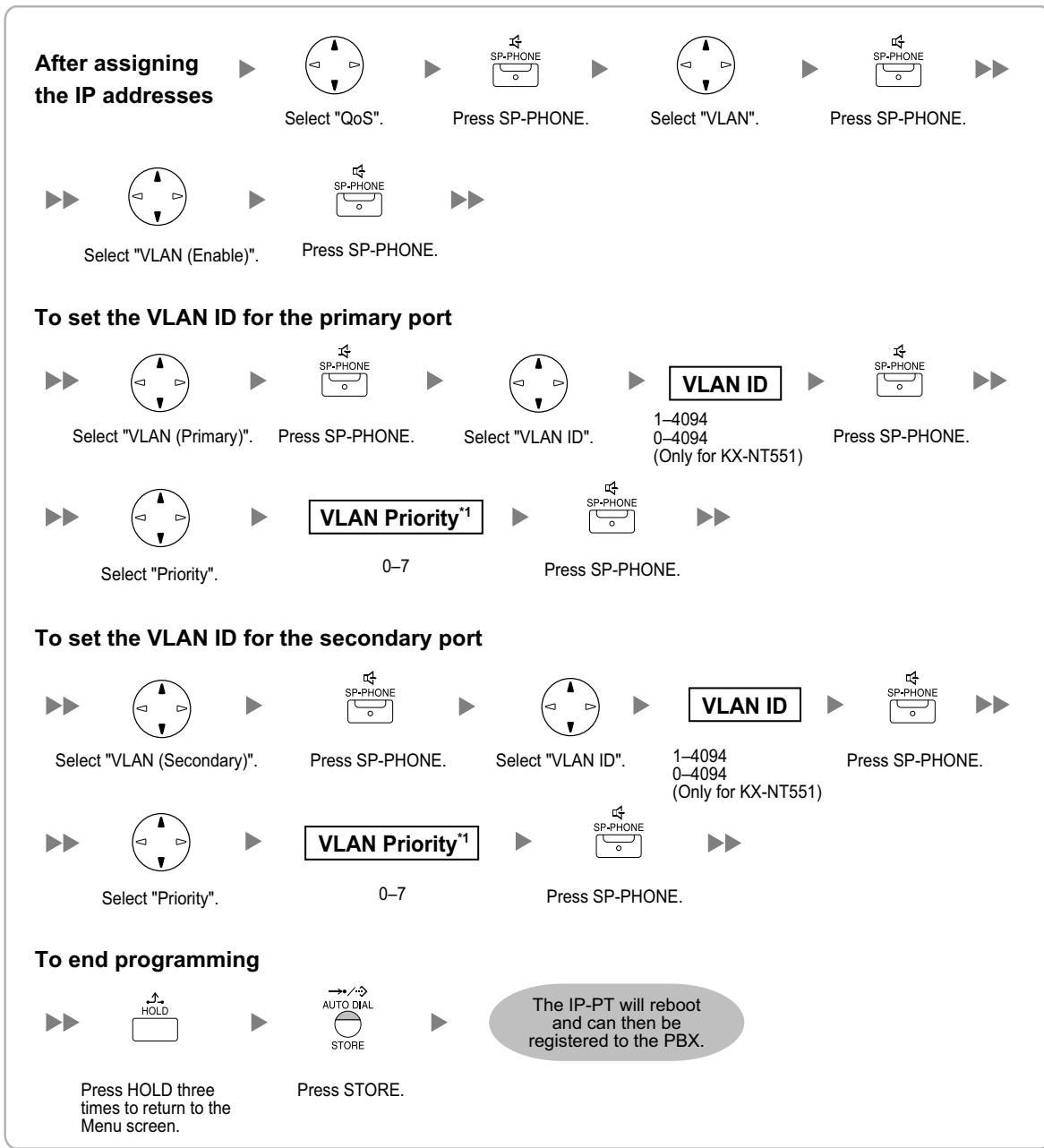
KX-NT300 series (except KX-NT321) and KX-NT500 series (except KX-NT551)



^{*1} The VLAN priority of the primary port must be set higher than the priority of the secondary port. The larger the number, the higher the priority.

Note

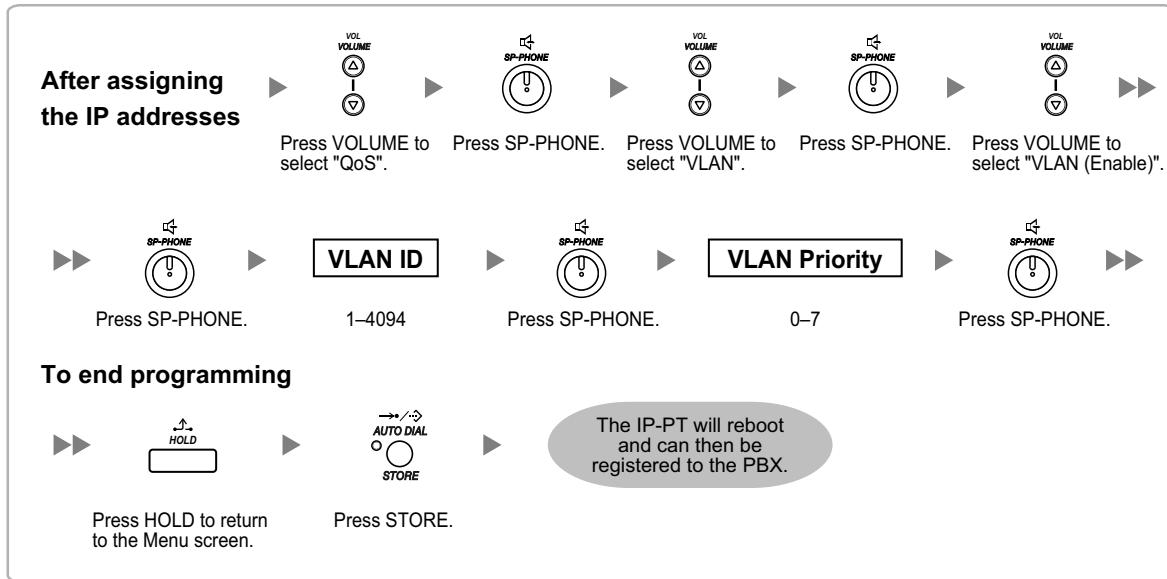
The illustrations may differ from the buttons on your telephone.

KX-NT321/KX-NT551

¹ The VLAN priority of the primary port must be set higher than the priority of the secondary port. The larger the number, the higher the priority.

5.8.2 Setting VLAN Parameters

KX-NT265 (Software version 2.00 or later only)



5.8.3 Setting LLDP Parameters

LLDP-MED is a technique for IP telephones to obtain VLAN settings automatically from a network device, such as a Network Switch.

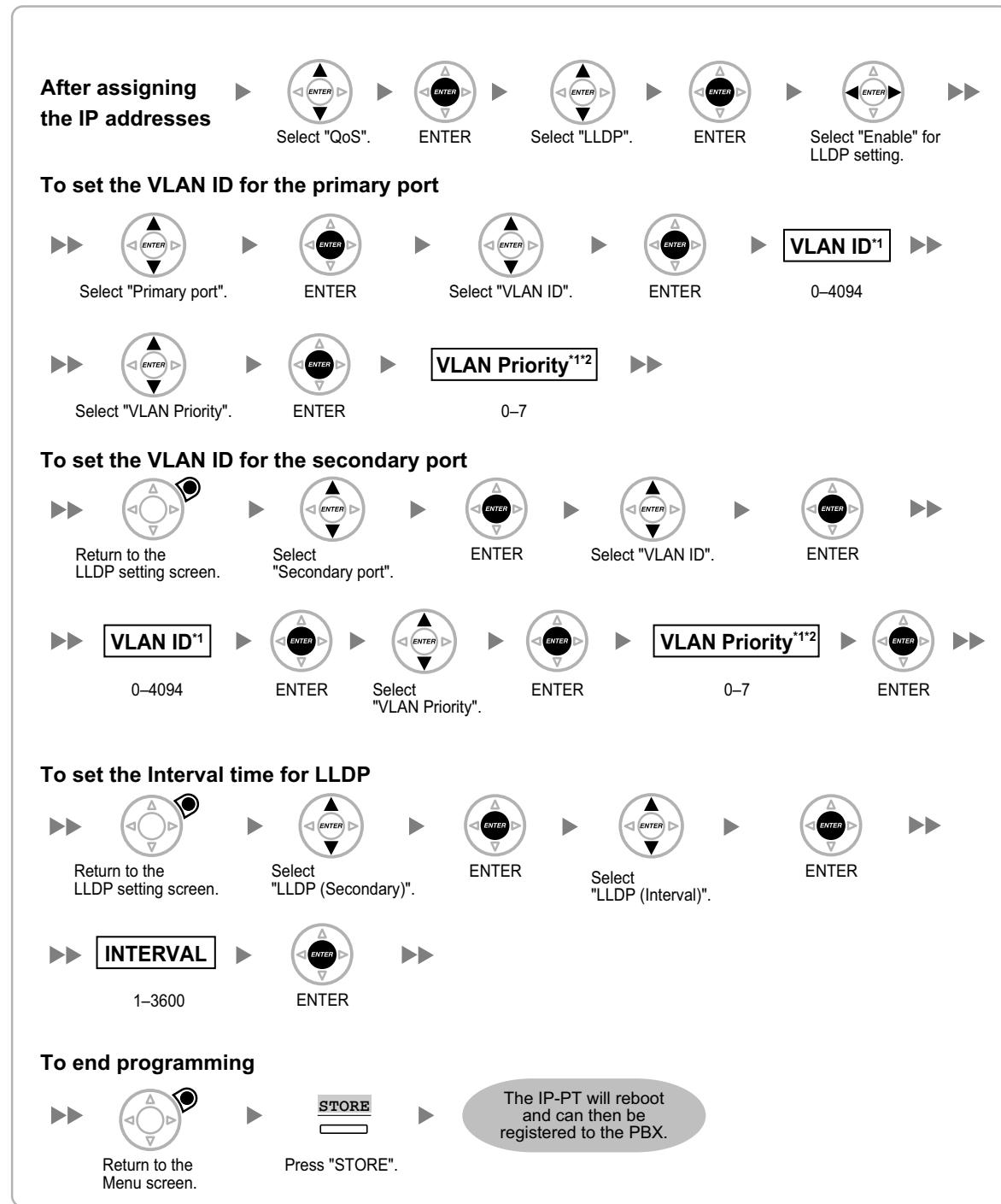
If you are using an IP telephone equipped with two LAN ports, the primary and secondary ports of the IP telephone can be placed on different VLANs by assigning a separate VLAN ID to each port. Follow the procedure below for all IP-PTs on the network, using appropriate VLAN IDs.

Note

- This feature is available only for KX-NT551, KX-NT553, and KX-NT556 IP-PTs.
- VLAN settings configured through PT programming have priority over VLAN settings configured through the LLDP-MED function.
- To enable or disable the sending of LLDP packets from the KX-NS1000, consult your dealer.

5.8.3 Setting LLDP Parameters

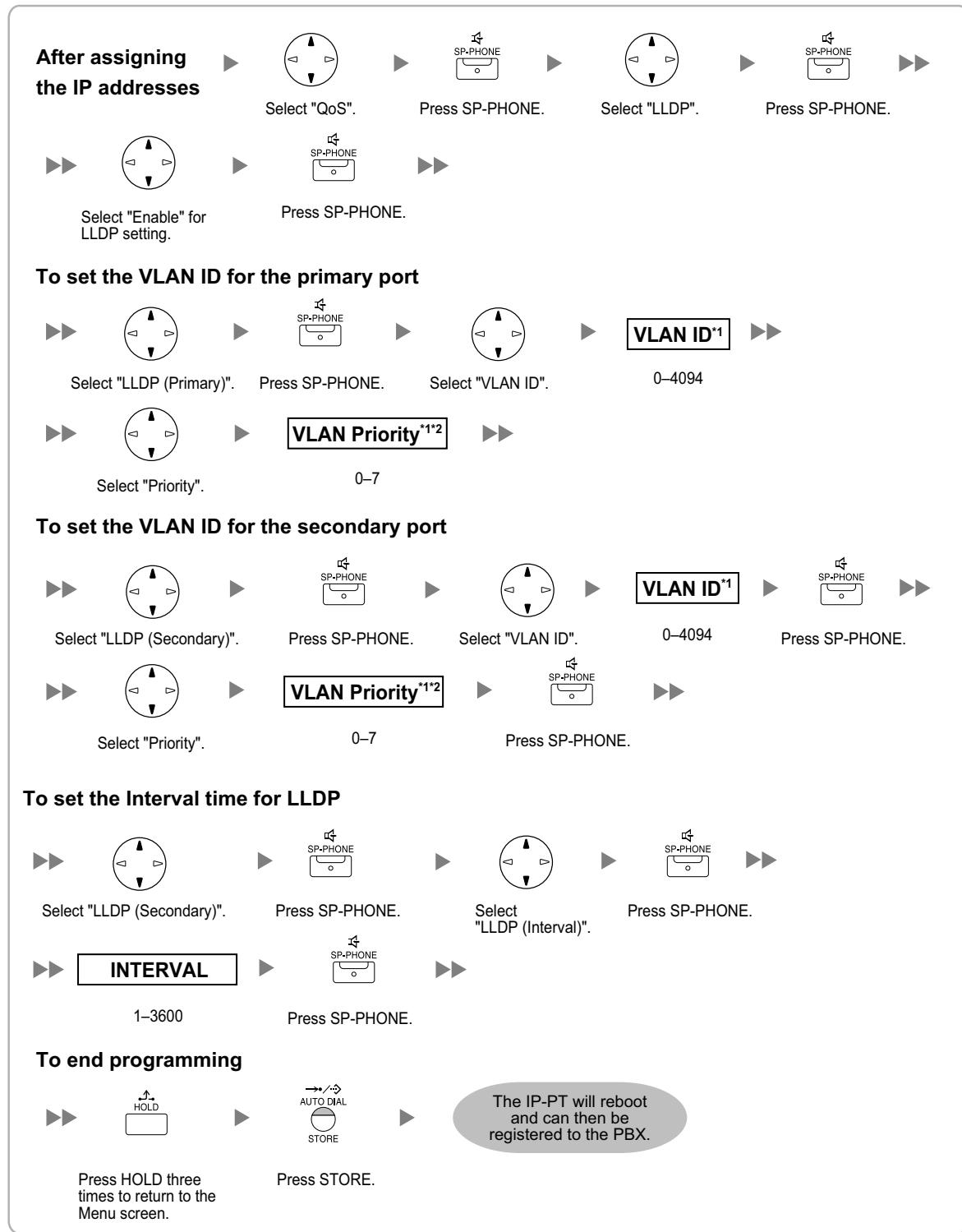
KX-NT553/KX-NT556



^{*1} The VLAN ID and the VLAN priority are set automatically for the primary port; these are reference only. However, the VLAN ID and the VLAN priority for secondary port must be set manually.

^{*2} The VLAN priority of the primary port must be set higher than the priority of the secondary port. The larger the number, the higher the priority.

KX-NT551



¹ The VLAN ID and the VLAN priority are set automatically for the primary port; these are reference only. However, the VLAN ID and the VLAN priority for secondary port must be set manually.

² The VLAN priority of the primary port must be set higher than the priority of the secondary port. The larger the number, the higher

5.8.3 Setting LLDP Parameters

the priority.

5.8.4 Setting Diffserv Parameters

Differentiated Services (DiffServ, or DS) is an IP-based QoS technique used to control QoS of VoIP communications by setting the DS field in the header of IP packets. Consult your network administrator for the appropriate setting values for the DS field.

Follow the procedure below to set the Diffserv parameters. Only KX-NT300 series IP-PTs, KX-NT500 series IP-PTs, and KX-NT265 IP-PTs can be used to set the parameters.

KX-NT300 series (except KX-NT321) and KX-NT500 series (except KX-NT551)

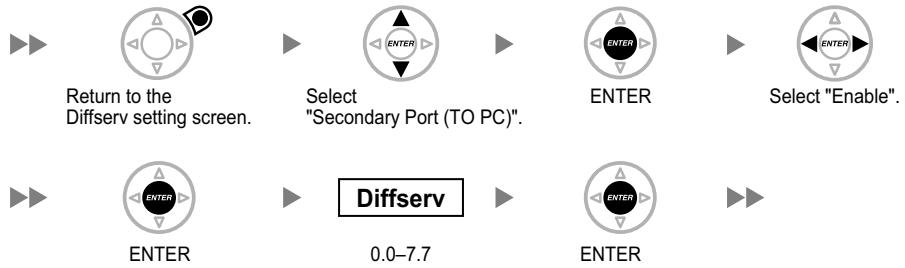
To start programming



To set the DS field value for the primary port



To set the DS field value for the secondary port (only for KX-NT300 series)



To end programming



Note

The illustrations may differ from the buttons on your telephone.

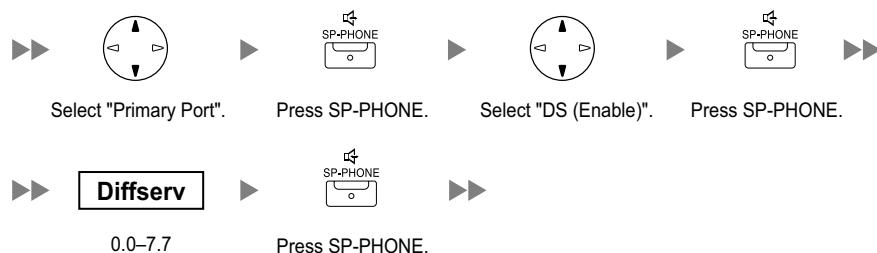
5.8.4 Setting Diffserv Parameters

KX-NT321/KX-NT551

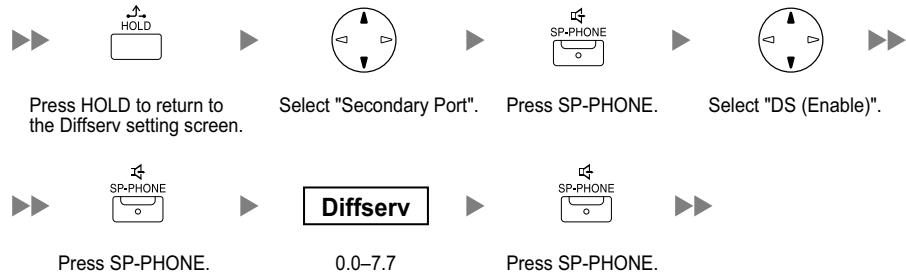
To start programming



To set the DS field value for the primary port



To set the DS field value for the secondary port (only for KX-NT300 series)



To end programming



KX-NT265 (Software version 2.00 or later only)

To start programming



To set the DS field value



To end programming



5.8.5 Configuration of IP Ports

A KX-NT300 series IP-PT user, KX-NT500 series IP-PT user, or KX-NT265 IP-PT user can configure the port number of PTAP, DHCP, and FTP ports. Consult your network administrator to check whether the configuration of the IP ports is required.

Follow the procedure below to configure the port number of the IP ports.

Note

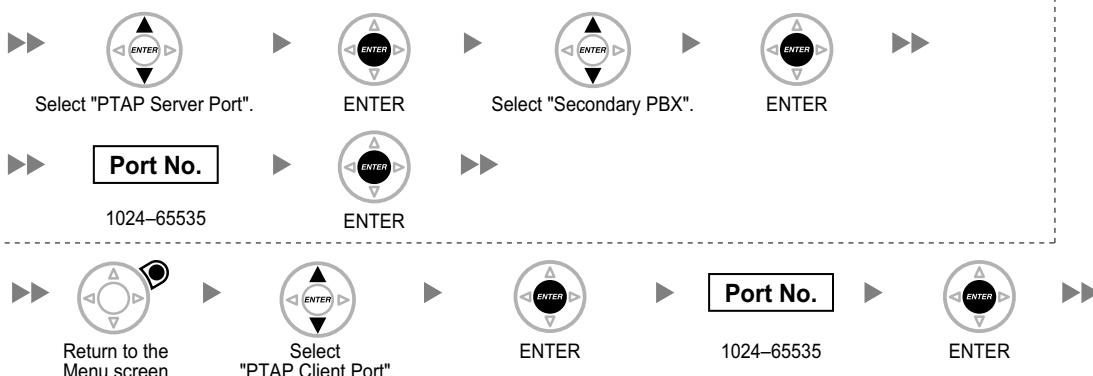
- If you wish to change the port number back to default, enter **0** as the port number for the desired port.
- To delete 1 character, use "**CLEAR**" for KX-NT300 series IP-PTs and KX-NT500 series IP-PTs, or use **[TRANSFER]** for KX-NT265, KX-NT321 and KX-NT551.

KX-NT300 series (except KX-NT321) and KX-NT500 series (except KX-NT551)

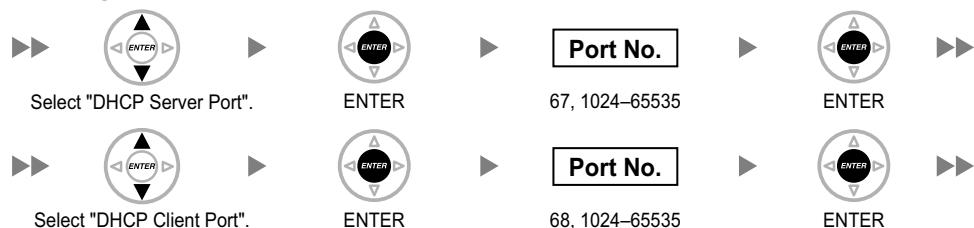
To start programming



To configure the port number of PTAP Ports

To configure the port number of PTAP Ports for the Secondary PBX
(optional for KX-NT300 series [Software version 2.00 or later only] and KX-NT500 series [Software version 1.00 or later only])

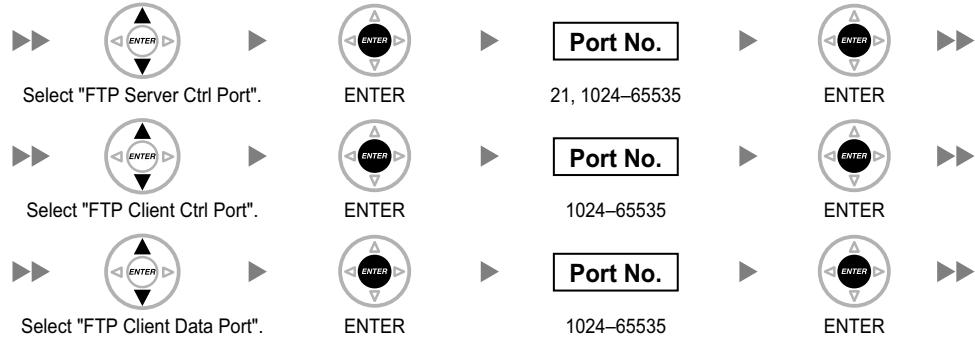
To configure the port number of DHCP Ports



►► Continued on next page

Continued from previous page ►►

To configure the port number of FTP Ports



To end programming



Note

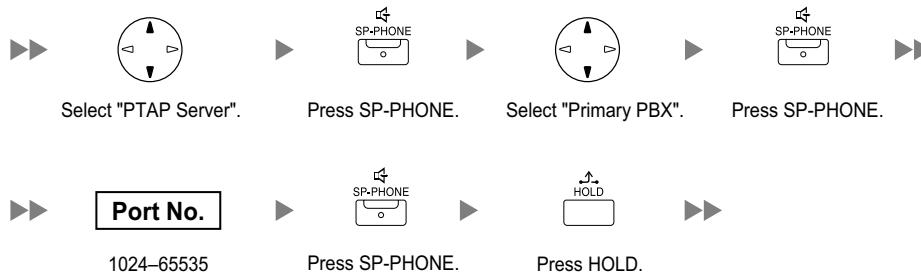
The illustrations may differ from the buttons on your telephone.

KX-NT321/KX-NT551

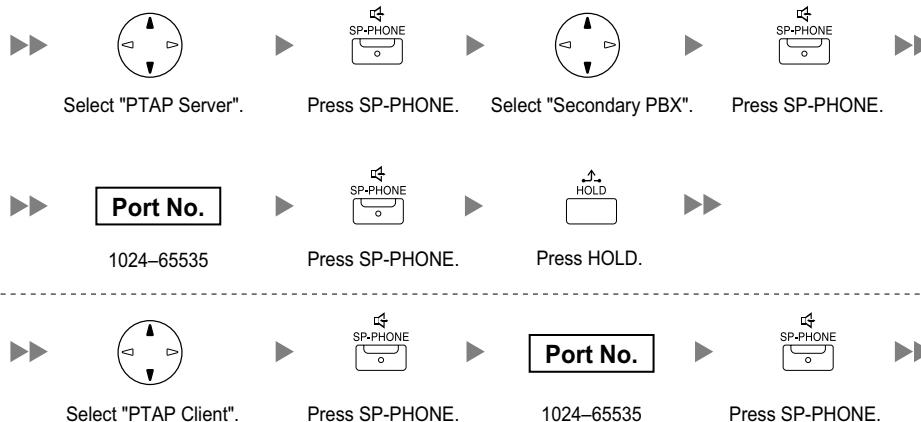
To start programming



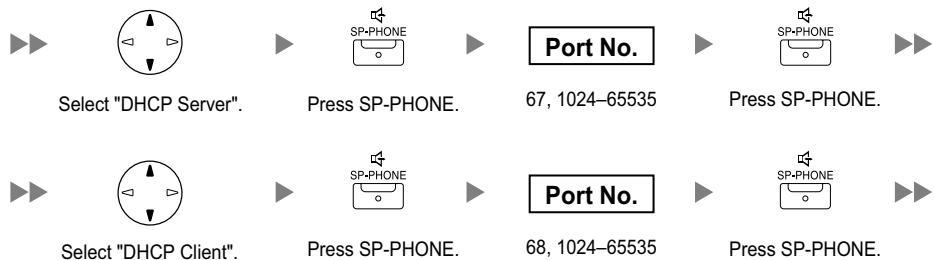
To configure the port number of PTAP Ports



To configure the port number of PTAP Ports for the Secondary PBX (if required)



To configure the port number of DHCP Ports



►► Continued on next page

5.8.5 Configuration of IP Ports

Continued from previous page ►►

To configure the port number of FTP Ports



Select "FTP Server Ctrl". Press SP-PHONE. 21, 1024-65535 Press SP-PHONE.



Select "FTP Client Ctrl". Press SP-PHONE. 1024-65535 Press SP-PHONE.



Select "FTP Client Data". Press SP-PHONE. 1024-65535 Press SP-PHONE.

To end programming



Press HOLD to return to the Menu screen.

Press STORE.

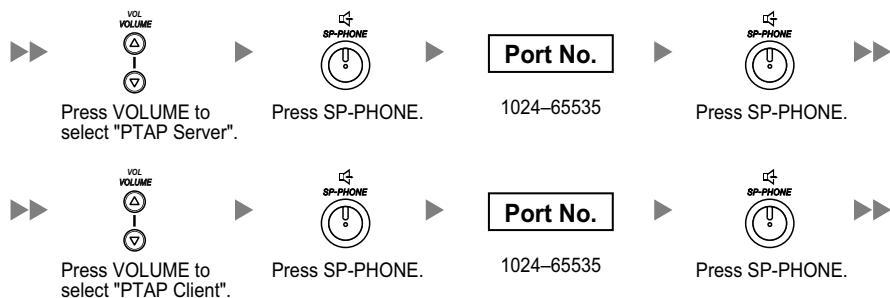
The IP-PT will reboot and can then be registered to the PBX.

KX-NT265 (Software version 2.00 or later only)

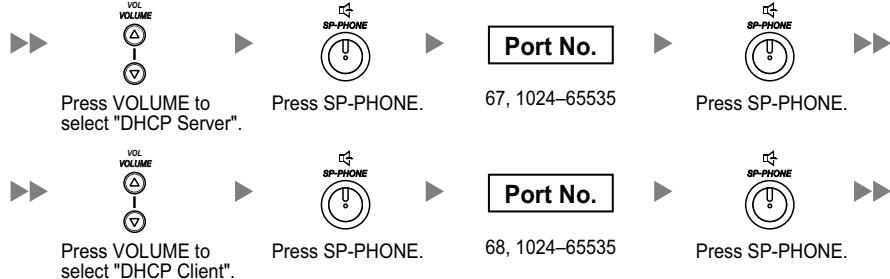
To start programming



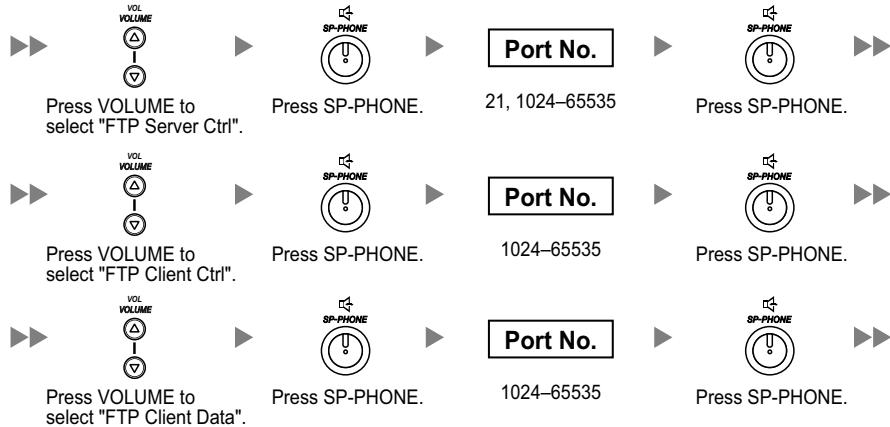
To configure the port number of PTAP Ports



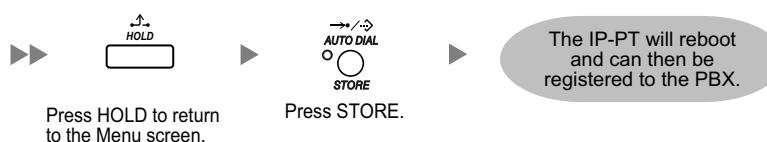
To configure the port number of DHCP Ports



To configure the port number of FTP Ports



To end programming

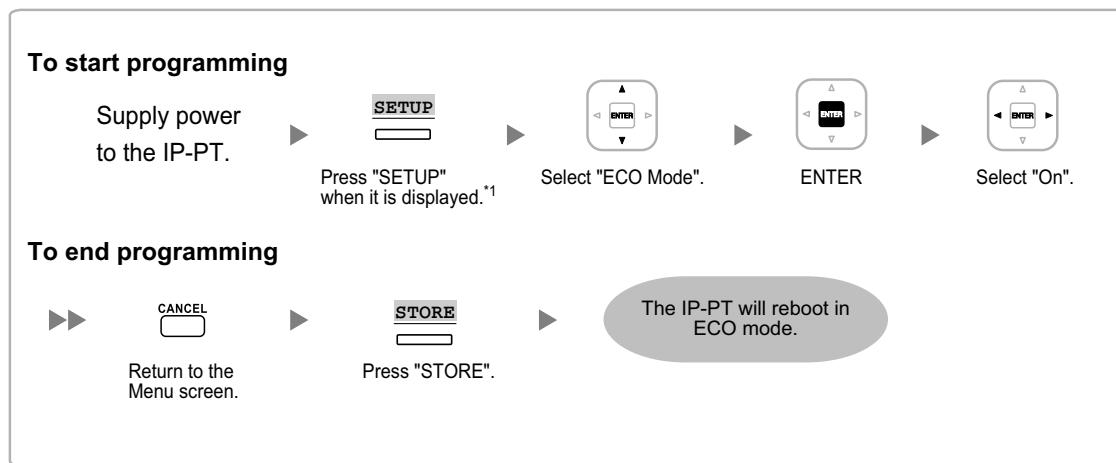


5.8.6 ECO mode (KX-NT500 series only)

5.8.6 ECO mode (KX-NT500 series only)

ECO mode allows a KX-NT500 series IP-PT to consume less power than in normal mode.

To start ECO mode, follow the procedure below.



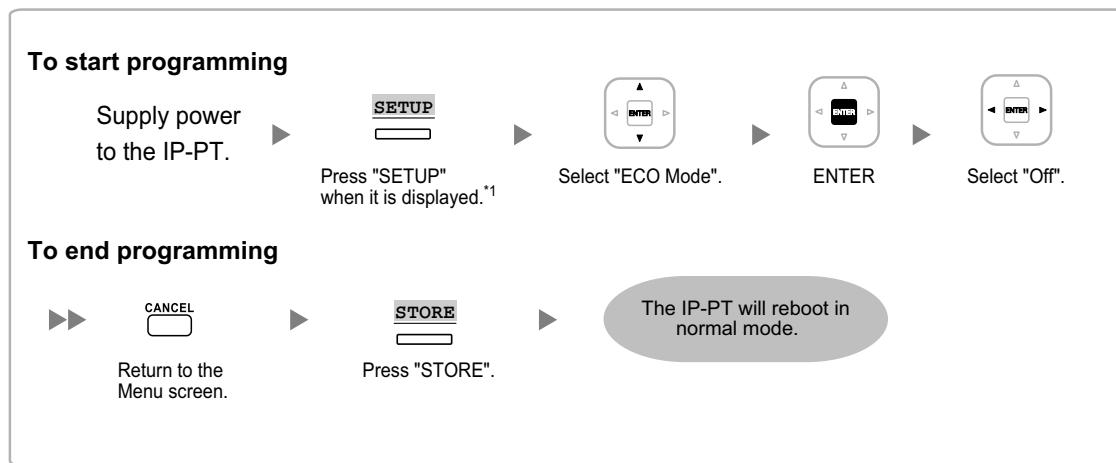
*¹ For KX-NT551 users only

Press PROGRAM when "Searching" is displayed.

Notice

- When a KX-NT500 series IP-PT is in ECO mode, the following limitations are applied:
 - The second Ethernet port is disabled.
 - The port of the switching hub to which the telephone is connected must be 10 Mbps (Fixed)/full duplex.
- For KX-NT500 series IP-PTs (software version 1.010 or later), you can specify the connection mode (Auto Negotiation, 10 Mbps/full duplex, 10 Mbps/half duplex, 100 Mbps/full duplex, 100 Mbps/half duplex). If a connection with Auto Negotiation fails, the connection will be made in either 10 Mbps/half duplex or 100 Mbps/half duplex.

To exit from ECO mode, turn off the KX-NT500 series IP-PT, and then follow the procedure below.



*¹ For KX-NT551 users only

Press PROGRAM when "Searching" is displayed.

Note

The illustrations may differ from the buttons on your telephone.

5.9 Registering IP Telephones

5.9.1 Registering IP Telephones

After the programming of the PBX and IP telephones is finished (refer to "5.8 Assigning Networking Information to IP Telephones"), the IP telephones must be registered to the PBX. The procedure for registering IP telephones differs according to the IP terminal registration mode specified during the Easy Setup Wizard. This setting can also be changed in the **Site Property—Main** screen of the Web Maintenance Console (refer to "9.5.1 PBX Configuration—[1-1] Configuration—Slot—Site Property—Main—Main◆ IP Terminal Registration Mode" in the PC Programming Manual). Refer to the following table:

IP Terminals	IP Terminal Registration Mode		
	Full Automatic Mode	Extension Number Input Mode	Manual Mode
IP-PTs	✓	✓	✓
KX-UT Series SIP Phones	✓	✓ ¹	✓
Non-KX-UT series SIP phones	✓ ²	✓ ²	✓
IP-CSs ³			✓

✓: Available

¹ KX-UT series SIP phones will be registered automatically, in the same way as Full Automatic mode.

² Non-KX-UT series SIP phones must always be registered to the PBX manually, even if Full Automatic mode or Extension Number Input mode is selected.

³ IP-CSs must always be registered to the PBX manually. For details about registering IP-CSs, refer to the Quick Installation Guide for the IP-CS.

Notice

You can specify an air sync group for IP-CSs after registration only when IP Terminal Registration Mode is set to "Manual Mode".

Note

- For KX-UT series SIP phones, the SIP extension password is automatically set to "1234".
- For IP softphones, follow the same registration procedure as IP-PTs.

Full Automatic Mode

If networking settings have been completed, when IP-PTs or KX-UT series SIP phones are connected to the same network as the PBX, they will be registered automatically. No registration procedure is required.

Extension Number Input Mode

For IP-PTs

If networking settings have been completed, when IP-PTs are connected to the same network as the PBX, they will be registered automatically, but extension numbers for the IP-PTs will not be set. Follow the procedure below to register an extension number to complete registration.

- After completing networking settings, connect the IP-PT to the same network as the PBX. The screen to enter the extension number is displayed on the IP-PT.

2. Enter an extension number.

Note

When no extension number is entered in this step, the process will time out and the IP-PT will be registered without an extension number.

3. Press **[ENTER]**¹ on the IP-PT.
4. Press **[PAUSE]** or **"EXIT"** on the IP-PT.

¹ For KX-NT551 and KX-NT321 users, press **[AUTO DIAL/STORE]**.

For models other than the above models that do not have the applicable buttons, consult your dealer.

For KX-UT Series SIP Phones

If networking settings have been completed, when KX-UT series SIP phones are connected to the same network as the PBX, they will be registered automatically as same as when they are registered in Full Automatic mode. No registration procedure is required.

Note

- No more than 64 IP-PTs can register extension numbers at the same time.
- If an extension number that is input for an IP-PT has already been set to another extension, registration by this mode will fail.

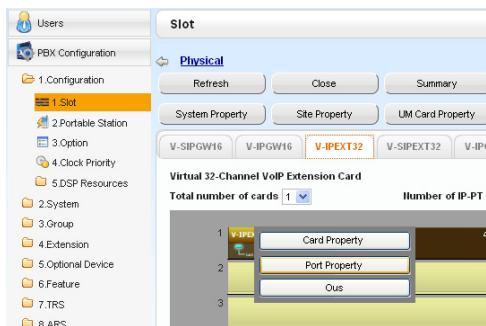
Note that some extension numbers are pre-configured to other extensions by default. Avoid using such numbers, or delete them before starting the registration process.

Manual Mode

For IP-PTs or KX-UT Series SIP Phones

After connecting IP-PTs or KX-UT series SIP phones to the PBX over a network, register those IP terminals to the PBX manually.

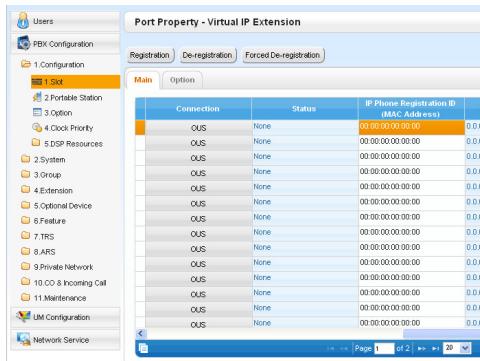
Follow the procedure below for registration.



1. a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
 b. For IP-PTs:
 Click **Virtual** → **V-IPEXT32**.
For KX-UT series SIP phones:
 Click **Virtual** → **V-UTEXT32**.
 c. For IP-PTs:
 Move the mouse pointer over the **V-IPEXT32** card (Virtual 32-Channel VoIP Extension Card).
For KX-UT series SIP phones:
 Move the mouse pointer over the **V-UTEXT32** card (Virtual UT Extension Card).
 A menu will be shown under the mouse pointer.
 d. Click **Port Property**.

To register the IP-PT or KX-UT series SIP phone by entering the MAC address directly:

5.9.1 Registering IP Telephones

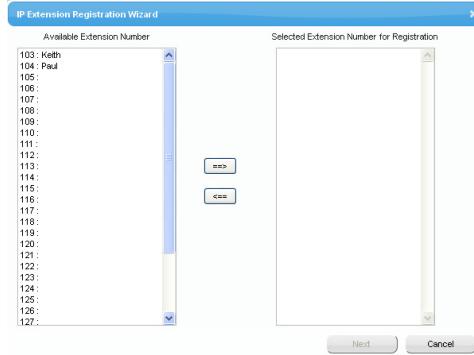


2. If the **Connection** column for the port is **INS**, click **INS**, and then click **OUS** on the dialogue box to change the port's status.
3. Enter the MAC address of the IP-PT or SIP phone in the **IP Phone Registration ID (MAC Address)** cell.
4. **Click Apply.**
Once the IP-PT or SIP phone is successfully registered, its status will update to show "Registered".
5. In the **Connection** column for the port, click **OUS**, and then click **INS** on the dialogue box to change the port's status.
6. For KX-UT series SIP phones only:
Follow the procedure below to change the **IP Terminal Registration Mode** from **Manual** to **Full Automatic**.
 - a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot** → **Site Property** → **Main**.
 - b. In the **Main** tab, select **Full Automatic** for **IP Terminal Registration Mode**.
 - c. Click **OK**.

To register the IP-PT or KX-UT series SIP phone using the wizard:

2. **Click Registration.**
A dialogue box will appear. Non-registered (available) extension numbers and names are displayed on the left.
3.
 - a. Highlight numbers and names and click the right arrow to select them for registration, and then click **Next**.
 - b. Click **Next**. A screen will appear with information on the current IP-PT or SIP phone extension number and name, and index number for programming.

Note



- If the IP-PT or SIP phone has been connected to the LAN and power has been turned on, the IP address of the PBX will be assigned automatically.
- If not, connect the IP-PT or SIP phone to the LAN and turn the power on within 15 minutes after this operation is done. The IP address of the PBX will then be assigned automatically.
- If the registration is still in progress, the dialogue box will show "Registration Executing". If the registration is successful, the dialogue box will show "Registration Completed". Click **Close**. Once the IP-PT or SIP phone is successfully registered, its status will update to show "Registered".

For Non-KX-UT Series SIP Phones

After connecting non-KX-UT series SIP phones to the PBX over a network, register those IP terminals to the PBX manually.

Follow the procedure below for registration.



Slot	Port	Extension Number
1		135
2		136
3		137
4		138
5		139
6		140
7		141
8		142
9		143
10		144
11		145

1.
 - a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
 - b. Click **Virtual** → **V-SIPEXT32**.
 - c. Move the mouse pointer over the V-SIPEXT32 card (Virtual 32-Channel SIP Extension Card). A menu will be shown under the mouse pointer.
 - d. Click **Port Property**.
2. Assign extension numbers to the SIP extensions.
 - If the Automatic Extension Number Set for Extension Card feature is enabled, the extension numbers of SIP extension are automatically assigned. To programme this feature, refer to "9.32 PBX Configuration—[1-3] Configuration—Option—◆ New Card Installation—Automatic Extension Number Set for Extension Card" in the PC Programming Manual.
 - If not, enter the extension number for each SIP extension manually.

5.9.1 Registering IP Telephones

No.	Site	Shelf	Slot	Port	Extension Number	Password	Connection
1	1	Virtual	48	1	136	1234	OUS
2	1	Virtual	48	2	136	1234	OUS
3	1	Virtual	48	3	137	1234	OUS
4	1	Virtual	48	4	138	1234	OUS
5	1	Virtual	48	5	139	1234	OUS
6	1	Virtual	48	6	140	1234	OUS
7	1	Virtual	48	7	141	1234	OUS
8	1	Virtual	48	8	142	1234	OUS
9	1	Virtual	48	9	143	1234	OUS
10	1	Virtual	48	10	144	1234	OUS
11	1	Virtual	48	11	145	1234	OUS
12	1	Virtual	48	12	146	1234	OUS

3. Set passwords for the SIP extensions.
 - a. Click the cell in the **Connection** column for each SIP extension you wish to register. The Command Connection screen appears.
 - b. Click **OUS**.
 - c. Enter a password in the **Password** cell for each SIP extension.
 - d. Click **Apply**.
 - e. Click the cell in the **Connection** column for each SIP extension to which a password has been assigned. The Command Connection screen appears.
 - f. Click **INS**.
 - g. Click **OK**.

Note

- Alternatively, it is possible to set an extension number as a password for each SIP extension automatically.
- In order to set the password automatically, do the following in substitution for step **c** of the procedure above.
 - a. Click **Copy to**. A screen will appear with information on assigned extension numbers for SIP extensions.
 - b. Click **Select All**.
 - c. Click **Execute** to copy each Extension Number to Password.
 - d. Click **Yes**.
 - e. Click **OK** to return to the Port Property screen.
- When copying extension numbers to passwords, you can also use the  icon on the bottom left of the Virtual SIP Extension Port Property screen.

4. Programme the SIP extension you wish to register.
 - a. Set the IP address of the PBX, extension number, and password in the corresponding fields for your SIP extension.
 - b. Send a request from the SIP extension to the PBX for registration.
 - If the authentication information of the SIP extension and the PBX match, the registration is successful.

Note

- When programming the SIP extension, the names of the corresponding fields may differ depending on the type of SIP phone you are using.
- For details about the actual operation of SIP phones, refer to the documentation of the SIP phone.
- For certain SIP phones, you may need to set a Sign-in name, which should consist of the extension number and the IP address of the PBX (e.g., 350@192.168.0.101).

5.9.2 De-registering IP Telephones

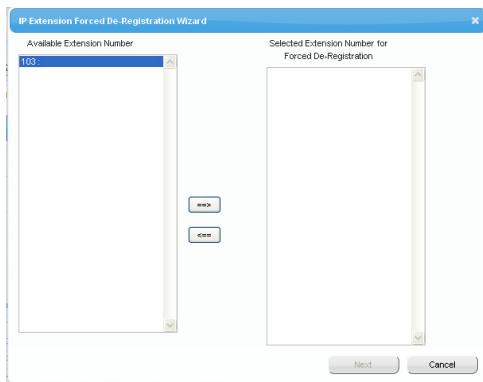
De-registration of IP-PTs or KX-UT Series SIP Phones

1. Make sure the **IP Terminal Registration Mode** is set to **Manual**.
 - a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot** → **Site Property** → **Main**.
 - b. In the **Main** tab, select **Manual** for **IP Terminal Registration Mode**.
 - c. Click **OK**.
2. a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
 - b. For **IP-PTs**:
Click **Virtual** → **V-IPEXT32**.
For KX-UT series SIP phones:
Click **Virtual** → **V-UTEXT32**.
 - c. For **IP-PTs**:
Move the mouse pointer over the **V-IPEXT32** card (Virtual 32-Channel VoIP Extension Card).
For KX-UT series SIP phones:
Move the mouse pointer over the **V-UTEXT32** card (Virtual UT Extension Card).
A menu will be shown under the mouse pointer.
 - d. Click **Port Property**.
3. Click **De-registration**.
A dialogue box will appear. Registered extension numbers and names are displayed on the left.
4. a. Highlight numbers and names and click the right arrow to select them for de-registration.
 - b. Click **Next**.
A dialogue box will appear.
 - c. Click **Confirm**.
 - If the de-registration is successful, the dialogue box will show "De-registration succeed!".
 - d. Click **Close**.

Once the IP-PT or SIP phone is successfully de-registered, the status of the IP telephone will update to show "None".

Forced De-registration of IP-PTs or KX-UT Series SIP Phones

Follow the steps below to forcibly de-register an IP-PT when normal de-registration was unsuccessful.

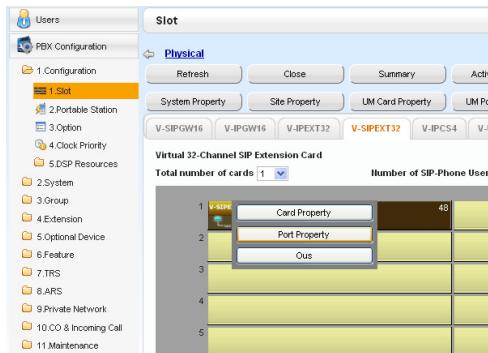


1.
 - a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
 - b. **For IP-PTs:**
Click **Virtual** → **V-IPEXT32**.
For KX-UT series SIP phones:
Click **Virtual** → **V-UTEXT32**.
 - c. **For IP-PTs:**
Move the mouse pointer over the **V-IPEXT32** card (Virtual 32-Channel VoIP Extension Card).
For KX-UT series SIP phones:
Move the mouse pointer over the **V-UTEXT32** card (Virtual UT Extension Card).
A menu will be shown under the mouse pointer.
 - d. Click **Port Property**.
2. Click **Forced De-registration**.
A dialogue box will appear. Registered extension numbers and names are displayed on the left.
3.
 - a. Highlight numbers and names and click the right arrow to select them for de-registration.
 - b. Click **Next**.
A dialogue box will appear.
 - c. Click **OK**.
A dialogue box will appear.
 - d. Click **Confirm**.
 - If the de-registration is successful, the dialogue box will show "Forced de-registration succeed!".
 - e. Click **Close**.

Once the IP-PT or SIP phone is successfully de-registered, the status of the IP telephone will update to show "None".

De-registration of Non-KX-UT Series SIP Phones

The de-registration of non-KX-UT series SIP phones is carried out by deleting either the extension number or password registered in the PBX.



1.
 - a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
 - b. Click **Virtual** → **V-SIPEXT32**.
 - c. Move the mouse pointer over the **V-SIPEXT32** card (Virtual 32-Channel SIP Extension Card). A menu will be shown under the mouse pointer.
 - d. Click **Port Property**.
2.
 - a. Click the cell in the Connection column for the port of the SIP phone to de-register.
 - b. In the Command window, click **Ous** to change the status of the port to "OUS".
3. Repeat step 2 for each SIP phone to de-register.
4. Delete either the extension number or password for the SIP phone to de-register, as shown here.
5. Click **OK**.

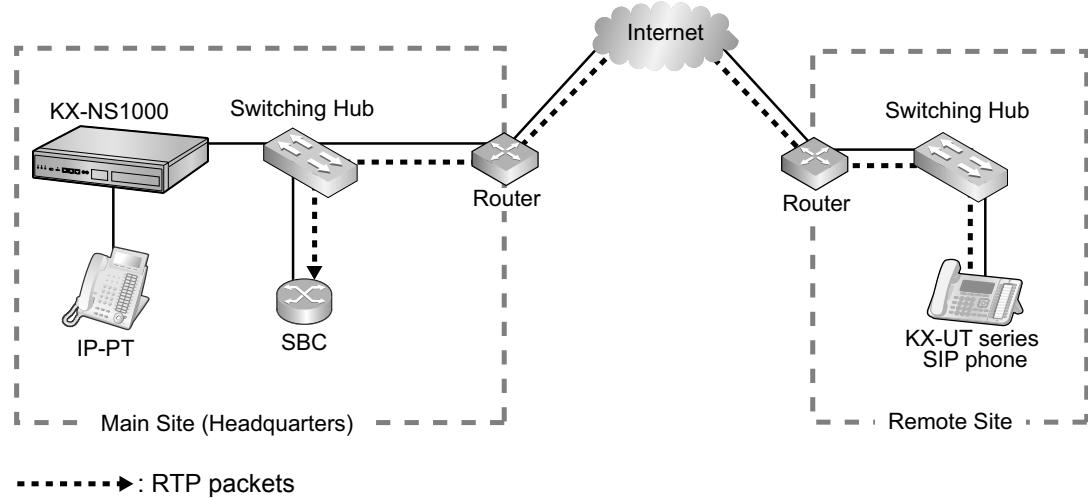
Extension			
Slot	Port	Extension Number	Password
48	1	135	1234
48	2	136	1234
48	3	137	1234
48	4	138	1234
48	5	139	1234
48	6	140	1234
48	7	141	1234
48	8	142	1234
48	9	143	1234
48	10	144	1234
48	11	145	1234
48	12	146	1234
48	13	147	1234
48	14	148	1234

5.9.3 Installing SIP Phones at a Remote Site

If an SBC (Session Border Controller) is present on the same local network as the KX-NS1000, you can install SIP phones at remote sites without needing to configure special network settings (NAT traversal, etc.).

This section provides information about the procedure for connecting SIP Phones at a remote site that has SBC hardware.

When SIP phones in remote sites use the internet to communicate with the PBXs, use the HTTPS protocol for security. If the connection is within a VPN and protected, you may use the HTTP protocol.



Note

- Install the SBC in the same LAN as the KX-NS1000.
- A KX-NS1000 can work with only one SBC. Also, multiple sites can share an SBC.
- A KX-NS1000 can support up to 20 remote extensions at the same time via SBC when using the HTTPS protocol.
- All the RTP packets in between the main site and the remote site is routed to the SBC for security and for IP address conversion.
- When settings of remote extensions being used at remote sites are changed at the KX-NS1000 at the main site, the reflection of the changes to the remote extension may require some time due to data transfer protocols.

Programming the KX-NS1000

Follow the procedures below to configure remote port settings using Web Maintenance Console.

Note

For the procedures below, programme WAN side IP information of the router at the main site. This information is sent to KX-UT series SIP phones at the remote site after completing all programming.

For Site Property Settings

1. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
2. Move the mouse pointer over **Site Property**.
A menu will be shown under the mouse pointer.
3. Click **Main**.
4. Click the **SIP Extension** tab.
5. Click **Advanced Setting for Remote SIP-MLT**.
Programme the WAN side IP information in **Setting parameters assigned to Remote SIP-MLT**.

5.9.3 Installing SIP Phones at a Remote Site

- a. Programme the following common settings.

Configure the following items in **Setting parameters assigned to Remote SIP-MLT**.

WAN Side IP information of the router at the main site	Web Maintenance Console Parameter
CWMP	
IP Address	NAT - CWMP Server IP Address
SIP	
IP Address	NAT - SIP Proxy Server IP Address
Port Number	NAT - SIP Proxy Server Port No.
NTP	
IP Address	NAT - NTP Server IP Address
Port Number	NAT - NTP Server Port No.

- b. Programme the following settings according to the protocol used by KX-UT series SIP phones in the remote site.

When the KX-UT series SIP phones are using HTTPS

WAN Side IP information of the router at the main site	Web Maintenance Console Parameter
CWMP	
Port Number	NAT - CWMP Server (HTTPS) Port No.
For Data Download	
Port Number	NAT - SIP-MLT Data Download Server (HTTPS) Port No.

When the KX-UT series SIP phones are using HTTP

WAN Side IP information of the router at the main site	Web Maintenance Console Parameter
CWMP	
Port Number	NAT - CWMP Server (HTTP) Port No.
For Data Download	
Port Number	NAT - SIP-MLT Data Download Server (HTTP) Port No.

6. Click **OK**.
7. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
8. Move the mouse pointer over **Site Property**.
A menu will be shown under the mouse pointer.
9. Click **Main**.
10. Click **Port Number** tab.
11. Programme the following items according to the protocol used by KX-UT series SIP phones in the remote site.
 - a. When the KX-UT series SIP phones are using HTTPS:
 - **CWMP (HTTPS) Port No. for SIP-MLT**
 - **Data Transmission Protocol (HTTPS) Port No. for SIP-MLT**
 - b. When the KX-UT series SIP phones are using HTTP:
 - **CWMP (HTTP) Port No. for SIP-MLT**
 - **Data Transmission Protocol (HTTP) Port No. for SIP-MLT**

Note

For the default port numbers of the KX-NS1000, refer to "8.5 Port Security".

12. Click **OK**.
13. Make a backup of the data that includes the above settings.
Click **Setup** → **System Control** → **System Reset** → **Backup**.

Using a KX-NS1000 as an NTP server

When the KX-NS1000 will be used as a NTP server, follow the procedures below.

1. Click **Setup** → **Network Service** → **Server Feature** → **NTP**.
2. Select **Enable**.
3. Click **OK**.

Programming the SBC

The following items need to be configured on the SBC. For information about configuring the SBC, refer to the documentation of the SBC.

- IP address of the KX-NS1000
- Port numbers of the KX-UT series SIP phones installed in the remote site
- IP address and subnet mask of the SBC
- LAN side IP address of the router at the main site
- WAN side IP address of the router at the main site
- SIP receiving port settings (For details, refer to the documentation of your SBC)

Note

For SIP receiving port of the SBC, specify the same port number that is specified at **NAT - SIP Proxy Server Port No.** in step 5 in "Programming the KX-NS1000" in this section.

- RTP Start Port (UDP) and RTP End Port (UDP)

Note

Make sure the RTP Start Port (UDP) and RTP End Port (UDP) specified for the SBC above are in the range of the RTP port numbers that KX-NS1000 uses.

For range of RTP port number of KX-NS1000, refer to "Port Numbers for Optional DSP Cards" in "8.5 Port Security".

- Firewall settings to allow SIP packets and RTP packets

Programming the router at the main site

Port forwarding settings (Router – SBC)

Configure the following items for port forwarding in between the SBC and the router.

Application	LAN Side Port Number	WAN Side Port Number
SIP Proxy	NAT-SIP Proxy Port No. (Use the same value as NAT - SIP Proxy Server Port No. in step 5 of "Programming the KX-NS1000".)	NAT-SIP Proxy Port No. (Use the same value as NAT - SIP Proxy Server Port No. in step 5 of "Programming the KX-NS1000".)
RTP (UDP)	Start/End RTP (UDP) Port No. (Use port numbers that are in the range of the RTP ports that the KX-NS1000 uses.)	Start/End RTP (UDP) Port No. (Use port numbers that are in the range of the RTP ports that the KX-NS1000 uses.)

Make sure the RTP Start Port (UDP) and the RTP End Port (UDP) specified for the router are in the range of the RTP ports that the KX-NS1000 uses.
For the range of RTP port numbers that the KX-NS1000 uses, refer to "Port Numbers for Optional DSP Cards" in "8.5 Port Security".

Note

For information about configuring port forwarding on the router, refer to the documentation of the router.

Port forwarding settings (Router – KX-NS1000)

Configure the following items for port forwarding between the KX-NS1000 and the router.

Application	LAN Side Port Number	WAN Side Port Number
CWMP		
HTTP	CWMP (HTTP) Port No. for SIP-MLT (Use the same value as in step 11 of "Programming the KX-NS1000".)	NAT - CWMP Server (HTTP) Port No. (Use the same value as in step 5 of "Programming the KX-NS1000".)
HTTPS	CWMP (HTTPS) Port No. for SIP-MLT (Use the same value as in step 11 of "Programming the KX-NS1000".)	NAT - CWMP Server (HTTPS) Port No. (Use the same value as in step 5 of "Programming the KX-NS1000".)
SIP-MLT Data		
HTTP	Data Transmission Protocol (HTTP) Port No. for SIP-MLT (Use the same value as in step 11 of "Programming the KX-NS1000".)	NAT - SIP-MLT Data Download Server (HTTP) Port No. (Use the same value as in step 5 of "Programming the KX-NS1000".)
HTTPS	Data Transmission Protocol (HTTPS) Port No. for SIP-MLT (Use the same value as in step 11 of "Programming the KX-NS1000".)	NAT - SIP-MLT Data Download Server (HTTPS) Port No. (Use the same value as in step 5 of "Programming the KX-NS1000".)

Application	LAN Side Port Number	WAN Side Port Number
NTP	123 ¹	NAT - NTP Server Port No. (Use the same value as in step 5 of "Programming the KX-NS1000".)

¹ The port number for NTP that the KX-NS1000 uses is fixed to 123.

Note

For information about configuring port forwarding on the router, refer to the documentation of the router.

Installing KX-UT series SIP phones at a remote site

There are 2 methods to install KX-UT series SIP phones at a remote site:

- Set up KX-UT series SIP phones at the main site using the KX-NS1000, and then send them to the remote site.
- Set up KX-UT series SIP phones without connecting them to the KX-NS1000 at the main site, and then send them to the remote site.

Setting up KX-UT series SIP phones at the main site, and then sending them to remote site

1. Register the KX-UT series SIP phone. For details, refer to "5.9.1 Registering IP Telephones".
2. Programme the settings for the KX-UT series SIP phones.
 - a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
 - b. Click **Virtual** → **V-UTEXT32**.
 - c. Move the mouse pointer over the V-UTEXT32 card (Virtual UT Extension Card).
A menu will be shown under the mouse pointer.
 - d. Click **Port Property**.
 - e. Click **Remote Place** tab.
 - f. Configure the items shown below.
 - Select a protocol (HTTP/HTTPS) for **Protocol for Remote SIP-MLT**.

Note

When a SIP phone at remote site uses the internet to communicate with a KX-NS1000, use the HTTPS protocol for security. If the connection is on VPN and protected, you may use the HTTP protocol.

- a. Change the value to **Remote (SBC)** for **Phone Location**.
 - g. Click **OK**.
3. Unplug the AC adaptor of the KX-UT series SIP phone, and then plug it in again to reboot the KX-UT series SIP phone manually.
The KX-UT series SIP phone will download settings automatically.

Note

- After downloading the setting information for the remote site, the KX-UT series SIP phone will not connect to the KX-NS1000 if it is connected to the LAN at the main site. After some time, the KX-UT series SIP phone will display "9002: Connection Failed".
 - Depending on the settings of your router, the KX-UT series SIP phone may connect to the PBX. In such cases, proceed to step 4.
4. Send the KX-UT series SIP phone to the remote site and connect it to the LAN in the remote site.

Note

The KX-UT series SIP phone is already registered to the KX-NS1000 and programmed with the remote site configuration. There is no operation required for the KX-UT series SIP phone at the remote site.

Setting up KX-UT series SIP phones without connecting to the KX-NS1000 at the main site, and then sending them to the remote site

1. Log in to the Web Maintenance Console of the site where the SIP phones will be registered. For details about logging in to a Slave unit via the Master unit, refer to "3.1 Home Screen" in the PC Programming Manual.
2. Click **Utility** → **File** → **File Transfer PBX to PC**.
3. Select the config file according to the protocol used and then download it to your PC.
 - HTTP is used
 - UT_ACS_xxxyy.cfg
 - HTTPS is used
 - UT_ACS_HTTPS_xxxyy.cfg

For more details about downloading files from a PBX to a PC, refer to "7.2.2 Utility—File—File Transfer PBX to PC" in the PC Programming Manual.

Note

xx: Site ID (2 digits)

yyyy: Site name¹ (Up to 32 characters²)

¹ Spaces as well as the following characters in site names will be replaced with underscores.

/, :, *, ?, ", <, >, | (vertical bar), &, +

² In some cases, the full site name may not be included in the file name even if it is less than 32 characters.

4. Download the config file to the KX-UT series SIP phone via the Web user interface of the KX-UT series SIP phone.
For details, refer to "When the SIP Phones are in a different LAN (Remote site installation)" in "5.8.1 Assigning IP Addressing Information".
5. Connect the KX-UT series SIP phone to the LAN at the remote site.
6. Register the KX-UT series SIP phone to the KX-NS1000 as a remote extension.
 - a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
 - b. Click **Virtual** → **V-UTEXT32**.
 - c. Move the mouse pointer over the V-UTEXT32 card (Virtual UT Extension Card).
A menu will be shown under the mouse pointer.
 - d. Click **Port Property**.
 - e. Click **Remote Place** tab.
 - f. Configure the items shown below.
 - Change the value to **Remote (SBC)** for **Phone Location**.
 - Change the value to **Enable** for **Web-MC Ability**.
 - Select a protocol (HTTP/HTTPS) for **Protocol for Remote SIP-MLT**.

Note

Select the same value as you selected for **NAT - SIP Proxy Server Port No.** in step 5 of "Programming the KX-NS1000" in this section.

- a. Click **OK**.
7. Register the KX-UT series SIP phone. For details, refer to "5.9.1 Registering IP Telephones".

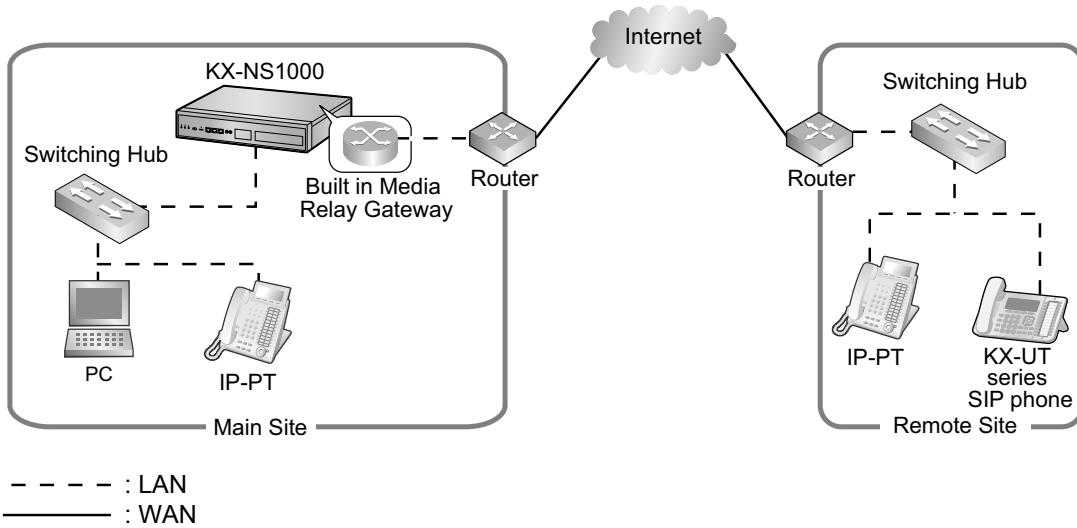
Note

- You can select **HTTPS** for **Protocol for Remote SIP-MLT** only when **Phone Location** is set as **Remote (SBC)**.
- If the KX-UT series SIP phones don't work normally, confirm if the KX-UT series SIP phones are able to access to internet.

5.9.4 Installing IP Phones at a Remote Site with a Built-in Media Relay Gateway

The KX-NS1000 contains a built-in Media Relay Gateway.

You can install and register IP-PTs (KX-NT500 series), KX-UT series SIP phones and third party SIP phones at a remote site without adding an SBC (Session Border Controller). Also, you do not need to configure special network settings (NAT traversal, etc.) at the remote site.



Note

- This feature does not require an activation key.
- There is no limit to the number of terminals that can use the Media Relay Gateway feature. However, there are some conditions, as follows:
 - Peer-to-peer communication is not supported for the built-in Media Relay Gateway.
 - The number of terminals using TR-069 (CWMP)-based HTTPS is limited.
- For information about which telephone models support the built-in Media Relay Gateway, consult your dealer.

Programming the KX-NS1000 with Built-in Media Relay Gateway

Follow the procedures below to configure remote port settings using Web Maintenance Console.

Note

For the procedures below, programme WAN side IP information of the router at the main site. This information is sent to KX-NT500 series or KX-UT series SIP phones in the remote site after completing all programming.

For Site Property Settings

1. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
2. Move the mouse pointer over **Site Property**.
A menu will be shown under the mouse pointer.
3. Click **Main**.
4. Click the **Media Relay** tab.

5.9.4 Installing IP Phones at a Remote Site with a Built-in Media Relay Gateway

5. Programme the WAN side information in **Media Relay** tab.
- a. Programme the following common settings in **Common**.

WAN Side IP information of the router at the main site	Web Maintenance Console Parameter
IP Address	NAT - External IP Address¹

¹ You can also programme individual items of the **NAT - External IP Address**. For more details, see step e.

- b. Programme the following settings according to the protocol used by the KX-NT500 series IP extensions in the remote site. Configure the following items in **IP Extension**.

WAN Side IP information of the router at the main site	Web Maintenance Console Parameter
MGCP	
Port Number	NAT - MGCP Server Port No.

- c. Programme the following settings according to the protocol used by the KX-UT series IP extensions and SIP extensions in the remote site. Configure the following items in **SIP Extension / UT Extension**.

WAN Side IP information of the router at the main site	Web Maintenance Console Parameter
SIP	
Port Number	NAT - SIP Proxy Server Port No.

- d. Programme the following settings according to the protocol used by the KX-UT series IP extensions in the remote site. Configure the following items in **UT Extension**.

- When the KX-UT series SIP phones are using HTTPS:

WAN Side IP information of the router at the main site	Web Maintenance Console Parameter
CWMP	
Port Number	NAT - CWMP Server (HTTPS) Port No.
Port Number	NAT - CWMP Server (HTTPS) Port No. for Network Survivability
For Data Download	
Port Number	NAT - SIP-MLT Data Download Server (HTTPS) Port No.

- When the KX-UT series SIP phones are using HTTP:

WAN Side IP information of the router at the main site	Web Maintenance Console Parameter
CWMP	

WAN Side IP information of the router at the main site	Web Maintenance Console Parameter
Port Number	NAT - CWMP Server (HTTP) Port No.
Port Number	NAT - CWMP Server (HTTP) Port No. for Network Survivability
For Data Download	
Port Number	NAT - SIP-MLT Data Download Server (HTTP) Port No.

- e. Programme the following common settings in **Option**.

WAN Side IP information of the router at the main site	Web Maintenance Console Parameter
RTP	
IP Address	NAT - RTP IP Address
SIP	
IP Address	NAT - SIP Proxy Server IP Address
CWMP	
IP Address	NAT - CWMP Server IP Address
IP Address	NAT - CWMP Server IP Address for Network Survivability
NTP	
IP Address	NAT - NTP Server IP Address

If necessary, you can programme the individual settings here and overwrite the **NAT - External IP Address** setting programmed in step a.

6. Click **OK**.
7. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
8. Move the mouse pointer over **Site Property**.
A menu will be shown under the mouse pointer.
9. Click **Main**.
10. Click the **Port number** tab.
11. Programme the following items according to the protocol used by KX-UT series SIP phones in the remote site.
 - a. When the KX-UT series SIP phones are using HTTPS:
 - **CWMP (HTTPS) Port No. for SIP-MLT**
 - **Data Transmission Protocol (HTTPS) Port No. for SIP-MLT**

- b. When the KX-UT series SIP phones are using HTTP:

- **CWMP (HTTP) Port No. for SIP-MLT**
- **Data Transmission Protocol (HTTP) Port No. for SIP-MLT**

Note

For the default port numbers of the KX-NS1000, refer to "8.5 Port Security".

12. Click OK.

Using a KX-NS1000 as an NTP server

When the KX-NS1000 will be used as a NTP server, follow the procedures below.

1. Click **Setup** → **Network Service** → **Server Feature** → **NTP**.
2. Select **Enable**.
3. Click OK.

Programming the router at the main site with Built-in Media Relay Gateway

Port forwarding settings (Router – KX-NS1000)

Configure the following items for port forwarding between the Media Relay Gateway and the router.

For the KX-NT500 series:

Application	LAN Side Port Number	WAN Side Port Number
PTAP	Signalling (PTAP) UDP Port No. (Server) (refer to PC Programming Guide "9.14 PBX Configuration—[1-1] Configuration—Slot—V-IPEXT32—Card Property")	Signalling (PTAP) UDP Port No. (Server) (refer to PC Programming Guide "9.14 PBX Configuration—[1-1] Configuration—Slot—V-IPEXT32—Card Property")
MGCP	Signalling (MGCP) UDP Port No. (Server) (refer to PC Programming Guide "9.14 PBX Configuration—[1-1] Configuration—Slot—V-IPEXT32—Card Property")	NAT - MGCP Server Port No. (Use the same value as in step 5 of "Programming the KX-NS1000 with Built-in Media Relay Gateway".)
RTP (UDP)	Start/End RTP (UDP) Port No. (Use port numbers that are in the range of the RTP ports that the KX-NS1000 uses.) ¹	Start/End RTP (UDP) Port No. (Use port numbers that are in the range of the RTP ports that the KX-NS1000 uses.) ¹
	Make sure the RTP Start Port (UDP) and the RTP End Port (UDP) specified for the router are in the range of the RTP ports that the KX-NS1000 uses. For the range of RTP port numbers that the KX-NS1000 uses, refer to "Port Numbers for Optional DSP Cards" in "8.5 Port Security". ¹	

¹ The port number ranges must be within the range of RTP/RTCP for NAT traversal (16000–18047). Up to 4 IP addresses can be assigned to the KX-NS1000's optional DSP cards. The following example shows the port number ranges set for each IP address:

[Example]

Port forward destination	Port number range
DSP#1–1	16000–16511

DSP#1-2	16512-17023
DSP#2-1	17024-17535
DSP#2-2	17536-18047

For the KX-UT series:

Application	LAN Side Port Number	WAN Side Port Number
SIP Proxy	UDP Port No. for SIP Extension Server (refer to PC Programming Guide "9.5.1 PBX Configuration—[1-1] Configuration—Slot—Site Property—Main—Port Number")	NAT-SIP Proxy Port No. (Use the same value as NAT - SIP Proxy Server Port No. in step 5 of "Programming the KX-NS1000 with Built-in Media Relay Gateway")
CWMP		
HTTP	CWMP (HTTP) Port No. for SIP-MLT (Use the same value as in step 11 of "Programming the KX-NS1000 with Built-in Media Relay Gateway".)	NAT - CWMP Server (HTTP) Port No. (Use the same value as in step 5 of "Programming the KX-NS1000 with Built-in Media Relay Gateway".)
HTTPS	CWMP (HTTPS) Port No. for SIP-MLT (Use the same value as in step 11 of "Programming the KX-NS1000 with Built-in Media Relay Gateway".)	NAT - CWMP Server (HTTPS) Port No. (Use the same value as in step 5 of "Programming the KX-NS1000 with Built-in Media Relay Gateway".)
SIP-MLT Data		
HTTP	Data Transmission Protocol (HTTP) Port No. for SIP-MLT (Use the same value as in step 11 of "Programming the KX-NS1000 with Built-in Media Relay Gateway".)	NAT - SIP-MLT Data Download Server (HTTP) Port No. (Use the same value as in step 5 of "Programming the KX-NS1000 with Built-in Media Relay Gateway".)
HTTPS	Data Transmission Protocol (HTTPS) Port No. for SIP-MLT (Use the same value as in step 11 of "Programming the KX-NS1000 with Built-in Media Relay Gateway".)	NAT - SIP-MLT Data Download Server (HTTPS) Port No. (Use the same value as in step 5 of "Programming the KX-NS1000 with Built-in Media Relay Gateway".)
NTP	123 ¹	NAT - NTP Server Port No. (Use the same value as in step 5 of "Programming the KX-NS1000 with Built-in Media Relay Gateway".)

5.9.4 Installing IP Phones at a Remote Site with a Built-in Media Relay Gateway

Application	LAN Side Port Number	WAN Side Port Number
RTP (UDP)	Start/End RTP (UDP) Port No. (Use port numbers that are in the range of the RTP ports that the KX-NS1000 uses.) ²	Start/End RTP (UDP) Port No. (Use port numbers that are in the range of the RTP ports that the KX-NS1000 uses.) ²

¹ The port number for NTP that the KX-NS1000 uses is fixed to 123.

² The port number ranges must be within the range of RTP/RTCP for NAT traversal (16000–18047). Up to 4 IP addresses can be assigned to the KX-NS1000's optional DSP cards. The following example shows the port number ranges set for each IP address:

[Example]

Port forward destination	Port number range
DSP#1-1	16000–16511
DSP#1-2	16512–17023
DSP#2-1	17024–17535
DSP#2-2	17536–18047

Installing KX-NT500 series IP-PTs at a remote site with Built-in Media Relay Gateway

You can install KX-NT500 series IP-PTs at the remote site directly or from the local site as follows.

1. Register the IP-PT. For details, refer to "5.9.1 Registering IP Telephones".
2. Programme the settings for the IP-PT.
 - a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
 - b. Click **Virtual** → **V-IPEXT32**.
 - c. Move the mouse pointer over the V-IPEXT32 card (Virtual 32-Channel VoIP Extension Card). A menu will be shown under the mouse pointer.
 - d. Click **Port Property**.
 - e. Click the **Remote Place** tab.
 - f. Configure the items shown below.
 - Change the value to **Remote (MRG)** for **Phone Location**.
 - g. Click **OK**.
3. Unplug the AC adaptor of the IP-PT, and then plug it in again to reboot the IP-PT manually. The IP-PT will download settings automatically.

Installing KX-UT series SIP phones at a remote site with Built-in Media Relay Gateway

There are 2 methods to install KX-UT series SIP phones at a remote site:

- Set up the phones at the main site using the KX-NS1000, and then send them to the remote site.
- Set up the phones without connecting them to the KX-NS1000 at the main site, and then send them to the remote site.

Setting up KX-UT series SIP phones at the main site, and then sending them to remote site

1. Register the phone. For details, refer to "5.9.1 Registering IP Telephones".
2. Programme the settings for the phone.
 - a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
 - b. Click **Virtual** → **V-UTEXT32**.
 - c. Move the mouse pointer over the **V-UTEXT32** card (Virtual UT Extension Card). A menu will be shown under the mouse pointer.
 - d. Click **Port Property**.
 - e. Click the **Remote Place** tab.
 - f. Configure the items shown below.
 - Change the value to **Remote (MRG)** for **Phone Location**.
 - Select a protocol (HTTP/HTTPS) for **Protocol for Remote SIP-MLT**.

Note

When a SIP phone at a remote site uses the internet to communicate with a KX-NS1000, use the HTTPS protocol for security. If the connection is on a VPN and is protected, you may use the HTTP protocol.

- g. Click **OK**.
3. Unplug the AC adaptor of the phone, and then plug it in again to reboot the phone manually. The phone will download settings automatically.

Note

- After downloading the setting information for the remote site, the KX-UT series SIP phone will not connect to the KX-NS1000 if it is connected to the LAN at the main site. After some time, the KX-UT series SIP phone will display "9002: Connection Failed".
- Depending on the settings of your router, the KX-UT series SIP phone may connect to the PBX. In this case, proceed to step 4.

4. Send the KX-UT series SIP phone to the remote site and connect it to the LAN in the remote site.

Note

The KX-UT series SIP phone is already registered to the KX-NS1000 and programmed with the remote site configuration. No operation is required for the KX-UT series SIP phone in the remote site.

Setting up KX-UT series SIP phones without connecting to the KX-NS1000 at the main site, and then sending them to the remote site

1. Log in to Web Maintenance Console of the site where the SIP phones will be registered. For details about logging in to a Slave unit via the Master unit, refer to "3.1 Home Screen" in the PC Programming Manual.
2. Click **Utility** → **File** → **File Transfer PBX to PC**.
3. Select the config file according to the protocol used and then download it to your PC.
 - If HTTPS is used:
 - **UT_MRGS_HTTPS_xxyyyy.cfg**

For more details about downloading files from a PBX to a PC, refer to "7.2.2 Utility—File—File Transfer PBX to PC" in the PC Programming Manual.

Note

xx: Site ID (2 digits)

yyyy: Site name¹ (Up to 32 characters)²

¹ Spaces as well as the following characters in site names will be replaced with underscores.

/, :, *, ?, ", <, >, | (vertical bar), &, +

² In some cases, the full site name may not be included in the file name even if it is less than 32 characters.

4. Download the config file to the KX-UT series SIP phone via the Web user interface of the KX-UT series SIP phone. For details, refer to "When the SIP Phones are in a different LAN (Remote site installation)" in "5.8.1 Assigning IP Addressing Information".
5. Connect the KX-UT series SIP phone to the LAN in the remote site.
6. Register the KX-UT series SIP phone to the KX-NS1000 as a remote extension.
 - a. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
 - b. Click **Virtual** → **V-UTEXT32**.
 - c. Move the mouse pointer over the V-UTEXT32 card (Virtual UT Extension Card). A menu will be shown under the mouse pointer.
 - d. Click **Port Property**.
 - e. Click the **Remote Place** tab.
 - f. Configure the items shown below.
 - Change the value to **Remote (MRG)** for **Phone Location**.
 - Change the value to **Enable** for **Web-MC Ability**.
 - Select a protocol (HTTP/HTTPS) for **Protocol for Remote SIP-MLT**.

Note

Select the same value as you selected for **NAT - SIP Proxy Server Port No.** in step 5 of "Programming the KX-NS1000" in this section.

- g. Click **OK**.
7. Register the KX-UT series SIP phone. For details, refer to "5.9.1 Registering IP Telephones".

Note

- You can select **HTTPS** for **Protocol for Remote SIP-MLT** only when **Phone Location** is set as **Remote (MRG)**.
- If the KX-UT series SIP phone does not work normally, confirm whether the KX-UT series SIP phone can access the internet.

5.10 Configuration of Users

The system manages information about each user.

Before programming other user settings, the following information must be configured for each user:

- Extension number
- Name
- Unified Messaging mailbox
- Web Maintenance Console login account (ID and password)

Follow the procedure below to efficiently programme basic personal information by adding multiple users with the Add Range feature.

1. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.

Add one or more extension cards to the system, according to your equipment and needs. Extension numbers will be automatically created for each extension card that is added. For details about adding extension cards, refer to "9.1 PBX Configuration—[1-1] Configuration—Slot" in the PC Programming Manual.

2. Click **Setup** → **PBX Configuration** → **Extension**.

Enter an extension name for each extension number to be used. For details, refer to the following sections in the PC Programming Manual:

- 12.1.1 PBX Configuration—[4-1-1] Extension—Wired Extension—Extension Settings
- 12.2.1 PBX Configuration—[4-2-1] Extension—Portable Station—Extension Settings

Note

You also can import extension names from a CSV file. For details refer to "6.6 Tool—Import" in the PC Programming Manual.

3. Click **Setup** → **Users** → **User Profiles**.

Select **Rule of copy to extension name** on the **Option** tab.

- **Rule-A: [First Name] [space] [Last Name]**
- **Rule-B: [Last Name] [,] [First Name]**

4. Click **Setup** → **Users** → **User Profiles**.

You can create multiple user profiles automatically by using the Add Range feature for extension numbers. You can also set an extension number, first name, last name, Unified Messaging mailbox, and Web Maintenance Console login account for each user manually.

For details, refer to "User Controls" in "8.1 Users—User Profiles" in the PC Programming Manual.

For each user profile added using the Add Range feature, the following information is automatically assigned:

- **First Name/Last Name**

Extension Name, which is the name displayed on extension LCDs, can be copied all at once to the **First Name** and **Last Name** settings for each extension.

The format you selected in **Rule of copy to extension name** in step 3 determines how these are copied.

- Case 1: You selected Rule-A, and the format of the name is assumed to be "[First Name] (space) [Last Name]".
- Case 2: You selected Rule-B, and the format of the name is assumed to be "[Last Name], [First Name]".
- Case 3: **Extension Name** is set to not follow **Rule of copy to extension name**:

Example of copying Extension Name

	Extension Name	User Profile	
		First Name	Last Name
Case 1	Tarou Yamada	Tarou	Yamada

	Extension Name	User Profile	
		First Name	Last Name
Case 2	Yamada,Tarou	Tarou	Yamada
Case 3	TarouYamada	Ext. 101	TarouYamada

- **Login ID:** The extension number (i.e., if the extension is "101", the Login ID for the user will also be "101")
 - **Password:** "PWD" + the extension number for the user (e.g., "PWD101")
5. If additional editing is required for users, settings can be configured on the following screens:
- To edit user information: **Setup → Users → User Profiles**
 - To edit extension settings: **Setup → PBX Configuration → Extension**
 - To edit mailbox settings: **Setup → UM Configuration → Mailbox Settings**

Note

- You also can create mailboxes for Incoming Call Distribution Groups on the **Mailbox Settings** screen.
- Since the Built-in Unified Messaging System is part of this PBX, the settings of the following items are shared between the PBX and Unified Messaging system.
 - Date and time, and enable/disable settings in **Holiday Table**
The following 2 items are shared. For details, refer to the PC Programming Manual.
 - 10.5 PBX Configuration—[2-5] System—Holiday Table
 - 23.4 UM Configuration—[4-4] Service Settings—Holiday Table
 - Mailboxes with the same mailbox number as their associated extension numbers
When the same mailbox number is used as the extension number, it is possible to select whether the system keeps the two synchronised (i.e., one changes when the other does). For details about the setting, refer to "10.9 PBX Configuration—[2-9] System—System Options—Option 9" in the PC Programming Manual.
For instance, when an extension number is changed, the mailbox number of the mailbox assigned to that extension changes to match the new extension number. However, if a mailbox with the same number already exists, the mailbox number will not change.
 - Mailbox COS
When assigning COS levels to user profiles (either extension or mailbox), by default the extension COS and mailbox COS are set to the same level. You can specify whether these values are synchronised by the system.
For details, refer to "10.9 PBX Configuration—[2-9] System—System Options—Option 9" in the PC Programming Manual.
If enabled, when one COS setting is changed, the other will change to match the new setting. (When this setting is first enabled, the extension COS setting is used as the mailbox COS.)
 - Since the outside line access number and trunk call (transfer) procedures are synchronised in the PBX settings, each outside line access number (e.g., idle line access, trunk group access, specified line access) are available for features that make calls (e.g., External Message Delivery). These features will first recognise the outside line access number part of a number, and then perform dial tone detection, etc.

5.11 Programming E-mail Integration for UM Voice/Fax Messages

Users with Unified Messaging (UM) mailboxes (referred to below as "subscribers") can receive their voice or fax messages as data using the following methods:

- Receiving attachments to a POP3 e-mail account
- Accessing data through an IMAP4 e-mail account

Note

KX-NSU201, KX-NSU205, KX-NSU210, KX-NSU220, or KX-NSU299 (Activation Key for Unified Messaging E-mail Notification) is required to enable this feature for users.

For details about these activation keys, see "Unified Messaging System (Mailbox)" in "3.1.1 Type and Maximum Number of Activation Keys".

Receiving Attachments to a POP3 E-mail Account

An e-mail can be sent to Unified Message system subscribers, notifying them of a new voice or fax message. Subscribers can also choose to have the voice message and/or fax data attached to the notification, as well as choose to have the message deleted from the system after it has been sent.

1. Specify SMTP server settings.
 - a. Click **Setup** → **Network Service** → **Server Feature** → **SMTP**.
 - b. Specify the name to be used for the e-mail messages that will be sent from the system in **Mail sending—Mail sender information name**.
 - c. Specify the e-mail address for the e-mail messages that will be sent from the system in **Mail sending—Mail Address**.
 - d. Specify the IP address or host name of the SMTP server to use in **SMTP server for relay—SMTP server address**.
 - e. Specify the port number of the SMTP server to use in **SMTP server for relay—SMTP server Port number**.
 - f. Specify the following parameters if required.
 - **SMTP over TLS**
 - **SMTP Authentication**
 - **POP before SMTP**
 - **Receive Port number (SMTP)**
 - **Receive Port number (SMTPs)**

Note

For details about these parameters, refer to "28.2.5 Network Service—[2-6] Server Feature—SMTP" in the PC Programming Manual.

- g. Click **OK**.
2. Specify e-mail options.
 - a. Click **Setup** → **UM Configuration** → **System Parameters** → **Parameters** → **E-mail Option**.
 - b. Specify the following parameters.
 - **Mail Address (Up to 128 ASCII characters)**
 - **Full Name (Up to 64 ASCII characters)**
 - **Maximum Message Length (Selection)**
 - **Maximum Message Length (Other) (1-30 min)**
 - c. Click **OK**.
3. Enable e-mail notification.
 - a. Click **Setup** → **UM Configuration** → **Class of Service** → **General**.
 - b. In **E-mail Option**, select **Yes** for all Class of Service members that will receive e-mail notifications.

- c. Click **OK**.
4. Specify notification parameters.
 - a. Click **Setup** → **UM Configuration** → **Mailbox Settings** → **Notification Parameters**.
 - b. Click **Edit** in **E-mail/Text Message Device**.
 - c. Specify the following parameters for **Device No. 1, 2, and 3** as required.
 - **User name**
 - **E-mail Address**
 - **Notification Type**
 - **Only Urgent Messages**
 - **Title Order**
 - **Title String**
 - **Callback Number**
 - **Send Wait Time [0-120 min]**
 - **Attach Voice File**
 - **Attach Fax File**
 - **Use Mode**

Note

For details about these parameters, refer to "20.1 UM Configuration—[1] Mailbox Settings—Notification Parameters" in the PC Programming Manual.

- d. Click **OK**.

Accessing Data Through an IMAP4 E-mail Account

Downloading the IMAP Session Controller Software

When more than 24 users will be accessing data through IMAP4 e-mail accounts, each user must use the IMAP Session Controller software.

The IMAP Session Controller software can be downloaded from Web Maintenance Console:

1. Log in with a User level account.
The **Edit User** screen is displayed.
2. Click the **Unified Message** tab.
3. Click **Download for Unified Messaging Plug in** to access the download site for the IMAP Session Controller software.

Note

For details about installing and setting up the IMAP Session Controller software, refer to the User Manual.

Configuring IMAP Accounts

By configuring an IMAP account, subscribers can access the contents of their UM mailboxes through an e-mail client. All that is necessary is an e-mail client that supports IMAP4.

Once IMAP integration is programmed, users can do the following:

- Listen to voice messages or view fax messages
 - Save voice and fax message data to their PCs
 - Delete voice and fax messages stored on the PBX
1. Enable IMAP integration.
 - a. Click **Setup** → **UM Configuration** → **Class of Service** → **General**.
 - b. In **Desktop Messaging**, select **Yes** for all Class of Service members that will use IMAP integration.
 - c. Click **OK**.
 2. Specify the mailbox password.
 - a. Click **Setup** → **UM Configuration** → **Mailbox Settings** → **Mailbox Parameters**.
 - b. Click **Edit** in **Mailbox Password (Message Client)**.

- c. Enter a password in **Enter new password**.
 - d. Enter the password again in **Confirm new password**.
 - e. Click **OK**.
 - f. Click **OK**.
3. Specify IMAP parameters.
- a. Click **Setup** → **Network Service** → **Server Feature** → **IMAP4**.
 - b. Specify the following parameters (if required).
 - **IMAP4 server**
 - **Port Number**
 - **IMAP4 over SSL**
 - **CAPABILITY command**
 - **Authenticated Connection Timeout**

Note

For details about these parameters, refer to "28.2.6 Network Service—[2-7] Server Feature—IMAP4" in the PC Programming Manual.

- c. Click **OK**.

Setting Up the IMAP Account in a Subscriber's E-mail Client

An account must be set up in each subscriber's e-mail client for use with the Unified Messaging system. The setup procedure will vary depending on the e-mail client application used and the configuration of your network. When adding the account, the settings must be specified as follows:

- The e-mail address will be the subscriber's existing e-mail address.
- The type of the account must be set to "IMAP".
- The incoming mail server must be set as the IP Address of the PBX where the subscriber's UM mailbox is located.
- The user name/ID will be the subscriber's UM Mailbox Number.
- The password will be the **Mailbox Password (Message Client)** set in step 2 above.
- A valid SMTP server must be used (i.e. the SMTP server used for existing mail accounts).

Note

- To allow faxes to be received and stored in a mailbox:
 1. Click **Setup** → **UM Configuration** → **Class of Service** → **General**.
 2. In **Fax Option**, select **Yes** for all Class of Service members that will receive faxes.
 3. Click **OK**.
- A FAX card (KX-NS0106) must be installed in the main unit to send or receive faxes.

The following example setup procedure is for Microsoft Outlook® 2010. Subscribers' e-mail client setting names and locations may differ.

1. In Outlook 2010, select **File**, and then **Info**.
2. Click the **Add Account** button.
3. Select **Manually configure server settings or additional server types**.
4. Select **Internet E-mail**, and then click **Next**.
5. Configure the server settings as follows:

User Information

- In **Your Name**, enter the name of the subscriber. (In the example, "John Smith")
- In **E-mail Address**, enter the existing mail address of the subscriber. (In the example below, "j.smith@example.com")

Server Information

- Select **IMAP** for **Account type**.

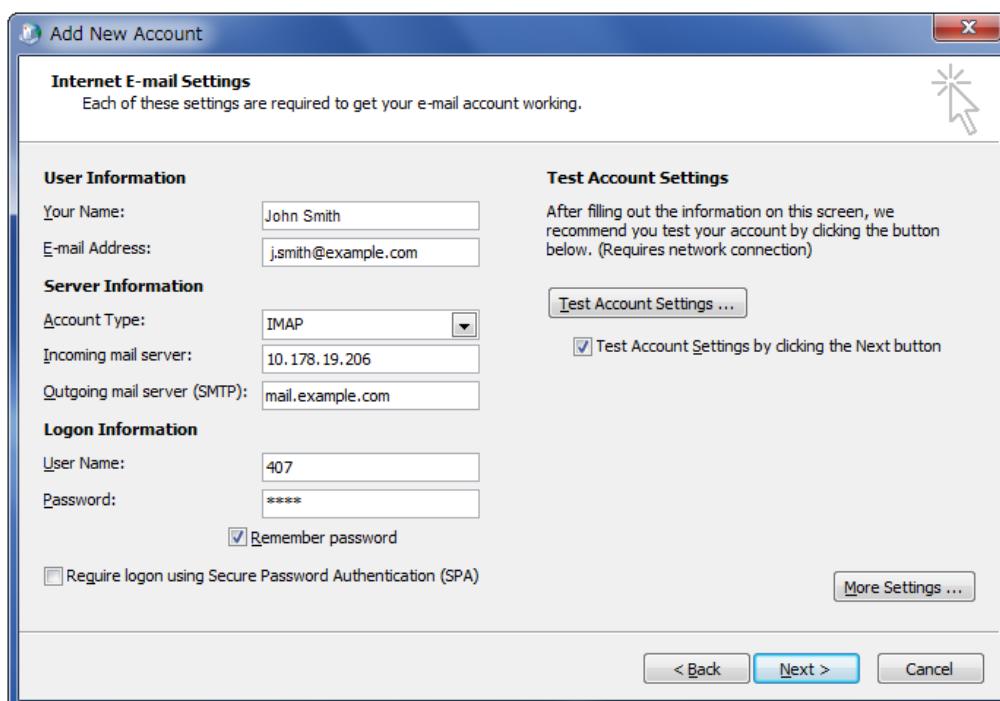
- In **Incoming mail server**, enter the IP address of the PBX where the subscriber's UM mailbox is located. (In the example below, "10.178.19.206")
- In **Outgoing mail server (SMTP)**, enter the SMTP server used for the subscriber's existing mail account. (In the example below, "mail.example.com")

Logon Information

- In **User Name**, enter the subscriber's Mailbox Number. (In the example below, "407")
- In **Password**, enter the password for the subscriber specified in **Mailbox Password (Message Client)**.

6. Click **Next** and then complete the account settings.

Example IMAP Account Settings (Outlook 2010)



5.12 Automatic Configuration of Mailboxes

Mailboxes can be automatically created and associated with an extension number if these items do not already exist. There are 2 modes for creating mailboxes. For each specified extension number, a mailbox is automatically created if one is not already associated with the extension. The results of creating and associating mailboxes and user profiles with extension numbers are output both to a file and to the syslog. If many mailboxes must be created or deleted, the amount of time required to complete the task is displayed on the screen.

Creating mailboxes for all extensions

Note

If a mailbox does not satisfy the conditions for automatic creation, neither will be created for the corresponding extension.

1. In Web Maintenance Console, click Setup-UM Configuration-Mailbox Settings-Auto Configuration-Create all mailboxes.
2. Select the radio button where you want the mailboxes to be created.
 - Create mailboxes to the UM group of the PBX where extensions belong to
 - Create mailboxes to the specified UM group (UM Group No. 1 to 16)
3. Click Execute.
 - Mailboxes are created with the same number as the extension number.
 - However, a mailbox will not be created in any of the following conditions:
 - a. A mailbox with the same number as the extension number already exists
 - b. The extension number has only 1 digit
 - c. The total number of mailboxes, including already existing mailboxes, exceeds 1024
 - d. The extension number has wild cards used with MSN (Multiple Subscriber Number) provided by ISDN (e.g., 21X, 40XX)

Re-creating all mailboxes

IMPORTANT

This procedure deletes all existing voice data, all settings and all prompts from all mailboxes. In this procedure, voice data (e.g., mailbox voice data, personal greetings) and settings (e.g., the password) are not deleted from the managers' mailboxes. Be sure to make a backup of any important data beforehand. If mailbox numbers are changed after mailboxes have been deleted using this feature, even if a backup of the mailbox settings, voice data (e.g., personal greetings), and messages has been made, the data cannot be restored. After executing this function, all messages will have been deleted, and it is necessary to reconfigure all mailbox settings and re-record all prompts.

1. In Web Maintenance Console, click Setup→UM Configuration→Mailbox Settings→Auto Configuration→Re-create all mailboxes
2. Select the radio button where you want the mailboxes to be created.
 - Create mailboxes to the UM group of the PBX where the extensions belong to
 - Create mailboxes to the specified UM group (UM Group No. 1 to 16)
3. Click Execute.
 - Every type of mailbox, except the manager's mailboxes, will be deleted.
 - If there are currently mailboxes in use, you can select whether to delete them forcibly or cancel the operation.
 - All mailboxes will be recreated.
 - A mailbox will not be created in the following conditions:
 - The extension number has only 1 digit

Results of creating mailboxes

The results of creating mailboxes are recorded in a text file. Follow the procedure below to view the file.

1. When automatic configuration completes, click OK on the "Mailbox create result" dialogue box.
2. Mailbox_result.txt is saved to the local PC.
3. The meaning of the status in the generated file is as follows:

User Profile Status	Description
Exist	The user profile already existed and was assigned to the related mailbox and extension number.
Skipped	The user profile was already assigned to the related mailbox and extension number.

Mailbox Status	Description
Created	The new mailbox was successfully created.
Failed	The new mailbox was not created.
Assigned	The mailbox already existed, but was successfully assigned to the related extension number.
Exist	The mailbox was already assigned to the related extension number.
Skipped	The mailbox already existed, but assigning it to the related extension number failed.

The start and finish times of the automatic configuration is recorded in the syslog (INFO). For details, refer to "7.3.2 Utility—Log—Syslog" in the PC Programming Manual.

Section 6

Information about Stacking PBXs

This section provides information about stacking PBXs as legacy gateways.

6.1 Information about Stacking PBXs

Stacking KX-NCP series PBXs, KX-TDE series PBXs, KX-TDA series PBXs, or KX-TDA100D PBXs, with the KX-NS1000 allows you to design your PBX communication environment taking advantage of existing facilities. When PBXs are stacked, the KX-NS1000 will control communication, as well as all IP terminals on the site.

Note

The RS-232C ports of legacy gateways connected to a KX-NS1000 are not available.

For details about connecting a KX-NS1020 as a legacy gateway to a KX-NS1000, refer to the KX-NS1020 Installation Manual.

6.2 Methods of Stacking PBXs

There are 4 ways of stacking PBXs with the KX-NS1000.

Case 1

Stacking PBXs to a Stand-alone KX-NS1000 (not running).

To stack PBXs to a KX-NS1000 which is not running currently, refer to "Procedure for Case 1 and Case 2".

Case 2

Stacking PBXs to a Stand-alone KX-NS1000 (running).

To stack PBXs to a KX-NS1000 which is already running, refer to "Procedure for Case 1 and Case 2".

Case 3

Stacking PBXs to a KX-NS1000 running in a One-look network.

To stack PBXs after starting up One-look networking, refer to "Procedure for Case 3".

Note

- The order of installing legacy gateways to the Master units or Slave units is up to the user.
- Stop running the One-look network when stacking PBXs to the Master unit.
- Stop running the site when stacking PBXs to a Slave unit.

Case 4

Stacking PBXs to a Stand-alone KX-NS1000 (running) and then adding the site to a One-look network.

In a One-look network, the Master unit controls the system data of the Slave units.

To start up a One-look network with KX-NS1000s which already have stacked PBX(s), refer to "Procedure for Case 4".

Stacking Procedures

The following procedures show how to stack PBXs in each case.

CAUTION

- When installing or removing the optional service cards, the power switch must be turned off.
- When installing or removing the optional service cards, do not put pressure on any parts of the mother board. Doing so may result in damage to the PBX.

Notice

If there is already a PBX stacked and connected to a STACK-M card installed in a KX-NS1000, you can skip shutting down the KX-NS1000 in the following procedures.

Note

- For information about starting the KX-NS1000 for the first time, refer to "4.13 Starting the KX-NS1000".
- The PBXs connected as legacy gateways will be initialised when started up with a STACK-S (NCP)/STACK-S (TDE) card mounted and extension numbers will be created automatically.

Procedure for Case 1 and Case 2

1. Follow the procedure below for the PBXs to be connected as legacy gateways.
 - a. Make sure the power switch is turned off. If the KX-NS1000 is running, shutdown the KX-NS1000 and then turn off the power switch.
 - b. Remove the MPR card, and then insert a STACK-S (NCP)/STACK-S (TDE) card.
 - c. Connect the stacking cable to the STACK-S (NCP)/STACK-S (TDE) card.

2. Follow the procedure below for the KX-NS1000.
 - a. Make sure the power switch is turned off.
 - b. Insert a STACK-M card into the free slot.
 - c. Connect the stacking cable to the STACK-M card.
3. Follow the procedure below for the KX-NS1000 and legacy gateways.
 - a. Turn the power switch on.

Procedure for Case 3

To stack PBXs to a running Master unit or Slave unit in a One-look network, follow the procedure below.

1. Follow the procedure below for the PBXs to be connected as legacy gateways.
 - a. Make sure the power switch is turned off.
 - b. Remove the MPR card, and then insert a STACK-S (NCP)/STACK-S (TDE) card.
 - c. Connect the stacking cable to the STACK-S (NCP)/STACK-S (TDE) card.
2. Follow the procedure below for the KX-NS1000.
 - a. Shutdown the Master unit and then turn off the power switch.

Note

The Slave units in the One-look network will reboot when the Master unit is shutdown.

- b. Connect the stacking cable to the STACK-M card.
3. Follow the procedure below for the KX-NS1000 and legacy gateways.
 - a. Turn the power switch on.

One-look network will start working normally.

Note

To programme the One-look network, refer to "5.5 Programming a One-look Network".

Procedure for Case 4

To stack PBXs with a KX-NS1000 which is running already as stand-alone, and then start One-look network, follow the procedure below.

Notice

- If you wish to continue to use the programmed settings (e.g., Speed Dial and Caller ID, DDI/DID Table, etc.) of PBXs that will be connected to the KX-NS1000 as legacy gateways, export each PBX's data before beginning the procedure for Case 4. Then, after completing the procedure for Case 4, import the data to the Master unit of the One-look network.
For exporting data from PBXs that will be connected to the KX-NS1000 as legacy gateways, refer to the PC Programming Manual of the corresponding PBX.
- When importing data from other PBXs to a Master unit, make sure no extension numbers or port numbers programmed in the import data are already in use on the Master unit.

1. Follow the procedure below for the PBXs to be connected as legacy gateways.
 - a. Make sure the power switch is turned off.
 - b. Remove the MPR card, and then insert a STACK-S (NCP)/STACK-S (TDE) card.
 - c. Connect the stacking cable to the STACK-S (NCP)/STACK-S (TDE) card.
2. Follow the procedure below for the KX-NS1000.
 - a. Shutdown the KX-NS1000, and then turn off the power switch.
 - b. Insert a STACK-M card into the free slot.
 - c. Connect the stacking cable to the STACK-M card.
3. Follow the procedure below for the KX-NS1000 and legacy gateways.
 - a. Turn the power switch on.
4. Follow the procedure below for the KX-NS1000.
When the KX-NS1000 is going to be a Master unit.
 - a. Reboot the other KX-NS1000s (Slave units).

- b. Add slave sites using the Add Site Wizard, and then start One-look networking.
For more information about the Add Site Wizard, refer to "5.5 Programming a One-look Network".

When the KX-NS1000 is going to be a Slave unit.

- a. Add the site containing the KX-NS1000 as a Slave unit to the One-look network using the Add Site Wizard, and then start One-look networking.
For more information about the Add Site Wizard, refer to "5.5 Programming a One-look Network".

Note

If desired, at this time import any data that was exported from the PBXs before beginning this stacking procedure. The data should be imported to the Master unit.

For more information about importing data with Web Maintenance Console, refer to "6.6 Tool—Import" in the PC Programming Manual.

Note

- When starting PBXs after stacking with the KX-NS1000, start the KX-NS1000 before the stacked PBX.
- When exchanging a PBX that is stacked with the KX-NS1000 and running already to a different model of PBX, delete current legacy gateway settings using Web Maintenance Console before the exchange.
- The activation keys that were obtained when the PBX was running are not available when the PBX is stacked with a KX-NS1000.
- Legacy gateways cannot be accessed by the PC Maintenance Console.
- Legacy gateways support VPSs. For more details, refer to the documentation for the PBX.

Pre-installing stacked PBXs connected to the STACK-M card

Once a STACK-M card has been added to the physical shelf on the **Slot** screen, you can pre-install stacked PBXs connected to the STACK-M card.

1. Log in to Web Maintenance Console. For details, refer to "Connecting to Web Maintenance Console" in "5.3 Starting Web Maintenance Console".
2. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot**.
3. Place the mouse cursor over the STACK-M card, and in the menu that appears, click **Pre-Install**.
4. In **Cabinet Type**, select the model of the PBX connected to connection port 1 of the STACK-M card, and then click the arrow button.
5. If a second stackable PBX is connected to connection port 2 of the STACK-M card, select the model of the PBX connected to connection port 1, and then click the arrow button.
6. Click **OK** when finished to complete pre-installation.

Programming Legacy Gateways

To programme legacy gateways that are stacked with a KX-NS1000, use Web Maintenance Console.

To log in to Web Maintenance Console, refer to "Connecting to Web Maintenance Console" in "5.3 Starting Web Maintenance Console".

For more information about programming legacy gateways, refer to the PC Programming Manual.

6.2 Methods of Stacking PBXs

Section 7

Troubleshooting

This section provides information on the PBX and telephone troubleshooting.

7.1 Troubleshooting

7.1.1 Installation

PROBLEM	PROBABLE CAUSE	SOLUTION
You cannot make/receive calls via an IP network.	<ul style="list-style-type: none"> DSP card malfunction Mother board malfunction Not enough activation keys Poor connection Network malfunction 	<ul style="list-style-type: none"> Replace the corresponding card. Replace the mother board (be sure to turn off the PBX when replacing). Purchase additional activation key codes. Please consult a certified dealer for details. Make sure that an 8-pin twisted pair cable is used for connection. Make sure that none of the CAT 5/CAT 5e cables in use are over 100 m in length. Make sure that a straight cable is used for connection to a switching hub. Make sure that all network devices in use are switched on. Make sure that there is no unwanted firewall in the IP network.
IP-PTs/SIP phones do not operate.	<ul style="list-style-type: none"> DSP card malfunction Mother board malfunction Not enough activation keys IP-PT/SIP phone not registered IP-PT/SIP phone malfunction Poor connection Network malfunction 	<ul style="list-style-type: none"> Replace the corresponding card. Replace the mother board (be sure to turn off the PBX when replacing). Purchase additional activation key codes. Please consult a certified dealer for details. Register the corresponding IP-PT/SIP phone. Replace the IP-PT/SIP phone. Make sure that an 8-pin twisted pair cable is used for connection. Make sure that none of the CAT 5/CAT 5e cables in use are over 100 m in length. Make sure that a straight cable is used for connection to a switching hub. Make sure that all network devices in use are switched on. Make sure that the IP-PT/SIP phone is not blocked by the firewall or other network devices.

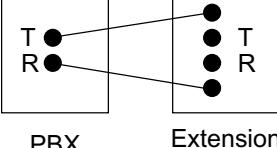
PROBLEM	PROBABLE CAUSE	SOLUTION
Extensions (except IP-PT/SIP phone) do not operate.	<ul style="list-style-type: none"> Extension card malfunction Poor connection between the PBX and the extension A telephone with an A-A1 relay is connected. Extension malfunction 	<ul style="list-style-type: none"> Replace the corresponding card. Take the extension and plug it into the same extension port using a short telephone cord. If the extension works, then the connection between the PBX and the extension must be repaired. Make sure that a 2-wire cord is used. Make sure that the A-A1 relay switch of the telephone is in "OUT" or "OFF" position. Take the extension and plug it into another extension port that is working. If the extension does not work, replace the extension.
The PBX does not operate properly.		<ul style="list-style-type: none"> Restart the PBX (refer to "7.1.5 Restarting the KX-NS1000"). Turn off the power switch, and then turn it back on. Turn off the power switch, and then unplug the PBX. After 5 minutes, plug the PBX back in, and turn the power switch back on.
Noise on external paging.	<ul style="list-style-type: none"> Induced noise on the wire between the PBX and the amplifier. 	<ul style="list-style-type: none"> Use a shielded cable as the connection wire between the PBX and amplifier. A short shielded cable is recommended.
Distorted external music.	<ul style="list-style-type: none"> Excessive input level from external music source. 	<ul style="list-style-type: none"> Decrease the output level of the external music source by using the volume control on the music source.
The STATUS indicator on the front of the cabinet turns on red.	<ul style="list-style-type: none"> A major system error occurs in the PBX. 	<ul style="list-style-type: none"> See the error log using Web Maintenance Console (refer to "7.1.6 Troubleshooting by Error Log").
The LINK indicator of the mother board does not turn on.	<ul style="list-style-type: none"> Mother board malfunction 	<ul style="list-style-type: none"> Replace the mother board (be sure to turn off the PBX when replacing).
	<ul style="list-style-type: none"> Poor connection. 	<ul style="list-style-type: none"> Make sure that an 8-pin twisted pair cable is used for connection. Make sure that none of the CAT 5/CAT 5e cables in use are over 100 m in length. Make sure that a straight cable is used for connection to a switching hub.
	<ul style="list-style-type: none"> Network malfunction 	<ul style="list-style-type: none"> Make sure that all network devices in use are switched on.

7.1.1 Installation

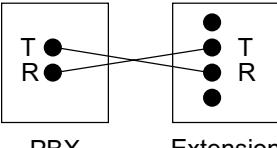
PROBLEM	PROBABLE CAUSE	SOLUTION
The LED (Link 1, Link 2) of the STACK-M card is not green, or the CARD STATUS LED of the STACK-S (NCP) card or the STACK-S (TDE) card is not green.	The stacking cable is not connected properly.	<ul style="list-style-type: none">Check the stacking cable connections.
	There was a failure in the stacking card.	<ul style="list-style-type: none">Replace the stacking card.

7.1.2 Connection

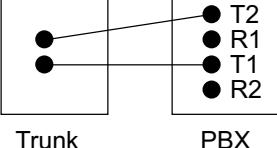
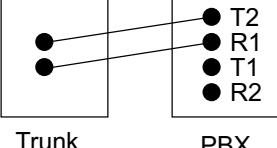
Connection between the PBX and an SLT:

		CAUSE	SOLUTION
Can you dial an extension?	No	<p>The T/R is connected to the D1/D2.</p> 	<p>Use the correct cord (the inner 2 wires are for T/R).</p> <ul style="list-style-type: none"> • If a telephone equipped with an A-A1 relay is connected to the PBX, set the A-A1 relay switch of the telephone to "OFF".

Connection between the PBX and an SLT that is polarity-sensitive:

		CAUSE	SOLUTION
Yes		<p>The "T" is connected to the "R".</p> 	Reverse the connections of the T/R.

Connection between the trunk and the PBX:

		CAUSE	SOLUTION
Can you dial out on a trunk?	No	<p>Trunk is connected to the T2/T1.</p> 	Reconnect the trunk to the T1/R1 or T2/R2 of the telephone jack using 2-conductor wiring.
		<p>Trunk is connected to the T2/R1.</p> 	

7.1.3 Operation

Note

For devices connected to a PBX other than the KX-NS1000, refer to the Troubleshooting for that PBX.

PROBLEM	PROBABLE CAUSE	SOLUTION
<ul style="list-style-type: none"> Cannot set the IP address, subnet mask address, and PBX IP address to the IP-PT. 	<ul style="list-style-type: none"> An unusable value is being set. 	<ul style="list-style-type: none"> Set an IP address within the valid range. IP address of the IP-PT/PBX: "1.0.0.0" to "223.255.255.255" Subnet mask address: "0-255.0-255.0-255.0-255" (except "0.0.0.0" and "255.255.255.255")
<ul style="list-style-type: none"> Cannot register the IP-PT. 	<ul style="list-style-type: none"> The necessary network parameters are not set to the IP-PT. 	<ul style="list-style-type: none"> When not using the DHCP Server feature or an external DHCP server, set the IP address, subnet mask address, and enter the PBX IP address. If necessary, also enter the IP address of the default gateway. When using the DHCP Server feature or an external DHCP server, enter the PBX IP address.
<ul style="list-style-type: none"> The IP-PT cannot connect to the PBX. 	<ul style="list-style-type: none"> The wrong IP address, subnet mask address, PBX IP address, or default gateway address was entered. 	<ul style="list-style-type: none"> Check each parameter and enter the correct value.
	<ul style="list-style-type: none"> The Ethernet cable is not connected correctly. 	<ul style="list-style-type: none"> Check the Ethernet cable connections.
	<ul style="list-style-type: none"> The DHCP server is not active. 	<ul style="list-style-type: none"> Restart the external DHCP server. Confirm whether the DHCP Server feature is enabled. Disable DHCP and re-enter settings as appropriate.
<ul style="list-style-type: none"> Whenever you try to make calls using a SIP phone, a busy tone is heard. 	<ul style="list-style-type: none"> The status of the port that the SIP phone is connected to is Out of Service. 	<ul style="list-style-type: none"> Change the port status from Out of Service to In Service using Web Maintenance Console.
<ul style="list-style-type: none"> The IP-PT does not ring. 	<ul style="list-style-type: none"> The ringer volume is off. 	<ul style="list-style-type: none"> Turn on the ringer volume.
<ul style="list-style-type: none"> Originating an outside call, call transfer, or conference cannot be performed. 	<ul style="list-style-type: none"> The corresponding flexible button does not exist on the PT. 	<ul style="list-style-type: none"> Programme the flexible button. Refer to "2.21.1 Fixed Buttons" in the Feature Guide.

PROBLEM	PROBABLE CAUSE	SOLUTION
<ul style="list-style-type: none">The IP address of the PBX for networking has been forgotten.	-	<ul style="list-style-type: none">Connect a PC to the MNT port of the PBX directly and start the Web Maintenance Console using the default IP address of the MNT port, and then confirm the IP address assigned for the LAN port. For details of connecting the PC directly to the PBX, refer to "5.2 PC Connection". For details of checking current IP address of the mother board, refer to "28.1 Network Service—[1] IP Address/Ports—◆ LAN Setting—IP Address" in the PC Programming Manual.

7.1.4 Error Messages

When a major system error occurs, an error message is displayed on the IP-PT.

For IP-PTs with a single line display (e.g., KX-NT265), only an error code (i.e., ERR XXXX-XXXX) will be displayed.

Error Message & IP-PT Activity	Probable Cause	Solution
ERR 1001-0000 HARDWARE ERROR Displays error and stops operating.	• Sub CPU malfunction	• Repair or replace the IP-PT.
ERR 1002-0000 HARDWARE ERROR Displays error and stops operating.	• Sound hardware malfunction	
ERR 1003-0000 HARDWARE ERROR Displays error and stops operating.	• Flash memory malfunction	
ERR 1004-XXXX HARDWARE ERROR Displays error and stops operating.	• PHY (network control IC) error	
ERR 1005-0000 HARDWARE ERROR Displays error and stops operating.	• SDRAM error	
ERR 1006-0000 HARDWARE ERROR Displays error and stops operating.	• SRAM error	
ERR 1007-0000 HARDWARE ERROR Displays error and stops operating.	• Sub CPU malfunction for Self Labelling	
ERR 1051-0000 SOFTWARE ERROR Displays error and stops operating.	• PBX software version error	• Consult your network administrator.
ERR 2001-XXXX SYSTEM ERROR Resets and displays error for 5 seconds while starting up.	• Unexpected error	• If this error is displayed frequently, repair or replace the IP-PT.
ERR 2002-0000 POOR LAN CONNECTION Resets and displays error for 5 seconds while starting up.	• Transmission error	• Check with the network administrator whether there is a problem with the LAN. • If this error is displayed frequently, repair or replace the IP-PT.
ERR 2003-0000 POOR LAN CONNECTION Resets and displays error for 5 seconds while starting up.		

Error Message & IP-PT Activity	Probable Cause	Solution
ERR 2004-0000 UNREGISTERED TO SERVER Resets and displays error for 5 seconds while starting up.	<ul style="list-style-type: none"> IP-PT not registered 	<ul style="list-style-type: none"> Check the registration status of the IP-PT.
ERR 2005-0000 NO MORE CONNECTIONS Resets and displays error for 5 seconds while starting up.	<ul style="list-style-type: none"> Connection refused by the PBX 	
ERR 2006-XXXX DHCP SERVER REJECTION Resets and displays error for 5 seconds while starting up.	<ul style="list-style-type: none"> IP address lease time from DHCP server has expired IP address lease renewal was refused by DHCP server 	<ul style="list-style-type: none"> Consult your network administrator.
ERR 2007-0000 HARDWARE ERROR Resets and displays error for 5 seconds while starting up.	<ul style="list-style-type: none"> Communication error with sub CPU 	<ul style="list-style-type: none"> If this error is displayed frequently, repair or replace the IP-PT.
ERR 2008-0000 HARDWARE ERROR Resets and displays error for 5 seconds while starting up.	<ul style="list-style-type: none"> Sound hardware control error 	
ERR 2009-XXXX MGCP SERVER REJECTION Resets and displays error for 5 seconds while starting up.	<ul style="list-style-type: none"> Error information from the PBX (MGCP server) 	<ul style="list-style-type: none"> Consult your network administrator.
ERR 2010-0000 HARDWARE ERROR Resets and displays error for 5 seconds while starting up.	<ul style="list-style-type: none"> Communication error with sub CPU for Self Labelling 	<ul style="list-style-type: none"> If this error is displayed frequently, repair or replace the IP-PT.
ERR 3001-0000 HARDWARE ERROR Displays error until reset the IP-PT.	<ul style="list-style-type: none"> Communication error with sub CPU 	
ERR 3002-0000 HARDWARE ERROR Displays error until reset the IP-PT.	<ul style="list-style-type: none"> Sound hardware control error 	
ERR 3003-XXXX DHCP SERVER NOT FOUND Displays error until reset the IP-PT.	<ul style="list-style-type: none"> IP address lease renewal was refused by DHCP server 	<ul style="list-style-type: none"> Consult your network administrator.
ERR 3100-0000 BLUETOOTH ERROR Resets the Bluetooth® wireless headset.	<ul style="list-style-type: none"> Bluetooth hardware error 	<ul style="list-style-type: none"> Repair or replace the Bluetooth wireless headset.

7.1.5 Restarting the KX-NS1000

If the PBX does not operate properly, restart the PBX using Web Maintenance Console. Before restarting the PBX, try the system feature again to confirm whether there definitely is a problem or not.

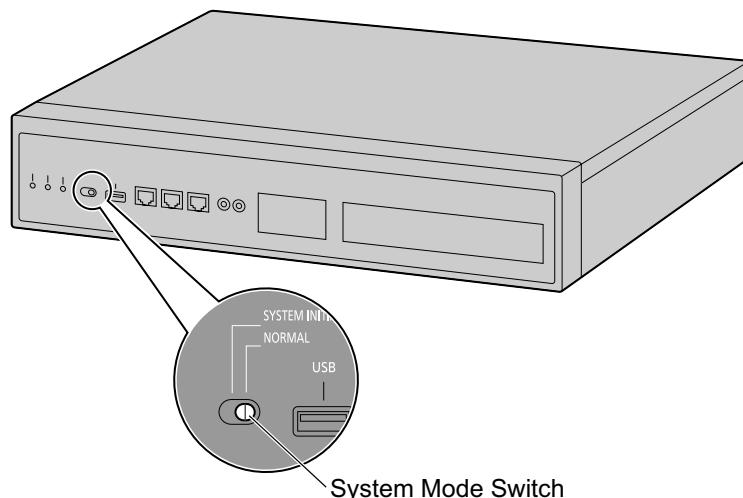
Note

- When the System Mode Switch is set to "NORMAL", restarting the PBX causes the following:
 - Camp-on is cleared.
 - Calls on hold are terminated.
 - Calls on exclusive hold are terminated.
 - Calls in progress are terminated.
 - Call park is cleared.Other data stored in memory, except the above, are not cleared.
- Be aware that restarting the PBX with the System Mode Switch in the "SYSTEM INITIALIZE" position clears all data stored in the PBX. Do not perform this operation unless you intend to delete all data from the PBX.
- When the PBX is set to obtain IP addressing information automatically, and the PBX is not able to obtain appropriate IP addressing information from an external DHCP server, the PBX starts up with its default IP addresses and the STATUS indicator on the front of the cabinet turns red. For the default IP addresses, refer to "5.3 Starting Web Maintenance Console".

Operation

If the PBX does not operate properly:

1. Slide the System Mode Switch to the "NORMAL" position.



2. Start the Web Maintenance Console.
3. Log in using the Installer level account.
4. On the Home screen, click **Maintenance** → **System Control** → **System Reset**.
5. Follow the prompts.
Restarting the PBX will start.

Note

- When the power switch is turned on, or when the PBX recovers from a power failure, the PBX will restart. The time required to restart depends on the number of connected extensions and the number of registered One-look network sites.

Example:

PBX	Extensions	Estimated Time for Starting Up
1 PBX (Stand-alone)	128 KX-UT series SIP phones	more than 5 minutes
16 PBXs (One-look network)	256 KX-UT series SIP phones	more than 15 minutes

- PBX functions cannot be used until restarting is complete. The use of a UPS is recommended; even a momentary power failure can result in a long delay as the PBX restarts, requiring the time as shown above.

7.1.6 Troubleshooting by Error Log

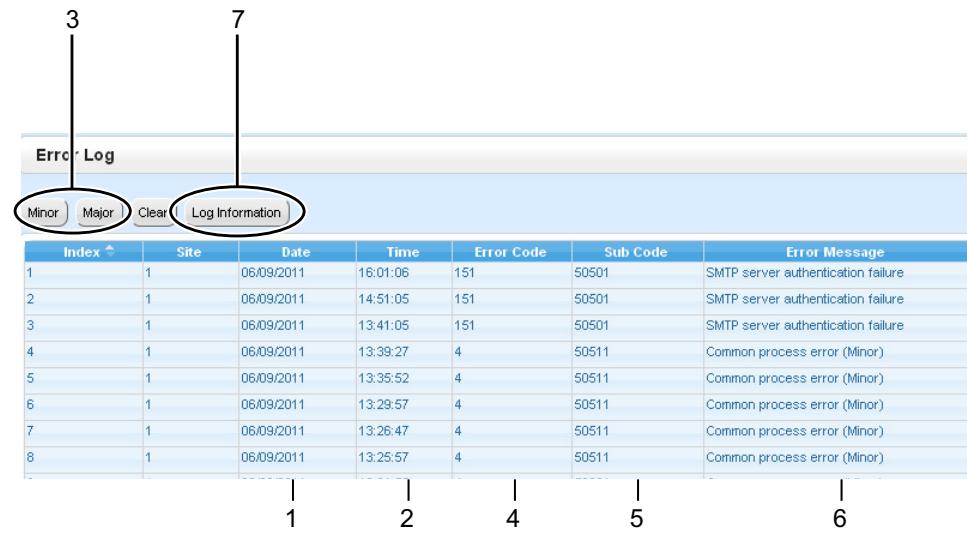
7.1.6 Troubleshooting by Error Log

When a major system error occurs in the PBX, the STATUS indicator on the front of the cabinet turns red, and the system logs the error information.

Error Log Display Format

Below is the display format of the error log. For information about how to view the error log using Web Maintenance Console, refer to "7.3.1 Utility—Log—Error Log" in the PC Programming Manual.

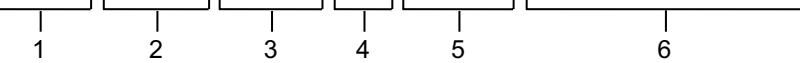
Example: Web Maintenance Console



Index	Site	Date	Time	Error Code	Sub Code	Error Message
1	1	06/09/2011	16:01:06	151	50501	SMTP server authentication failure
2	1	06/09/2011	14:51:05	151	50501	SMTP server authentication failure
3	1	06/09/2011	13:41:05	151	50501	SMTP server authentication failure
4	1	06/09/2011	13:39:27	4	50511	Common process error (Minor)
5	1	06/09/2011	13:35:52	4	50511	Common process error (Minor)
6	1	06/09/2011	13:29:57	4	50511	Common process error (Minor)
7	1	06/09/2011	13:26:47	4	50511	Common process error (Minor)
8	1	06/09/2011	13:25:57	4	50511	Common process error (Minor)

Example: Station Message Detail Recording (SMDR)

01/01/10 01:00AM MJ ALM #014 00 10000 FAN Alarm
01/01/10 01:29AM MN ALM #533 01 50401 Unit start up error
01/01/10 01:39AM MN ALM #091 00 10000 PT connection over



Description

	Item		Description
1	Date		The date of the error detection.
2	Time		The time of the error detection.
3	Level	Minor (MN ALM)	Displays minor errors, which affect only a certain part of system operation.
		Major (MJ ALM)	Displays major errors, which affect operation of the whole system, or result in system failure.
4	Error Code		The 3-digit error code assigned by the PBX.

	Item	Description
5	Sub Code	SMDR: The 8-digit sub code of the relevant hardware (BBWXYYZZ). Web Maintenance Console: The 6-digit sub code of the relevant hardware (WXYYZZ). (The site number of the PBX can be confirmed in the Site column of the Error Log.) For details about the contents of error sub codes, refer to "7.3.1 Utility—Log—Error Log" in the PC Programming Manual.
6	Error Message	A description of the error.
7	Log Information	Displays probable causes of the errors and their solutions.

7.1.6 Troubleshooting by Error Log

Section 8

Networking Information

This section provides information about topics such as using the PBX in a VoIP network, and the TCP ports used by the PBX.

8.1 Information about Using an IP Network

This section explains common IP network information necessary for setting up One-touch networks and QSIG networks.

8.1.1 Using a VoIP Network with the PBX

This PBX supports Panasonic KX-NT300 series, KX-NT500 series, and KX-NT265 IP proprietary telephones (IP-PTs), Panasonic IP softphones, and SIP (Session Initiation Protocol) phones (hardphones and softphones) for communication on a Voice over Internet Protocol (VoIP) network. These IP telephones can be used as extensions of the PBX when the local office LAN is connected to other LANs at different locations.

This PBX also enables VoIP communication with PBXs installed at different locations. Since the communication does not take place over conventional telephone network, the high cost of long distance communication is virtually eliminated.

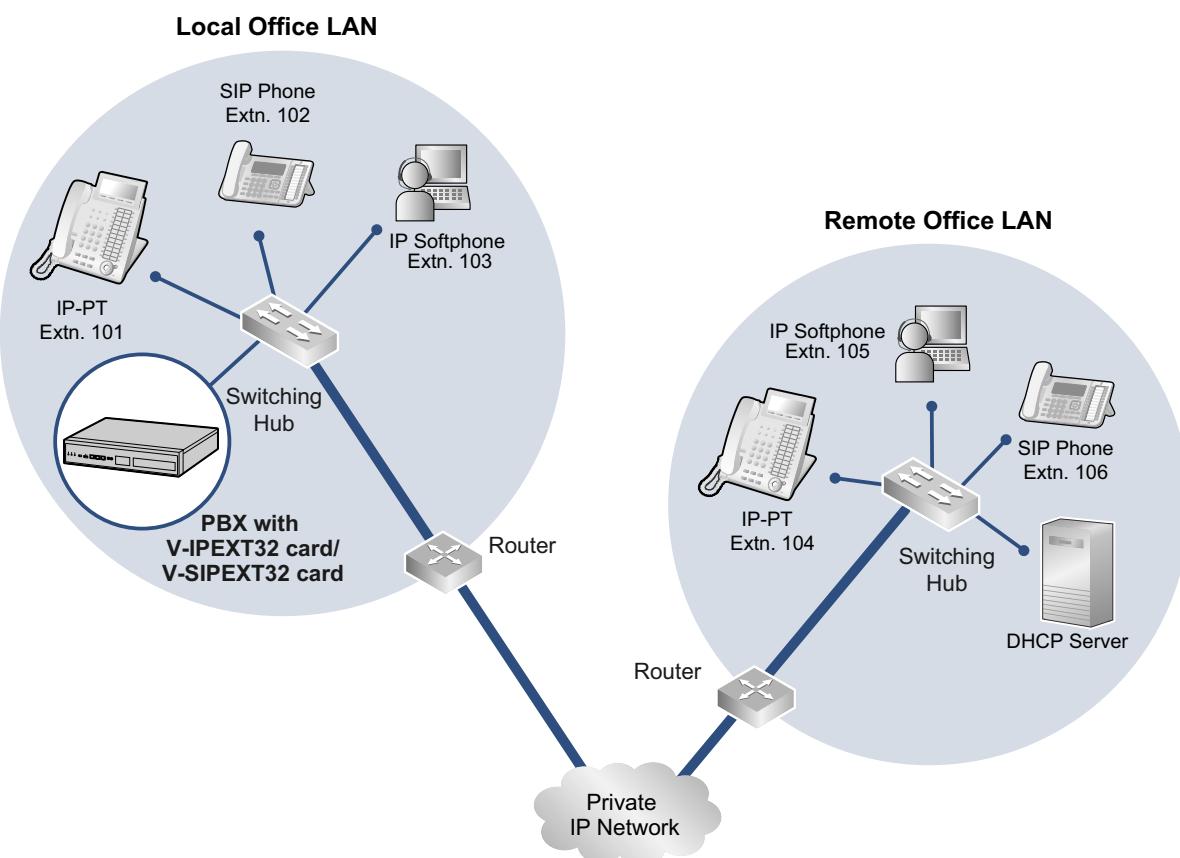
To establish a VoIP network, the virtual cards are used according to the requirement of the network. For details about virtual cards, see "4.4 Virtual Cards".

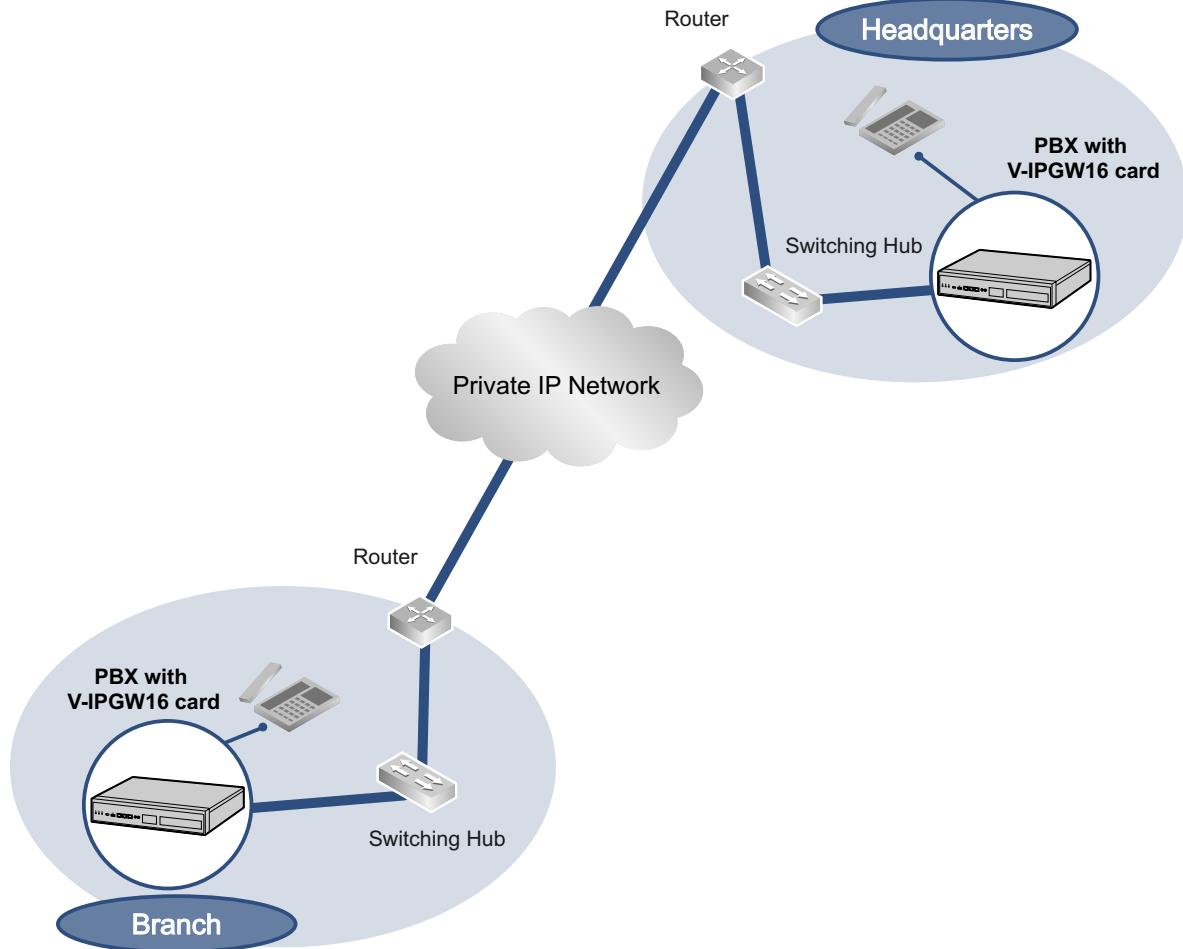
The following diagrams illustrate VoIP network with (i) a remote office LAN and (ii) another PBX installed at different location.

Note

Panasonic IP Cell Station (IP-CS) units are also supported by this PBX for communication on a VoIP network. For details, refer to the Quick Installation Guide for the IP-CS.

(i) Connection Outline of VoIP Network with Remote Office LAN



(ii) Connection Outline of VoIP Network with PBX in Other Network**Network Parameters**

You will need to have the following IP addressing and QoS information to establish VoIP communication on your network. This information is typically supplied by a network administrator. Consult your network administrator for specific values.

Parameter	Description
IP telephone IP Address	Identifies the location of IP telephones on the network. Each IP telephone must have a unique IP address.
Subnet Mask Address	Defines which digits of an IP address are used for the network address and the host address at each network location. The IP addresses of the IP telephones and the PBX must fall within the same subnet as that of the default gateway (e.g., router) of the LAN.
Default Gateway Address	Identifies the IP address of the primary gateway (typically a router or similar device) that exchanges IP packets with the other gateways on the VoIP network.

8.1.1 Using a VoIP Network with the PBX

Parameter	Description
PBX IP Address	Identifies the location of the PBX in the network during VoIP communications.
VLAN ID	Identifies the ID of the logical segment within the corporate LAN, through which voice packets from IP telephones travel. For details, refer to "8.1.3 VLAN (Virtual LAN)".
DiffServ (DS)	Identifies the value for the DS field in the header of IP packets, which determines the priority given to packets travelling from IP telephones. For details, refer to "5.8.4 Setting Diffserv Parameters".

Types of IP Network

The speech quality depends on the type of IP network in use. Managed IP networks provide better speech quality compared to unmanaged networks such as satellite communications, where quality of service cannot be guaranteed.

Examples of recommended IP networks

- Digital Leased Line
- IP-VPN (Virtual Private Network)
- Frame Relay

Not recommended

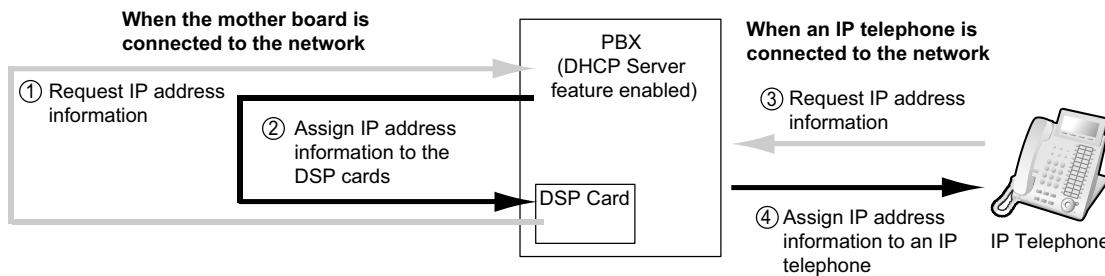
- Satellite communications (Very Small Aperture Terminal system [VSAT], etc.)

Note

- Peer-to-peer calls between IP telephones installed at different locations may not be possible if packet communication cannot be established between the respective networks. In this case, you need to configure the network settings (e.g., a VPN router when using an IP-VPN) to establish packet communication.
- Unlike an IP-VPN, which is set up over a network provider's own IP network, an Internet VPN is set up over the Internet. Internet VPNs are not recommended for VoIP communication because transmission delays and loss of data are likely to occur.
- If multiple Slave units exist in a One-look network using IP-VPN, each Slave unit must have peer-to-peer communication enabled. Therefore, inform your network administrator and make sure that the network supports this requirement.

8.1.2 DHCP (Dynamic Host Configuration Protocol) Server

To establish communication over a VoIP network, IP addresses must be assigned to IP telephones and the PBX to identify their locations on the network. While these addresses can be assigned manually, it is also possible to use a DHCP server to automatically assign IP address information. The KX-NS1000 has a DHCP Server feature. Therefore, the PBX can act as a DHCP server or DHCP client depending on its settings. When the PBX's DHCP Server feature is enabled, it allows you to centrally manage and automate the assignment of IP addresses with Web Maintenance Console. For details, refer to "◆ DHCP Server" in the PC Programming Manual.



Note

- The DHCP Server feature is disabled by default. To enable the feature, refer to "5.4.2 Enabling the DHCP Server Feature".
- An IP telephone and the mother board/DSP cards cannot request IP addresses from a DHCP server on another LAN (connected through an IP network). They can only receive IP addresses from a DHCP server on the same LAN. Therefore, when IP telephones are located on several LANs, a DHCP server is required on each LAN. If a DHCP server is not present on the LAN, IP addresses for IP telephones and the mother board/DSP cards on that LAN must be assigned manually.
- When the PBX has been set to act as a DHCP client, use an external DHCP server to assign IP address information automatically.
- When the KX-NS1000 is set as the DHCP client and cannot receive appropriate IP addressing information from an external DHCP server, the PBX keeps using the previous effective IP addressing information and checks whether any overlapping of IP addresses exists. If the IP address of the PBX overlaps with another IP address, the PBX displays a warning to encourage changing the IP address of the PBX.
- The DHCP Server feature is available regardless of whether the built-in router feature is enabled. For details, refer to "8.6.2 WAN Connection".

8.1.3 VLAN (Virtual LAN)

VLANs are logical segments within a corporate LAN. By assigning VLAN settings to IP telephones, it is possible to separate the packets transmitted by an IP telephone according to the type of data and specify which VLAN each data type will be sent over. This allows you to avoid generating unnecessary network traffic on each segment and to reduce the load on the network. As a consequence, speech quality can be assured. Therefore, we recommend using the VLAN feature to perform VoIP communication effectively.

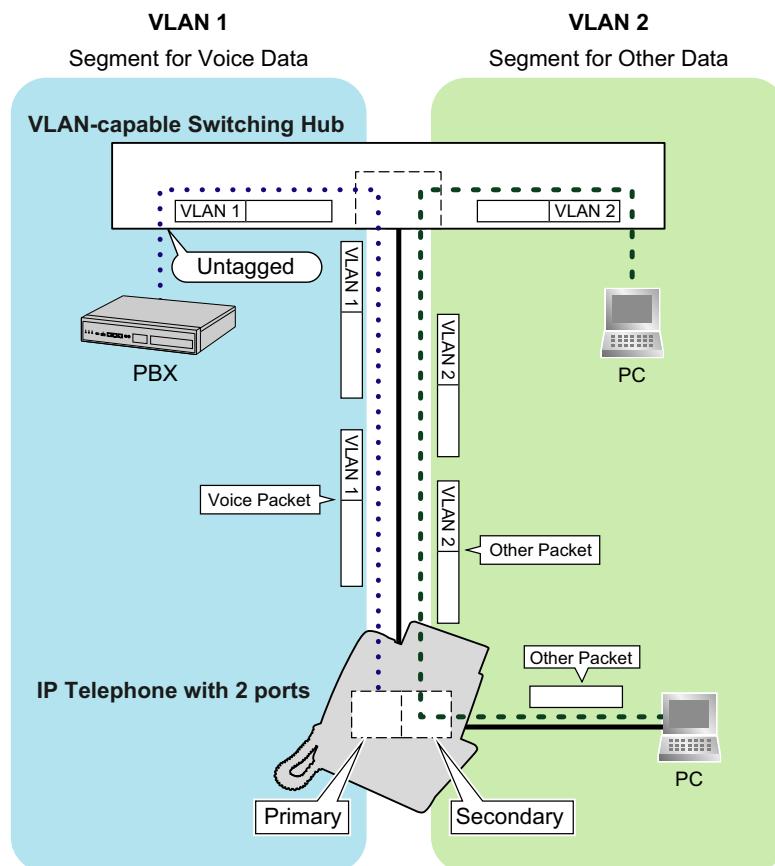
Some IP telephones (e.g., KX-NT300 series) are equipped with 2 ports, primary and secondary, for packet communication. Allocating these ports to different VLANs enables you to split the paths for packets depending on whether the packet contains voice signals or data.

VLAN settings (VLAN ID and VLAN priority) for the primary port affect voice data transmitted by the IP telephone, whereas VLAN settings for the secondary port apply to data transmitted by a PC connected to the IP telephone. When sending packets, the IP telephone can attach information on which VLAN the packets are to be transmitted over (VLAN Tagging). The switching hub that receives these packets reads the VLAN information and sends the packets over the appropriate VLAN. This helps to ensure bandwidth for IP telephone voice transmissions.

In this way, an IP telephone with 2 ports can transmit voice packets from the primary port with higher priority than other packets from the secondary port.

Notice

The PBX's LAN port does not support VLAN tagging. Therefore, connect the PBX's LAN port to a port of the switching hub that is set to "Untagged", and the IP telephone to a port set to "Trunk", to allow VLAN tagging. Consult your network administrator for details.



Note

- This VLAN feature complies with IEEE (Institute of Electrical and Electronics Engineers) 802.1Q.
- The PBX receives VLAN settings only from the connected switching hub. Therefore, VLAN settings for the PBX must be assigned at the switching hub.
- When using the VLAN feature on the network, make sure that the main unit is connected to a layer 2 switch that is IEEE 802.1Q compliant, and that is configured for VLANs. In addition, the port of the switching hub to which the card is connected must be set to "Untagged". Consult your network administrator for details.
- When using the VLAN feature on the network, make sure that the switching hub to be connected is IEEE 802.1Q compliant and is configured for VLANs. In addition, the port of a switching hub that the IP telephone is connected to must be set to "Trunk" port, to allow VLAN tagging. Consult your network administrator for details.
- Some PC LAN cards allow VLAN settings to be assigned. However, when using a PC connected to an IP telephone with 2 ports, the VLAN settings for PC communications must be assigned only to the secondary port of the IP telephone. Any VLAN settings assigned to the PC LAN card must be disabled. These settings can usually be identified by "802.1Q", "802.1p", or "VLAN" in their name.
- If you are using an IP telephone with a primary port only (e.g., KX-NT265), a PC cannot be connected to the IP telephone.

8.1.4 Jitter Buffer

When voice signals are packetised and transmitted, individual packets can take different paths through the network and arrive at the destination at varied timings. This is referred to as "jitter", and it can cause degradation in speech quality. To compensate for jitter problems, the "jitter buffer" accumulates the packets temporarily for processing.

To set the size of the jitter buffer, refer to "9.5 PBX Configuration—[1-1] Configuration—Slot—Site Property—VoIP-DSP Options" in the PC Programming Manual.

8.1.5 Voice Activity Detection (VAD)

VAD conserves bandwidth by detecting silent periods during a call and suppressing the packets of silence from being sent to the network. This feature can be enabled or disabled for codec G.711.

To configure the VAD feature, refer to the appropriate section in the PC Programming Manual.

8.1.6 Network Configuration

You must evaluate the structure of the existing network to see if a VoIP network can be implemented. Below are the points that should be evaluated.

Is the IP network a managed network?

A VoIP network should be implemented on a managed IP network such as Frame Relay, Leased Line, or IP-VPN (Virtual Private Network).

An unmanaged network, such as the Internet (including an Internet VPN), cannot be used to employ a VoIP network because delays and loss in data transmission can cause huge degradation in speech quality.

Is it possible to have static IP addressing?

IP telephones on the network always perform VoIP communications through the PBX. Therefore, the PBX must be assigned static IP addresses, which must be programmed to each IP telephone on the network.

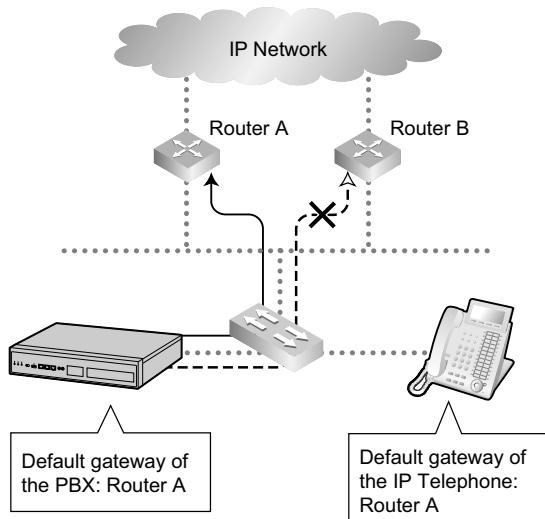
Note

When the DHCP Server feature is disabled and external DHCP servers are not used, static IP addressing must also be enabled for all IP telephones.

Does only a single router provide access to the IP network?

In a dual network, 2 routers provide access to the IP network as shown in the diagram below. However, only one router can be used as an access point to the network.

Therefore, in the diagram below, if router A, whose IP address is assigned as the default gateway IP address of the PBX and the IP telephones, fails, VoIP communications are no longer possible; they are not able to switch their default gateway from router A to router B to access the IP network.



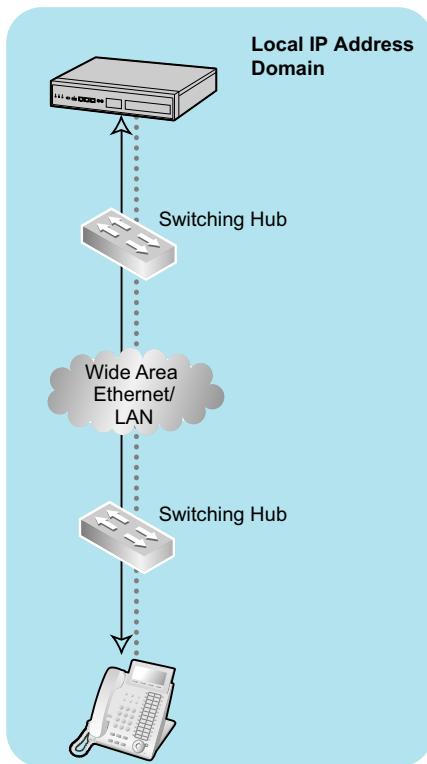
How is the PBX connected to remote extensions?

When the PBX is connected to a remote extensions via public IP network without using IP-VPN, address translation techniques (e.g., NAT/NAPT) are used. These methods prevent VoIP communications from being carried out effectively. In such cases, the use of an SBC/Media Relay Gateway will avoid this problem.

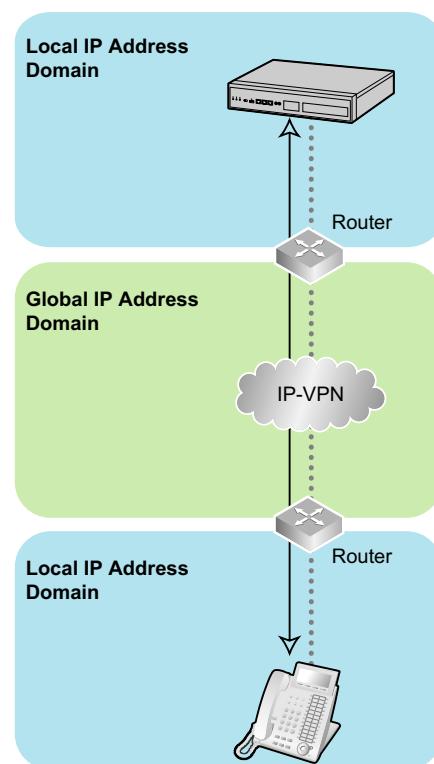
Note

- An SBC/Media Relay Gateway is not required for:
 - Connections via a Wide Area Ethernet or LAN
 - Connections via IP-VPN
- An SBC/Media Relay Gateway is required for:
 - Connections via a public IP network

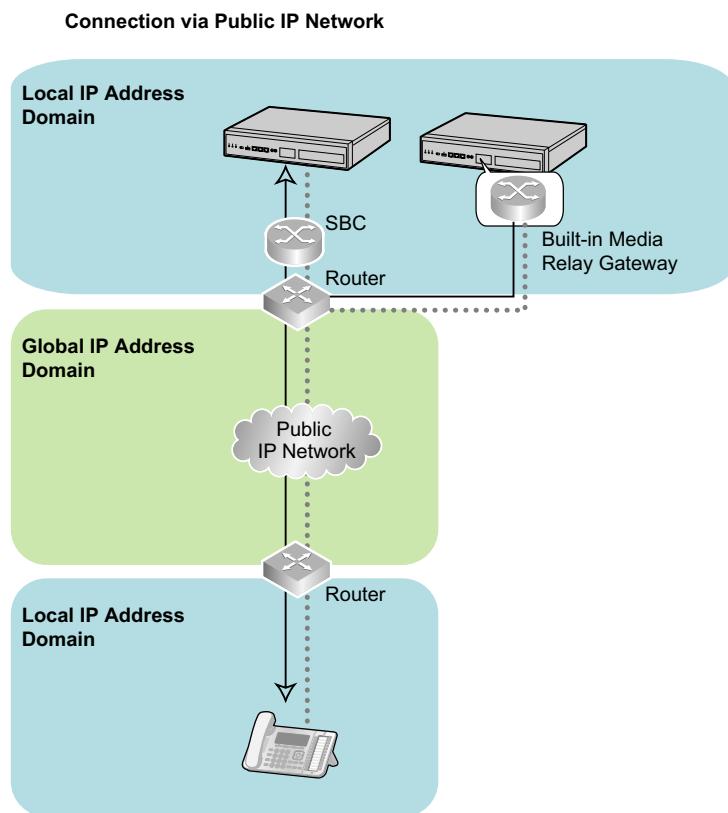
Connection via Wide Area Ethernet or LAN



Connection via IP-VPN



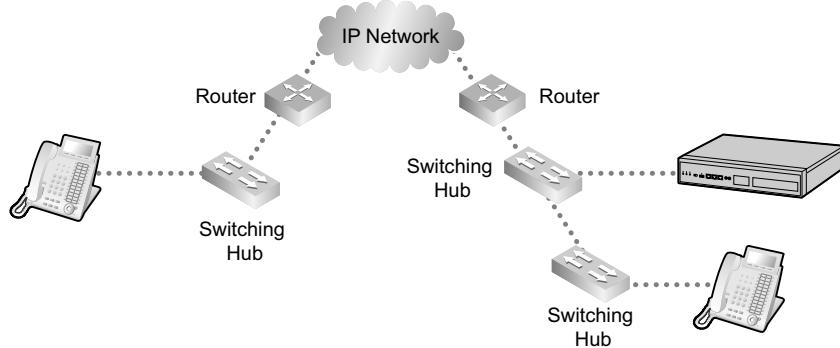
8.1.6 Network Configuration



Are the network devices located appropriately for effective VoIP communications?

Transmission delays can cause pauses and loss in VoIP communications. The more network devices (e.g., routers and switching hubs) there are between the PBX and IP telephones or the IP network interface, the longer the transmission delays. This is because a certain amount of delay is inevitable when packets go through each network device.

To prevent unnecessary delays, it is recommended to connect the PBX as close to the IP telephones and the IP network interface as possible so that the number of the network devices is kept to a minimum.



8.1.7 Network Devices

You must evaluate the network devices that are used in the existing network to see if a VoIP network can be implemented. Below are the points that should be evaluated.

Can the firewall pass packets appropriately?

If the VoIP network contains a firewall, the firewall must be configured appropriately to allow VoIP packets to pass through the network without being blocked by filtering. For details about the protocols and port numbers that the PBX uses for VoIP communication, refer to "8.5 Port Security".

The ports for which you need to configure the firewall may vary depending on the network conditions. For more information, consult your network administrator.

Are layer 2 or higher switches used?

Use of repeater hubs can increase the network load, and therefore may result in degradation in speech quality. To ensure high speech quality, use only layer 2 or higher switches. Use of layer 2 or higher switches is also strongly recommended for connecting IP telephones.

Note

Note that the port of the switching hub that connects to the mother board should be set to operate under "Auto Negotiation" mode.

Does all equipment on the LAN support 1000BASE-T connection?

To use the Gigabit Ethernet feature for the LAN, all equipment on the LAN must support 1000BASE-T. For more information, consult your network administrator.

Are Category 5 (CAT 5) or higher cables used for 10BASE-T/100BASE-TX?

When connecting network devices, make sure to use CAT 5 or higher cables for 10BASE-T/100BASE-TX connection. If other types of cables are used, communication may not be carried out normally.

Are Enhanced Category 5 (CAT 5e) or higher cables used for 1000BASE-T?

When connecting network devices, make sure to use CAT 5e or higher cables for 1000BASE-T. If other types of cables are used, communication may not be carried out normally.

8.1.8 QoS (Quality of Service)

Some routers permit the configuration of priority control features. This allows the router to give higher priority to voice packets and lower the rate of loss and delays during transmissions, hence improving speech quality. It is strongly recommended that you use this feature, especially in networks where traffic is heavy.

Typically, a router identifies what packets to pass in priority by checking the value in the ToS field of the header of IP packets. The V-IPGW16 card has the ability to set the ToS field of outgoing voice packets. When the card is appropriately configured, the router can give voice packets from the card higher priority.

Consult your network administrator when setting the ToS field, as the setting value must conform to the router's specifications.

Note

- Some switches also permit the configuration of priority control features. For more information, consult your network administrator.
- To adjust the value in the ToS field, refer to "9.12 PBX Configuration—[1-1] Configuration—Slot—V-IPGW16—Shelf Property" in the PC Programming Manual.

8.1.9 Network Time Protocol (NTP)

The KX-NS1000 can be configured to contact an NTP server to receive and update its time setting automatically.

KX-UT series SIP phones can receive and update their time setting either through the KX-NS1000 or by contacting an NTP server directly.

For a SIP phone to receive and update its time setting via the KX-NS1000, the NTP server feature must be enabled. To enable this feature refer to "28.2.4 Network Service—[2-5] Server Feature—NTP" in the PC Programming Manual.

If the NTP server feature is enabled:

- Case 1: An NTP server is specified in Web Maintenance Console.
 - The SIP phones use the specified IP address and contact the NTP server directly.
- Case 2: An NTP server is *not* specified in Web Maintenance Console.
 - The SIP phones use the IP address of the KX-NS1000 as their NTP server.
(The KX-NS1000 acts as an NTP server for the SIP phones.)

To specify the IP address of the NTP server, refer to "10.1.2 PBX Configuration—[2-1-2] System—Date & Time—SNTP / Daylight Saving" in the PC Programming Manual.

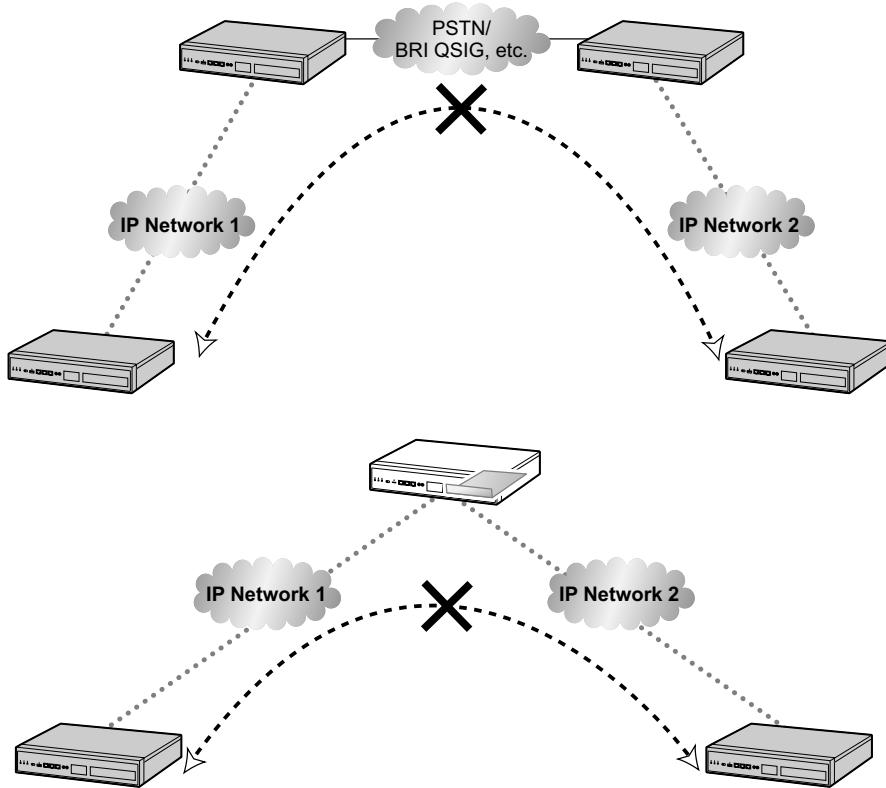
If the NTP server feature is disabled, the SIP phones use their own time settings.

8.2 H.323 Trunks

This section explains information that is necessary for setting up a H.323 QSIG network over an IP network.

8.2.1 Avoid Multiple IP Networks

A huge degradation in speech quality will be produced when calls are made through multiple IP networks as shown below; therefore, it is recommended that you avoid establishing a VoIP network in this fashion.



8.2.2 Gatekeeper

The following are the general functions of a gatekeeper:

- Dialled number-to-IP address translation
- Authentication
- Bandwidth control

The gatekeeper provides these network management functions to registered clients. To register with the gatekeeper, you need to configure the V-IPGW16 card to use the gatekeeper and programme the GK Settings table through system programming. For details, refer to "9.12 PBX Configuration—[1-1] Configuration—Slot—V-IPGW16—Shelf Property—◆ Gatekeeper Available" and "9.12.1 PBX Configuration—[1-1] Configuration—Slot—V-IPGW16—Shelf Property—GK Settings" in the PC Programming Manual. After programming, the V-IPGW16 card attempts to register with the gatekeeper using registration information such as the IP address of the mother board, and destination telephone numbers specified in the GK Settings table.

Note

- For more information about gatekeeper functions, consult the documentation of the gatekeeper.
- When using a gatekeeper, make sure to choose a compatible model. For more information about gatekeeper compatibility with the V-IPGW16 card, consult a certified dealer.

8.2.3 Bandwidth Assessment

When using the IP telephones and V-IPGW16 card, you must ensure that the IP network in use has enough bandwidth to support VoIP communications. If the amount of bandwidth required for VoIP communications is more than the network can accommodate, speech quality will be compromised. In addition, there may be an adverse effect on the performance of other applications (e.g., e-mail or Web applications) that use the same network. Therefore, care must be taken when assessing bandwidth requirements.

Inform your network administrator of the required bandwidth, and make sure that the network can support VoIP communications even under conditions of maximum network traffic.

Bandwidth Assessment for IP Extension Card

Required Bandwidth per IP Telephone for a Call

The required bandwidth depends on what combination of codecs and packet sending intervals is used. Keep in mind the following points about the type of codecs and packet sending intervals, in terms of speech quality:

- The speech quality of the codecs varies as follows: (High) G.722, G.711, G.729A (Low)^{**1}
 - The shorter the packet sending interval, the higher the speech quality.
 - The higher the speech quality the IP telephones provide, the more bandwidth the IP telephones require.
- ^{**1} When the preferred codec of each party differs, the call will be established using the lower codec. For example, if the caller prefers G.711 while the called party prefers G.729A, the call will be established using G.729A.

Codec	Packet Sending Interval			
	20 ms	30 ms	40 ms	60 ms
G.722 ^{**1} /G.711	87.2 kbps	79.5 kbps	—	—
G.729A	31.2 kbps	23.5 kbps	19.6 kbps	15.7 kbps

^{**1} G.722 is only available for calls between KX-NT300 series IP-PTs, KX-NT500 series IP-PTs, and some SIP phones that support this codec during peer-to-peer communication. For details, refer to "5.2.3 Peer-to-Peer (P2P) Connection" in the Feature Guide.

Required Bandwidth for Each IP Extension Card

To allow all IP telephones to make calls simultaneously, it is necessary to keep available the bandwidth required by an IP extension card with the maximum number of IP telephones connected.

Provided below is the formula to calculate the amount of bandwidth required for each IP extension card.

When using the V-IPEXT32/V-SIPEXT32 card:

Required Bandwidth = (Required Bandwidth per IP telephone \times 32)

Bandwidth Assessment for V-IPGW16 Card

Required Bandwidth for One VoIP Channel

The required bandwidth depends on what combination of codecs and packet sending intervals is used. Keep in mind the following points about the type of codec and packet sending interval, in terms of the speech quality:

- The speech quality of the G.711 codec is higher than that of the G.729A codec.
- The shorter the packet sending interval, the higher the speech quality.
- The higher the speech quality the V-IPGW16 card provides, the more bandwidth the card requires.

Via LAN

Codec	Packet Sending Interval				
	20 ms	30 ms	40 ms	60 ms	90 ms
G.711	87.2 kbps	79.5 kbps	75.6 kbps	71.7 kbps	—
G.729A	31.2 kbps	23.5 kbps	19.6 kbps	15.7 kbps	—

Via WAN (PPP: Point-to-Point Protocol)

Codec	Packet Sending Interval				
	20 ms	30 ms	40 ms	60 ms	90 ms
G.711	84 kbps	77.3 kbps	74 kbps	70.7 kbps	—
G.729A	28 kbps	21 kbps	18 kbps	14.7 kbps	—

Bandwidth Calculation

Provided below is the formula to find out the amount of bandwidth required for VoIP communications:

Required Bandwidth

= (No. of Fax Machines \times Required Bandwidth for the G.711 codec) +
[(16 - No. of Fax Machines) \times Required Bandwidth for Voice Communication]

Example

Consider the following case as an example:

- Communication: via LAN
 - No. of Fax Machines: 2
 - G.711 Packet Sending Interval: 20 ms (requiring 87.2 kbps per channel)
 - G.729A Packet Sending Interval for Voice Communication: 20 ms (requiring 31.2 kbps per channel)
- In this case, the required bandwidth will be as follows:

Required Bandwidth

= $(2 \times 87.2) + [(16 - 2) \times 31.2]$
= 611.2 (kbps)

8.2.3 Bandwidth Assessment

Therefore, inform your network administrator and make sure that the network can support a bandwidth of 611.2 kbps even when the network is under conditions of maximum traffic.

Note

It is recommended that all cards on a VoIP network have the same packet sending interval.

Additional Information

As described above, it is possible to control the required bandwidth by selecting a certain combination of codec and packet sending interval. However, it is also possible to control required bandwidth by limiting the number of available virtual VoIP channels.

The V-IPGW16 card supports a total of 8 ports, each having 2 separate channels. By disabling some of the ports, you can reduce the bandwidth required for VoIP communications.

To limit the number of VoIP channels:

Set the status of the ports you wish to disable (starting from the highest-numbered port) to **OUS**.

For example, if you wish to use only 10 of the available 16 virtual VoIP channels (i.e., disable 6 channels), set ports 8, 7, and 6 to **OUS** as shown below:

Gateway Port Property				
	Shelf	Slot	Port	Connection
Virtual	32	1		INS
Virtual	32	2		INS
Virtual	32	3		INS
Virtual	32	4		INS
Virtual	32	5		INS
Virtual	32	6		OUS
Virtual	32	7		OUS
Virtual	32	8		OUS

In this case, the equation for bandwidth calculation, based on the previous example, will change as follows:

Required Bandwidth

$$\begin{aligned} &= (\text{No. of Fax Machines} \times \text{Required Bandwidth for the G.711 codec}) + \\ &[(\underline{10} - \text{No. of Fax Machines}) \times \text{Required Bandwidth for Voice Communication}] \\ &= (2 \times 87.2) + [(\underline{10} - 2) \times 31.2] \\ &= 424 \text{ (kbps)} \end{aligned}$$

8.2.4 Virtual VoIP Gateway Card Specifications

For details about the RFCs and protocols for the V-IPGW16 card, refer to the following specifications.

ITU-T	H.323
	H.225.0
	H.245
Codecs	G.711 (a-law and μ -law)
	G.729A
Voice Operations	Echo Cancellation (48 ms)
	Jitter Buffer (200 ms)
	VAD (Voice Activity Detection) ¹
	PLC (Packet Loss Concealment)
DTMF Relay	Inband/Outband (RFC2833)/Outband (H.245)
Fax Relay	G.711 Inband/T.38
Protocol/Function	RTP
	RTCP

¹ VAD is only available for codec G.711.

8.3 SIP Trunks

This section provides information on using SIP trunks with the PBX.

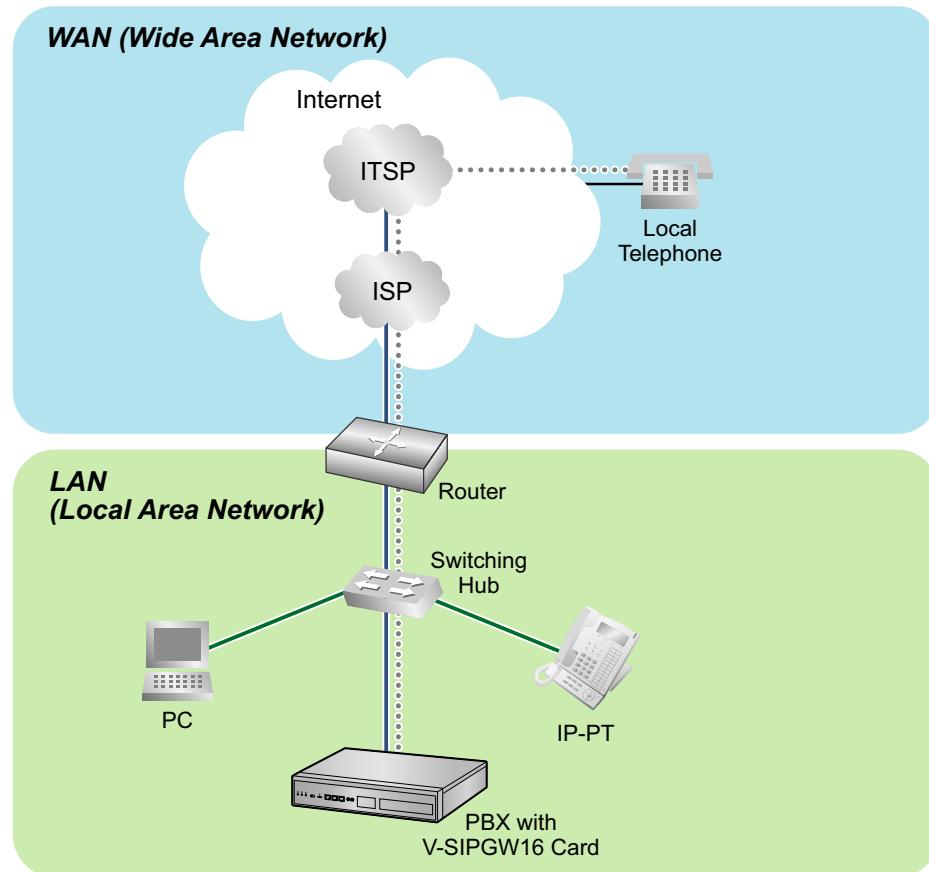
8.3.1 IP Telephony Service

The Virtual 16-Channel SIP Trunk Card (V-SIPGW16) is a virtual trunk card which is designed to be easily integrated into an Internet Telephony Service provided by an ITSP (Internet Telephony Service Provider).

As a major SIP Provider, an ITSP provides its telephony service partly through the conventional telephone network (e.g., ISDN and Mobile), which is fee-based. An ISP (Internet Service Provider), another major SIP Provider, does not provide telephone connection itself. However, providing its users with Internet access, an ISP provides voice communication on the Internet for free. In this way, with VoIP technology based on the SIP protocol, the cost of voice communication can be much cheaper than conventional telephone networks. A maximum of 16 V-SIPGW16 cards can be installed to the virtual slots of the PBX. The channel capacity of the card allows users to connect to up to 32 different ISP/ITSPs.

V-SIPGW16 Connection Outline

The following diagram illustrates a simple VoIP network connecting the V-SIPGW16 card to the Internet.



Requirements for Internet Telephony Service

- You need to subscribe with an ISP for Internet connection.

- You need to subscribe with an ITSP for telephone connection. The ISP and ITSP may be part of the same company.

Note

- VoIP communication using the V-SIPGW16 card may deteriorate depending on the ITSP being used.
- VoIP communication using the V-SIPGW16 card may deteriorate depending on the network conditions.

DNS (Domain Name System)

A DNS server normally provides the name resolution service for your PC. As domain names are alphabetic, they are easier to remember. The Internet, however, is based on IP addresses. Therefore, every time a domain name is used, a DNS server must translate the name into the corresponding IP address, and vice versa. For example, the domain name `www.example.com` may be translated to `192.0.34.166`. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

NAT Traversal

When NAT/NAPT (Network Address Port Translation) is enabled, the router translates a local IP address from the PBX into a global IP address. However, the router with NAT enabled does not translate local IP addresses stored in SIP messages into global IP addresses.

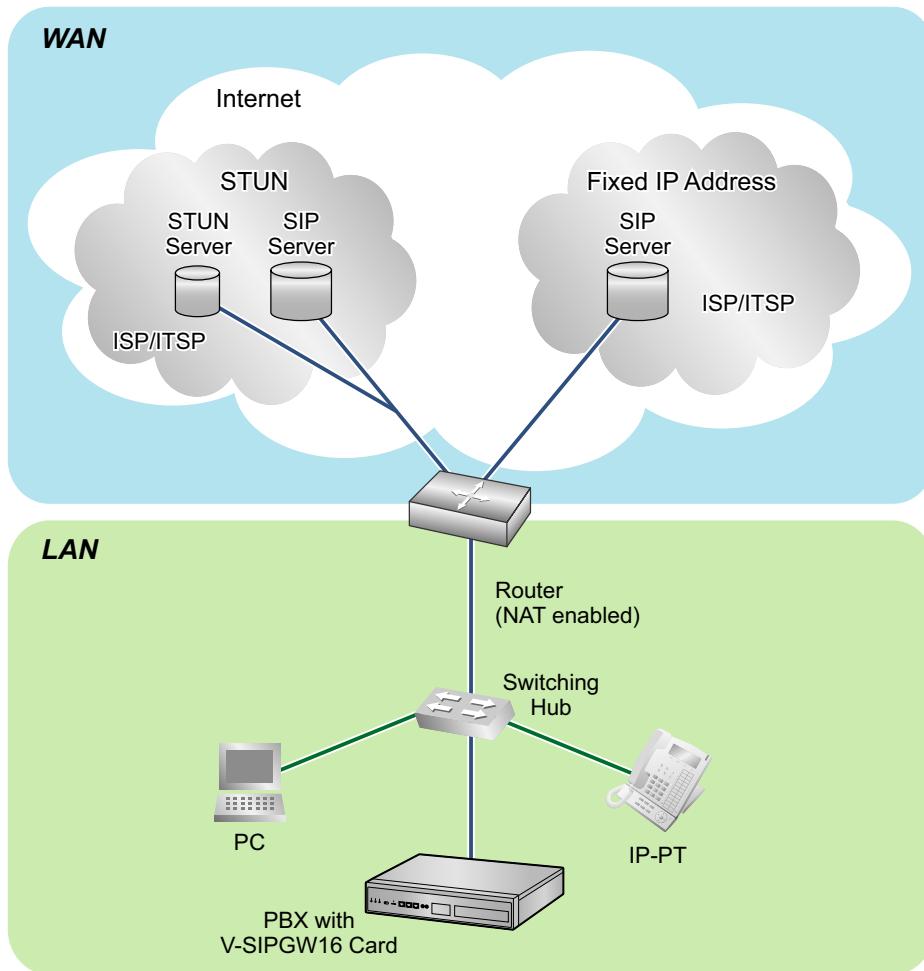
Therefore, the address which the SIP Server recognises as the destination IP address to reply to is actually the local IP address of the PBX, not the global IP address of the router. Therefore, if the SIP Server receives a SIP message from the PBX and sends a message back to the PBX using the address stored in the SIP message, the packet information will not reach the PBX.

STUN Servers function to solve the global IP address problem under certain NAT conditions, for example, in case of full duplex communication. A STUN Server, used alongside the SIP Server, finds out the global IP address of the router with NAT enabled. With the STUN feature enabled, the packet information sent by the SIP Server is able to "traverse" NAT and reach the PBX.

The settings can be configured to specify whether to enable the NAT Traversal feature for each ISP/ITSP. In addition, the NAT Traversal method can be selected from "STUN" and "Fixed IP Address". For details, refer to "9.9 PBX Configuration—[1-1] Configuration—Slot—V-SIPGW—Shelf Property" in the PC Programming Manual.

The V-SIPGW16 card may require the NAT Traversal feature to be enabled to connect to the WAN via a router. The following diagram illustrates how VoIP communication is enabled between the V-SIPGW16 card and the SIP Server (SIP Receiver) via a router with NAT enabled.

8.3.1 IP Telephony Service



Note

- If an ISP/ITSP uses a device such as SBC (Session Border Controller), you may not have to enable the NAT Traversal feature.
- A STUN Server is supplied by an ISP/ITSP, and not included with the PBX.

8.3.2 SIP Requirements

Port Requirements

Required Ports for Each Channel

When configuring a router with NAT enabled, you need to secure a certain number of ports for each SIP and RTP/RTCP channel. For RTP/RTCP, the number of required ports is double the number of activated SIP trunks (Ch). For SIP signalling, the number of required ports is always one regardless of the number of activated SIP trunks (Ch).

<Example>

If 4 SIP trunk channels are activated, you need the following number of ports:

Protocol Type	Required Port
RTP	4
RTCP	4
SIP	1
Total	9

Firewall Requirements

If the VoIP network contains a firewall, the firewall must be configured appropriately to allow VoIP packets to pass through the network without being blocked by filtering. For the protocols and port numbers that the PBX uses for VoIP communication, refer to "8.5 Port Security".

The ports for which you need to configure the firewall may vary depending on the network conditions. For more information, consult your network administrator.

8.3.3 Router Requirements

- Port Forwarding:
It may be necessary to set the NAT router so that it forwards the incoming packets to the IP address of the V-SIPGW16 card if all of the following conditions are met:
 - the PBX uses a STUN server;
 - a V-SIPGW16 card is located under a NAT router;
 - incoming packets are routed to a SIP Client port or NAT Voice (RTP) UDP port indicated in "8.5 Port Security".

- SIP-NAT Feature:

When a V-SIPGW16 card is located under a NAT router that supports the SIP-NAT feature^{**1}, it is recommended to disable this feature.

^{**1} When NAT is enabled, the router translates the IP address stored in the IP header and the port number stored in the UDP header. When SIP-NAT is enabled, the router also translates the IP address and port number stored in SIP messages.

8.3.4 Bandwidth Requirements

When using the V-SIPGW16 card, you must ensure that the WAN has enough bandwidth to support VoIP communications. Refer to the table below and ensure that the sum of the required bandwidth for each channel is smaller than the amount the WAN (e.g., ADSL network) can provide.

8.3.4 Bandwidth Requirements

Note that the amount in the table is only a guide. Subscribe to a network that has enough bandwidth. If the amount of bandwidth required for VoIP communications is larger than what the network can accommodate, speech quality will be compromised.

Required Bandwidth for Each Channel

The required bandwidth depends on what combination of codecs and packet sending interval is used. Keep in mind the following points about the type of codec and packet sending interval, in terms of the speech quality:

- The speech quality of the codecs varies as follows: G.711 (High), G.729A (Low)
- The shorter the packet sending interval, the higher the speech quality.
- The higher the speech quality the V-SIPGW16 card provides, the more bandwidth the WAN requires.

Codec	Packet Sending Interval					
	10 ms	20 ms	30 ms	40 ms	50 ms	60 ms
G.711	110.4 kbps	87.2 kbps	79.5 kbps	75.6 kbps	73.3 kbps	71.7 kbps
G.729A	54.4 kbps	31.2 kbps	23.5 kbps	19.6 kbps	17.3 kbps	15.7 kbps

8.3.5 Virtual SIP Trunk Card Specifications

For details about the RFCs and protocols for the V-SIPGW16 card, refer to the following specifications.

Items	Specification
SIP RFCs	RFC3261 (UDP only)
	RFC3262 (PRACK)
	RFC3264 (Offer/Answer)
	RFC3311 (UPDATE)
	RFC3581 (Symmetric Response Routing/rport)
	RFC4028 (Session Timer)
Codecs	G.711 (a-law and μ-law)
	G.729A
Voice Options	Echo Cancellation (48 ms)
	Jitter Buffer (200 ms)
	VAD (Voice Activity Detection) ¹
	PLC (Packet Loss Concealment)
DTMF Relay	Inband/Outband (RFC2833)/Outband (SIP INFO)
Fax Relay	G.711 Inband/T.38
Protocol/Function	RTP
	RTCP
	DNS (A/SRV)
	NAT Traversal (STUN)
	QoS (ToS field setting in IP header of RTP/RTCP)

¹ VAD is only available for codec G.711.

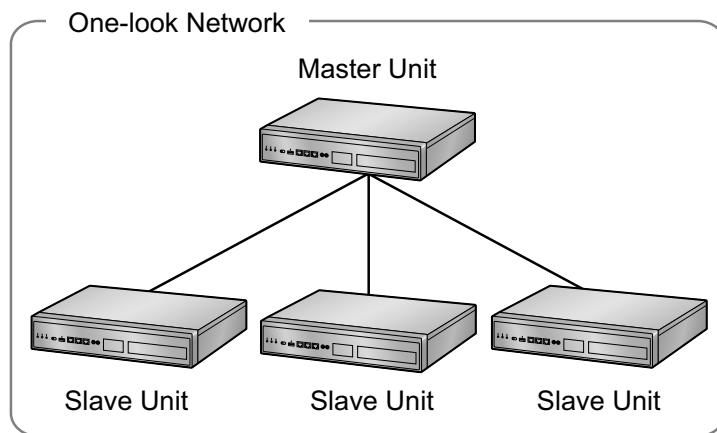
8.4 Types of PBX Networks

This section gives an overview of the types of networks the PBX can participate in.

8.4.1 One-look Network

This section gives an overview of One-look networks.

Image of a One-look network:



Features

- A maximum of 16 PBXs can be connected in a One-look network.
- A maximum of 8 legacy gateways can be included in a One-look network.
- The PBXs specified as Slave units use settings provided by the PBX specified as the Master unit, so a considerable amount of setup is done automatically.
- Resource sharing allows users to interact as if they were all connected to one PBX, which eliminates the need to manage information such as PBX access codes.
- All units in a One-look network can be programmed from one location.

Note

The MASTER indicator LED indicates whether the unit is configured as a Master unit or Slave unit. For details, refer to "LED Indications".

Conditions

- A One-look network must consist only of KX-NS1000 PBXs.
- The sites that will be included in a One-look network must be connected over a private IP network before setting up the One-look network.

Bandwidth Requirements

When implementing a One-look network, you must ensure that the IP network has enough bandwidth to support both VoIP communication and One-look network signalling between PBXs. If the amount of bandwidth required for VoIP communications and signalling is more than the network can accommodate, speech quality will degrade. In addition, there may be an adverse effect on the performance of other applications (e.g., e-mail or

Web applications) that use the same network. Therefore, care must be taken when assessing bandwidth requirements.

Inform your network administrator of the required bandwidth, and make sure that the network can support VoIP communications and signalling even under conditions of maximum network traffic.

Required Bandwidth per Call

The required bandwidth depends on the following factors:

- The maximum number of simultaneous calls
- Packet sending interval
- Type of codec used
- Telephone type

Keep in mind the following points about the types of codecs and packet sending intervals, in terms of speech quality:

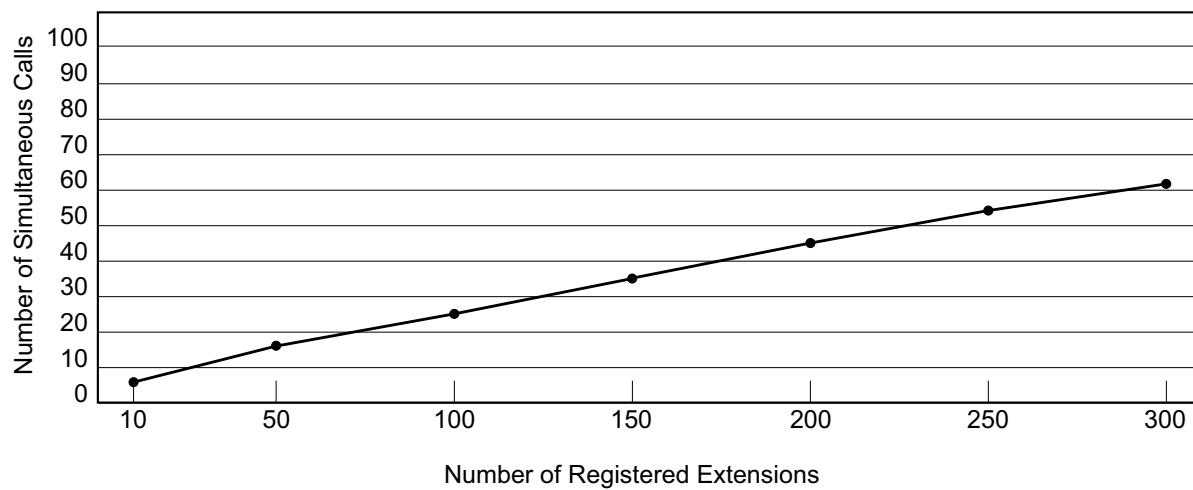
- The speech quality of the codecs varies as follows: (High) G.722, G.711, G.729A (Low)¹¹
- The shorter the packet sending interval, the higher the speech quality.
- The higher the speech quality an IP telephone provides, the more bandwidth it requires.

¹¹ When the preferred codec of each party differs, the call will be established using the lower quality codec.

For example, if the caller prefers G.711 while the called party prefers G.729A, the call will be established using G.729A.

Number of Simultaneous Calls

The number of simultaneous calls is proportional to number of extensions registered to the PBX, as shown in the chart below. The proportion is approximately 0.25 when the number of registered extensions is 100. For more information about the number of simultaneous calls, ask your local Panasonic dealer.



Number of Registered Extensions	10	50	100	150	200	250	300
Number of Simultaneous Calls	6	16	26	35	44	53	61

Required Bandwidth per Call for VoIP Communication

The required bandwidth for VoIP communication is determined by the codec used and the packet sending interval.

8.4.1 One-look Network

Codec	Packet Sending Interval			
	20 ms	30 ms	40 ms	60 ms
G.711/G.722	80 kbps	74.7 kbps	72 kbps	69.4 kbps
G.729A	24 kbps	18.7 kbps	16.0 kbps	13.4 kbps

¹ G.722 is only available for calls between KX-NT300 series IP-PTs, KX-NT500 series IP-PTs, and some SIP phones that support this codec during peer-to-peer communication. For details, refer to "5.2.3 Peer-to-Peer (P2P) Connection" in the Feature Guide.

Required Bandwidth per Call for Signalling

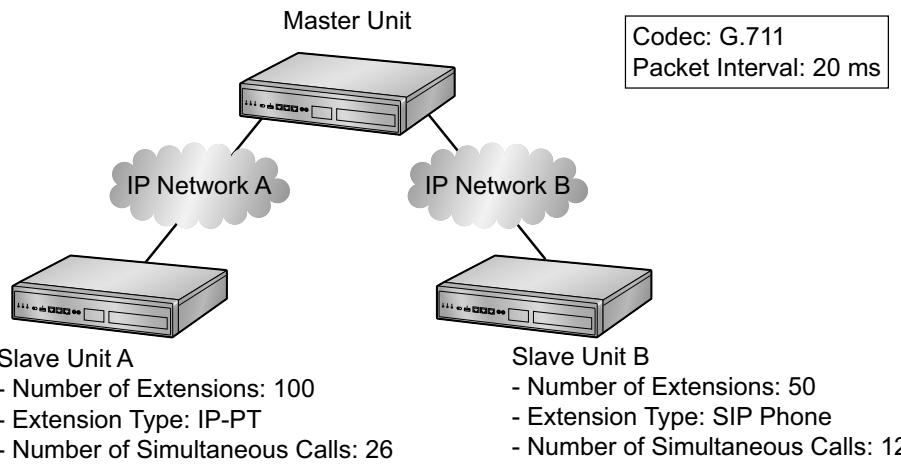
In a One-look network, a certain amount of bandwidth is required for the master unit to handle all the calls in the network. The required bandwidth depends on the type of IP telephone.

Phone Type	Required Bandwidth
IP Telephones (except SIP phones)	43.0 kbps
SIP Phone	16.0 kbps

Example:

The following examples show different cases of assessing bandwidth for a One-look network.

In this example, there are 3 PBXs in a One-look network.



Bandwidth assessment for IP network A:

- Bandwidth required for VoIP communication

$$\begin{aligned}
 &= \text{Number of simultaneous calls} \times 2 \times \text{Required bandwidth for codecs (kbps)} \\
 &= 26 \times 2 \times 80 \\
 &= 4160 \text{ kbps}
 \end{aligned}$$
- Bandwidth required for signalling

$$\begin{aligned}
 &= \text{Number of simultaneous calls} \times \text{Signalling bandwidth per a call for IP telephones (except SIP phones) (kbps)} \\
 &= 26 \times 43.0 \\
 &= 1118.0 \text{ kbps}
 \end{aligned}$$
- Total required bandwidth for IP network A

$$\begin{aligned}
 &= \text{Bandwidth required for VoIP communication (kbps)} + \text{Bandwidth required for signalling (kbps)} \\
 &= 4160 + 1118.0 \\
 &= 5278.0 \text{ kbps}
 \end{aligned}$$

Bandwidth assessment for IP network B:

- Bandwidth required for VoIP communication
= Number of simultaneous calls \times 2 \times Required bandwidth for codecs (kbps)
= $12 \times 2 \times 80$
= 1920 kbps
- Bandwidth required for signalling
Number of simultaneous calls \times Signalling bandwidth per a call for SIP phones (kbps)
= 12×16
= 192 kbps
- Total required bandwidth for IP network B
= Bandwidth required for VoIP communication (kbps) + Bandwidth required for signalling (kbps)
= $1920 + 192$
= 2112 kbps

Required Items

- KX-NSN001: Activation Key for One-look Network (One-look Network)

Networking Notes

- When setting up a PBX using Easy Setup Wizard, you specify whether the PBX will be the Master unit or a Slave unit. For more details, refer to "5.4.1 Easy Setup Wizard".
- You can add Slave units to the One-look network using Web Maintenance Console. For more details, refer to "5.5 Programming a One-look Network".

Note

- For more details about One-look networks, refer to "4.2 One-look Networking" in the Feature Guide.
- For details about configuring and programming a One-look networks, refer to "3.1.1 Home Screen—Add Site Wizard" in the PC Programming Manual.

8.4.2 One-look Networking Survivability

This section provides an overview of One-look Networking Survivability.

When a fault occurs in a site containing the Master unit, the communication services in the One-look network will stop. However, it is possible to use a Slave unit as a temporary Master unit to operate the communication services using One-look Networking Survivability.

This feature allows users to keep using communication services via a temporary Master unit even when the original Master is not operating.

Without this feature, when a fault occurs to the Master unit in a One-look network, all the services in all the sites in the One-look network will stop. However, if this feature is in use, some communication services can continue even during a network failure.

Elements in One-look Networking Survivability

When One-look Networking Survivability is used, sites in the network will be classed as one of the following.

Master site

A site in a One-look network that contains the Master unit which controls the One-look network.

Backup master site

A site in a One-look network that works as a Slave site normally. When a fault happens to the Master site, this site can act as Master site temporarily.

8.4.2 One-look Networking Survivability

Isolated site

A site that will be disconnected from other sites during a fault.

Slave site

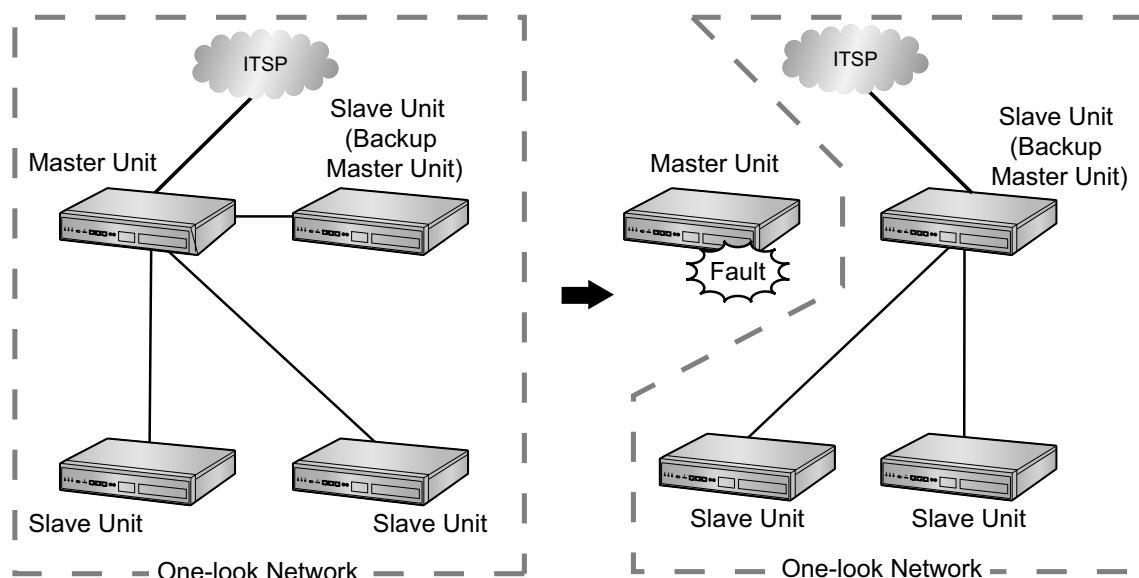
A Slave site where the Isolated setting is disabled.

Backup Master Mode

In this mode, you specify a Backup master site. When a fault occurs to a Master site in a One-look network, the Backup master site will act as Master site temporarily after the whole system resets. Communication services will then be provided from the Backup master site.

Notice

Only one Backup master site can exist in a One-look network.



Notice

All Slave units will restart. Depending on the makeup of the network, it may take 15 minutes or more for the system to become fully operational in Backup Master mode.

LED Indication

Operating Status	Master Unit		Slave Unit (Backup Master Unit)		Slave Unit	
	STATUS LED	MASTER LED	STATUS LED	MASTER LED	STATUS LED	MASTER LED
Normal	Green ON	Green ON	Green ON	Amber ON	Green ON	Amber ON
After a Fault at the Master Site	-	-	Green ON	Green Flashing	Green ON	Amber ON

For more information about LED indications, refer to "LED Indications" in "4.3.1 Mother Board".

Similarly, when you press the **System Alarm** button set for the flexible button on the PT, a message that indicates the PBX status has changed will be displayed on the LCD on the PT.

For details, refer to "5.6.4 Local Alarm Information" in the Feature Guide.

Backup Master Mode Setup Procedure

Specifying a Backup master site

To use Backup master mode, you have to specify a site in the One-look network as a Backup master site.

Only a Slave site that is in the INS or FAULT state can be specified as the Backup master site.

The Backup master site is set using Web Maintenance Console.

Procedure

1. On the Home screen, click .
2. Select the desired site in **Backup Master**.

Removing or changing the Backup master setting

You can remove, and change the Backup master site setting using Web Maintenance Console.

Procedure

1. On the Home screen, click .
2. Select **Unassigned** in **Backup Master** to remove the Backup master setting. If you want to assign a different site as the Backup master, select the desired site in **Backup Master**.

Note

- You must remove the Backup master setting before selecting a different site.
- If you selected a new Backup Master unit, it will restart.

Recovering from Backup Master Operation to Master Operation

Recovering from Backup master operation to Master operation is only possible when logged in to Web Maintenance Console as an Installer.

Login as Installer to Web Maintenance Console of the Master site, and then perform the recovery.

Procedure

1. Log in to the Backup Master site using Web Maintenance Console.
2. Right click the Backup Master site on the Home screen, and then click **Normal Mode**.
The Backup Master site will start acting as a Slave site, and the original Master site will take over control of the One-look network.

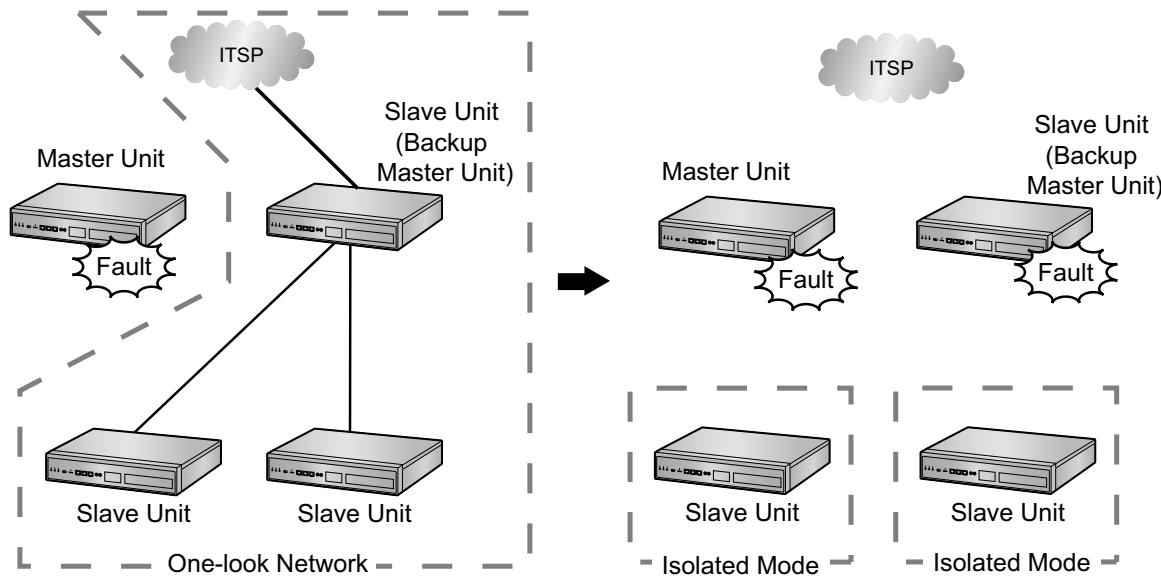
Reference

For more information about Backup master mode, refer to "4.2.3.1 Backup Master Mode and Isolated Mode" in the Feature Guide.

For more information about programming Backup master mode, refer to "3.1 Home Screen" in the PC Programming Manual.

Isolated Mode

When faults occur to a Master site and Backup master site, or when a Slave site is isolated because of network failure, the Slave site can continue limited communication services independently at its site.



Notice

The Slave unit will restart. Depending on the makeup of the network, it may take 15 minutes or more for the unit to restart in Isolated mode.

Note

The Slave site can act in Isolated mode in the following conditions:

- The connection to the Master site has failed.
- The connection to the Backup master site has failed. (If a backup master exists in the One-look network)
- The **Isolated Mode** setting is enabled in the Slave unit.

LED Indication

Operating Status	Slave Unit	
	STATUS LED	MASTER LED
Normal	Green ON	Amber ON
Isolated Mode	Green ON	Red Flashing

For more information about LED indications, refer to "LED Indications" in "4.3.1 Mother Board".

Similarly, the **System Alarm** button set for the flexible button on the PT lights to indicate the PBX status has changed, and a message will be displayed on the LCD on the PT.

For details, refer to "5.6.4 Local Alarm Information" in the Feature Guide.

Isolated Mode Programming Procedure

Enabling Isolated Mode

The **Isolated Mode** setting is set to **Disable** by default.

Follow the procedure below to enable this setting using Web Maintenance Console.

Procedure

1. Select the Slave unit to be programmed from the Home screen, or by using the site selection drop-down menu.
2. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot** → **Site Property** → **Main**.
3. Select **Enable** for **Isolated Mode**.
4. Click **OK**.

Disabling Isolated Mode

You can disable the **Isolated Mode** setting using Web Maintenance Console.

Procedure

1. Select the Slave unit to be programmed from the Home screen, or by using the site selection drop-down menu.
2. Click **Setup** → **PBX Configuration** → **Configuration** → **Slot** → **Site Property** → **Main**.
3. Select **Disable** for **Isolated Mode**.
4. Click **OK**.

Recovering from Isolated Operation

To recover from Isolated operation, restart the Slave site using Web Maintenance Console or edit the system data for the Isolated site.

Procedure

1. Log in to the Isolated site using Web Maintenance Console.
2. Right click the Isolated site on the Home screen, and then click **Normal Mode**.
The Isolated site will start running as a Slave unit in the One-look network.

Reference

For more information about Isolated mode, refer to "4.2.3.1 Backup Master Mode and Isolated Mode" in the Feature Guide.

For more information about programming Isolated mode, refer to "9.5.1 PBX Configuration—[1-1] Configuration—Slot—Site Property—Main—◆ Isolated Mode" in the PC Programming Manual.

Automatic Rerouting to Secondary PBX

IP terminals can switch connection from primary PBX to secondary PBX when a fault occurs to the primary PBX.

Notice

When an IP phone connects to the PBX via a VPN using the built-in router, the IP phone cannot be rerouted to the secondary PBX if the primary PBX fails. This is because if the PBX fails, the VPN session also fails. Therefore, the IP phone cannot communicate with the secondary PBX at the time. In addition, when the primary and secondary PBXs are connected to each other via a VPN using the built-in router, the same limitation is applied.

Therefore, if automatic rerouting functionality is required for IP phones, they should be connected using an external router instead of the built-in router.

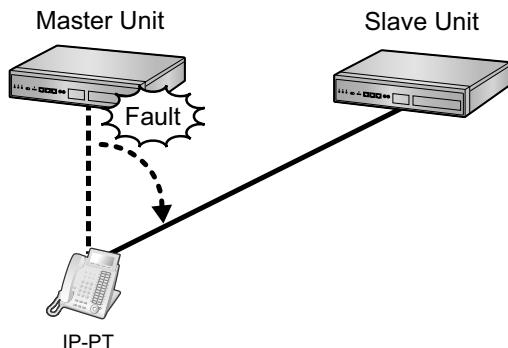
Note

- This feature is available for the following IP terminals.
 - KX-NT300 series and KX-NT500 series IP proprietary telephones
 - KX-UT series SIP phones (firmware update required)
 - SIP-CSs

8.4.2 One-look Networking Survivability

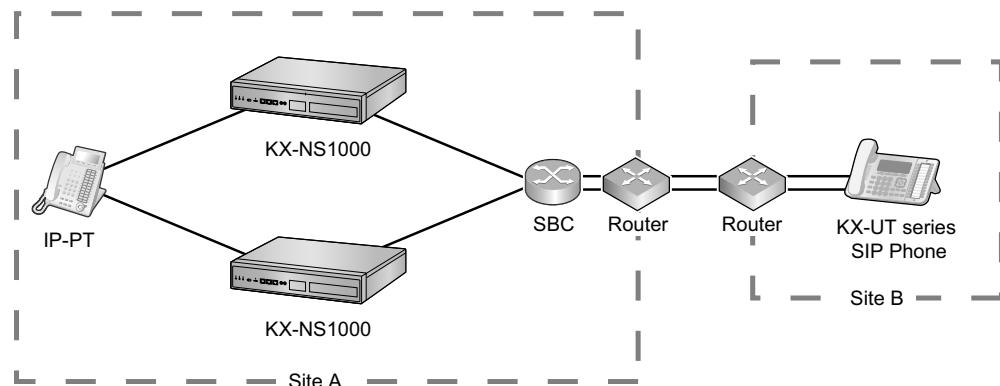
- The following extensions and trunks are not automatically rerouted.
 - Legacy extensions and legacy trunks that are connected to the KX-NS1000
 - Extensions and trunks used with legacy gateways
- There are conditions for specifying a Primary PBX and Secondary PBX for a KX-UT series SIP phone installed at a remote site when the One-look network consists of 3 or more sites.
For more details, refer to "5.2.2.3 Simple Remote Connection" in the Feature Guide.

Rerouting the IP terminal to the Slave unit



Notes for IP Terminals using Automatic Rerouting to Secondary PBX

When IP terminals switch PBXs via the Automatic rerouting feature, the IP terminals require 2 port forwarding settings to the gateway router.



Configuration Procedure

For KX-NT300 series and KX-NT500 series IP-PTs

To set a secondary PBX, refer to "5.8.1 Assigning IP Addressing Information".

For KX-UT series SIP phones

The secondary PBX setting is downloaded from Web Maintenance Console and automatically configured.
No operation on the SIP phones is required.

For S-PSs

To set a secondary PBX, refer to the documentation for the S-PS.

Reference

For more information about Automatic rerouting mode, refer to "4.2.3.2 Automatic Rerouting to Secondary PBX" in the Feature Guide.

For more information about programming Automatic rerouting mode, refer to "9.15 PBX Configuration—[1-1] Configuration—Slot—V-IPEXT32—Port Property—Secondary Setting" in the PC Programming Manual.

UM Group Failover

During a PBX operation failure, incoming calls will be automatically redirected to the specified Unified Messaging group.

Each Unified Messaging group can be assigned a failover destination.

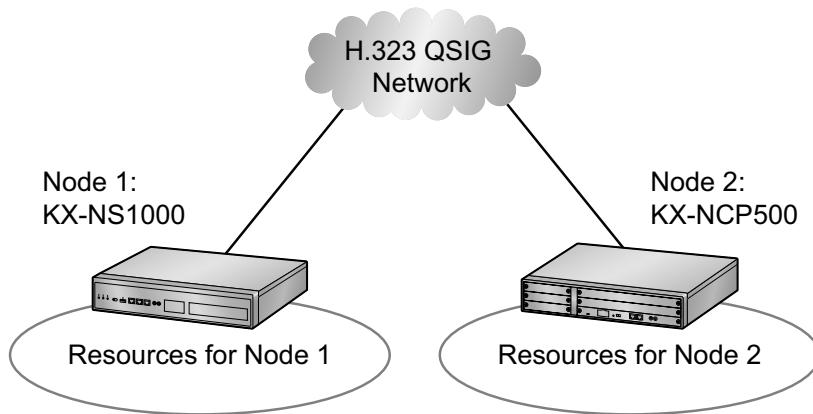
Reference

For more information about UM Group Failover, refer to "4.2.3.3 UM Group Failover" in the Feature Guide. For information about programming UM Group Failover, refer to "11.7.2 PBX Configuration—[3-7-2] Group—UM Group—Unit Settings" in the PC Programming Manual.

8.4.3 H.323 QSIG Network

This section gives an overview of H.323 QSIG networks.

Image of a H.323 QSIG network:



Features

- H.323 QSIG networks can include non-KX-NS1000 PBXs (e.g., KX-TDE200, KX-NCP500).
- Resources are not available to extension users of other PBX without explicit configuration.

Conditions

- PBXs in an H.323 QSIG network must be connected over a private IP network.

Bandwidth Requirements

Refer to "8.2.3 Bandwidth Assessment".

Required Items

- V-IPGW16: Virtual 16-Channel VoIP Gateway Card

Note

The following activation key is required for enhanced QSIG network features (NDSS, Centralised Voice Mail, etc.).

- KX-NSN002: Activation Key for QSIG Network (QSIG Network)

Networking Notes

When a KX-NS1000 is included in the H.323 QSIG network, the PBX must be specified as a Master unit.

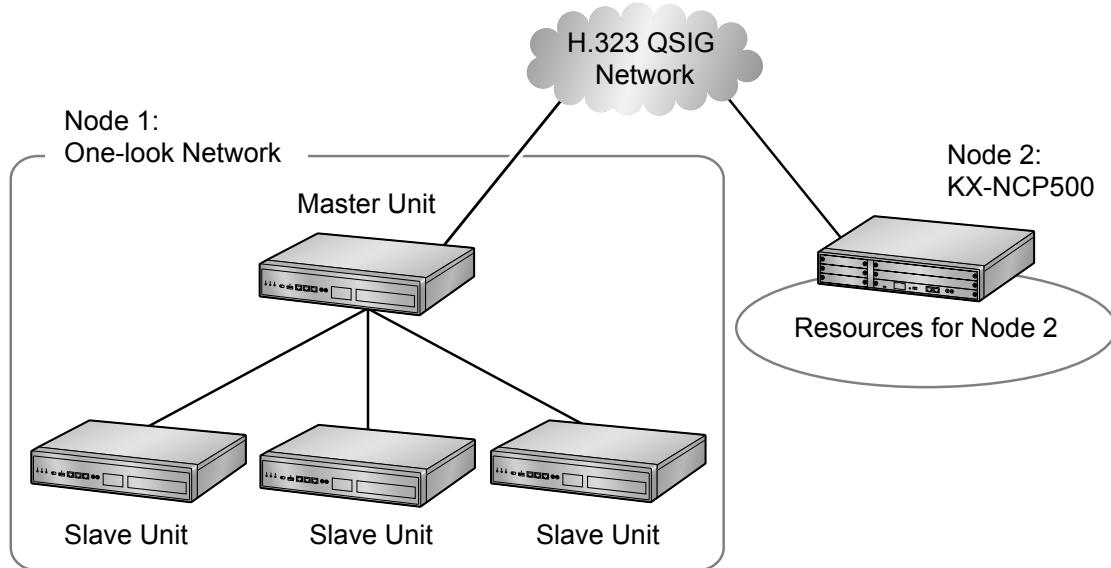
Note

- For more details about H.323 QSIG networks, refer to "4.3.1 TIE Line Service" in the Feature Guide.
- For details about configuring and programming a H.323 QSIG network, refer to "◆ TIE Line Access" in the PC Programming Manual.

8.4.4 Working with Multiple PBX Networks

It is possible to connect a One-look network to other PBXs via H.323 QSIG network. In an H.323 QSIG network, the One-look network appears as one PBX.

Image of multiple PBX networks:



The following table shows the maximum number of sites/nodes that can be included in each type of network.

Network Type	Method	Maximum Sites/Nodes
Private Network	One-look Network	16 sites
QSIG Network	H.323 QSIG Network	512 nodes
Multiple PBX Networks	One-look Network and H.323 QSIG Network	8192 sites

Note

For more details about using multiple PBX networks, refer to "4.2.2 Network Type Comparison" in the Feature Guide.

8.5 Port Security

If the VoIP network contains a firewall, the firewall must be configured appropriately to allow VoIP packets to pass through certain ports of the ports listed below without being blocked by filtering. The ports for which you need to configure the firewall may vary depending on the network conditions.

For more information, consult your network administrator.

The following table shows the PBX's ports used for IP communications. Any access to the ports not in this list is ignored.

Port Numbers for LAN Port

Port Number	Protocol	Application	Client/Server	Changeable/ Fixed
25	TCP/UDP	SMTP	Server	Changeable
53	UDP	DNS	Server	Fixed
67	UDP	DHCP	Server	Changeable
68	UDP	DHCP	Client	Changeable
80	TCP	HTTP	Server	Changeable
123	UDP	NTP	Server	Fixed
143	TCP	IMAP	Server	Changeable
161	UDP	SNMP	Server	Changeable
443	TCP	HTTPS	Server	Changeable
465	TCP/UDP	SMTP over SSL	Server	Changeable
993	TCP	IMAP over SSL	Server	Changeable
1717	UDP	Connectionless UDP	-	Changeable
1718	TCP	Connectionless TCP	-	Changeable
1719	UDP	H.225 RAS	-	Changeable
1720	TCP	H.225 Call Signal	-	Changeable
2103	TCP	CMM	Server	Fixed
2300	TCP	Telnet-SMDR	-	Changeable
2727	UDP	MGCP ¹	-	Changeable
3493	TCP	UPS ²	-	Fixed
3702	UDP	WSD	Server	Changeable
4560–4561	UDP	PSAP	-	Changeable
4562	UDP	SSAP	-	Changeable
5060	UDP	SIP UA (EXT)	-	Changeable
7547	TCP	CWMP	Server	Changeable
7580	TCP	HTTP	Server	Changeable

Port Number	Protocol	Application	Client/Server	Changeable/ Fixed
8080	TCP	Web Maintenance Console	-	Changeable
9300	UDP	PTAP	-	Changeable
10000– 10895	TCP	H.323 Dynamic Port (H.225 Send, H.245 Send/ Receive, Connection-less [TCP] Send Port)	-	Changeable
20000	TCP	UM-VMA ³	Server	Fixed
30021	TCP/UDP	FTP/FTPS	Server	Changeable
32727	UDP	MGCP ¹ for IP-CS	-	Changeable
33090	UDP	ACS-MDW	Server	Fixed
33091				
33092	TCP			
33131				
33321	TCP	Access Point Login (Telnet)	Server	Changeable
33333	TCP	CTI 3rd Party Connection	-	Changeable
33334	TCP	CTI 1st Party Connection	-	Changeable
33478	UDP	STUN	Client	Changeable
33702	UDP	ACS-MDW (WSD)	Server	Fixed
35060	UDP	SIP UA (CO)	-	Changeable
37547	TCP	CWMP	Server	Changeable
37580	TCP	HTTPS	Server	Changeable
39300	UDP	PTAP for IP-CS	-	Changeable
40000– 40095	TCP/UDP	FTP/FTPS-Data	Server	Changeable
50000– 65535 (Ephemeral)	UDP	SNMP TRAP	Client	Fixed
	TCP/UDP	FTP	Client	
	TCP/UDP	FTP/FTPS-Data	Client	
	UDP	NTP	Client	
	UDP	DNS	Client	
	UDP	SYSLOG	Client	
	TCP/UDP	SMTP	Client	
	TCP/UDP	SMTP over SSL	Client	
	TCP/UDP	POP3	Client	

8.5 Port Security

Port Number	Protocol	Application	Client/Server	Changeable/ Fixed
	TCP/UDP	ACS-MDW	Server	

¹ Media Gateway Control Protocol. Used for call control command data and LCD/LED data transmission.

² Used by UPS daemon.

³ Used by Unified Messaging.

Port Numbers for MNT Port

Port Number	Protocol	Application	Client/Server	Changeable/ Fixed			
21	TCP/UDP	FTP/FTPS	Server	Changeable			
25	TCP/UDP	SMTP	Server	Changeable			
53	UDP	DNS	Server	Changeable			
67	UDP	DHCP	Server	Changeable			
80	TCP	HTTP	Server	Changeable			
123	UDP	NTP	Server	Fixed			
143	TCP	IMAP	Server	Changeable			
161	UDP	SNMP	Server	Changeable			
443	TCP	HTTPS	Server	Changeable			
465	TCP/UDP	SMTP over SSL	Server	Changeable			
993	TCP	IMAP over SSL	Server	Changeable			
2103	TCP	CMM	Server	Fixed			
2300	TCP	Telnet-SMDR	-	Changeable			
3493	UDP	UPS ¹	-	Fixed			
3702	UDP	WSD	Server	Changeable			
7574	TCP	CWMP	Server	Changeable			
8080	TCP	Web Maintenance Console	-	Changeable			
33090	UDP	ACS-MDW	Server	Fixed			
30091							
30092	TCP						
33131							
33321	TCP	Access Point Login (Telnet)	Server	Changeable			
33333	TCP	CTI 3rd Party Connection	-	Changeable			
33334	TCP	CTI 1st Party Connection	-	Changeable			
33702	UDP	ACS-MDW (WSD)	Server	Fixed			

Port Number	Protocol	Application	Client/Server	Changeable/ Fixed
40000–40095	TCP/UDP	FTP/FTPS-Data	Server	Changeable
50000–65535 (Ephemeral)	UDP	SNMP TRAP	Client	Fixed
	TCP/UDP	FTP	Client	
	TCP/UDP	FTP/FTPS-Data	Client	
	UDP	NTP	Client	
	UDP	DNS	Client	
	UDP	SYSLOG	Client	
	TCP/UDP	SMTP	Client	
	TCP/UDP	SMTP over SSL	Client	
	TCP/UDP	POP3	Client	
	TCP/UDP	ACS-MDW	Server	

¹ Used by UPS daemon.

Port Numbers for Optional DSP Cards

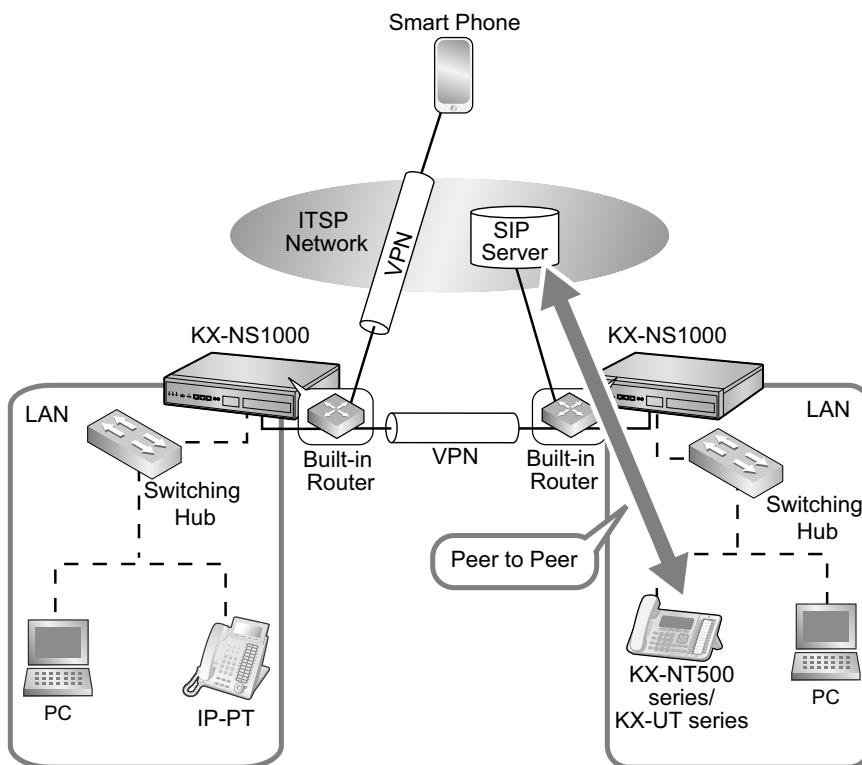
Port Number	Protocol	Application	Client/Server	Changeable/ Fixed
12000–13535	UDP	RTP/RTCP	-	Changeable
16000–18047	UDP	RTP/RTCP for NAT traversal	-	Changeable

8.6 Built-in Router

8.6.1 Built-in Router Overview

This PBX has a built-in router. Activating the built-in router allows you to separate PBX control traffic and voice packets from the existing LAN router. Additionally, the router supports IPsec VPN, which allows you to easily establish secure connections among multiple main units in a One-link network. Also, secure connections can be established with smart phones.

The built-in router functions as an IPv4 access router and supports Gigabit Ethernet.



The built-in router has the following features.

Feature		Description & Reference
WAN	WAN Connection	Sets WAN-interface settings. → 5.4.1 Easy Setup Wizard → 8.6.2 WAN Connection
	DHCP Relay Agent	Relays DHCP messages to a DHCP server on the WAN side. → 8.6.3 DHCP Relay Agent
	Dynamic DNS	Dynamically notifies and updates the DNS server with dynamically changing IP addresses. → 8.6.4 Dynamic DNS

Feature		Description & Reference
	DNS Client	The DNS client feature of the built-in router. → 8.6.5 DNS Client
	Protocol Bridge	Acts as a bridge between the WAN and LAN for packets of a specified protocol. → 8.6.6 Protocol Bridge—IPv6 Bridge → 8.6.7 Protocol Bridge—PPPoE Bridge
	MAC Address Clone	Changes the WAN interface's MAC address to match one registered with the ISP. → 8.6.8 MAC Address Clone
Routing		Sets the routing information. → 8.6.9 Routing
Firewall		Firewall security settings. → 8.6.10 Firewall
	Packet Filtering	Determines which packets are allowed to cross the WAN–LAN boundary, based on specified conditions. → 8.6.11 Firewall—Packet Filtering
	Stateful Packet Inspection (SPI)	Determines dynamically whether to allow or deny packets based on the packets' contents. → 8.6.12 Firewall—Stateful Packet Inspection
	DoS Protection	Contains security rules for protecting the system from port scans and DoS attacks. → 8.6.13 Firewall—DoS Protection
	Other Security Settings	Contains other security settings. → 8.6.14 Firewall—Other Security Settings
NAT/NAPT	Dynamic NAPT (IP masquerade)	Dynamically changes LAN-side IP addresses and port numbers for communication with the WAN side. → 8.6.15 Dynamic NAPT (IP masquerade)
	Static NAPT (Port Forwarding)	Fowards traffic from specific WAN-side ports to specified LAN-side IP addresses and port numbers. → 8.6.16 Static NAPT (Port Forwarding)
	DMZ Host	Fowards all incoming access to a specified IP address on the LAN. → 8.6.17 DMZ Host
	VoIP Port Dynamic Setting	Automatically changes the built-in router settings to handle NAPT traversal for protocols such as SIP. → 8.6.18 VoIP Port Dynamic Setting

8.6.2 WAN Connection

Feature		Description & Reference
Pass Through	IPsec Pass-through	Allows IPsec protocol packets to/from a specified device on the LAN to pass across the WAN–LAN boundary. → 8.6.19 IPsec Pass-through
	PPTP Pass-through	Allows PPTP protocol packets to/from a specified device on the LAN to pass across the WAN–LAN boundary. → 8.6.20 PPTP Pass-through
	L2TP Pass-through	Allows L2TP protocol packets to/from a specified device on the LAN to pass across the WAN–LAN boundary. → 8.6.21 L2TP Pass-through
Quality of Service (QoS)		Quality of Service settings offered by the built-in router. → 8.6.22 Quality of Service (QoS)
VPN	IPsec	VPN connection over IPsec. → 8.6.23 VPN—IPsec
	VPN Simple Settings	Provides simple VPN connectivity. → 5.4.1 Easy Setup Wizard → 8.6.24 VPN—VPSS Setting
Router Command		Displays the built-in router's status. → 8.6.25 Router Command
WAN Port Mirroring		Mirrors traffic from the WAN interface onto the MNT port. → 8.6.26 WAN Port Mirroring

Conditions

- This PBX supports only IPv4. It does not support IPv6. However, the IPv6 Bridge feature is supported. For details, refer to 8.6.6 Protocol Bridge—IPv6 Bridge.
- KX-NSN101 (Built-in Router) is required to use all the features in this section. This activation key is required at each site where the built-in router will be used.

8.6.2 WAN Connection

Description

The following protocols are supported for setting the IP address of the WAN interface.

Protocol	Description
IPoE	Sets a static IP address or retrieves an IP address dynamically from a DHCP server using the DHCP client feature.
PPPoE	Obtains an IP address dynamically from a PPPoE server.

You can confirm the current connection status of the WAN interface in Web Maintenance Console. Also, malfunctions in the WAN connection session (router malfunctions) are indicated by the status LED on the PBX itself.

Malfunction	Status LED
WAN connection session malfunction (router malfunction)	Red Flashing

- You can set 1 IP address for the WAN interface.
You can manually change the IP address of the WAN interface, the protocol for obtaining the IP address, and any necessary parameters that were configured in the Easy Setup Wizard when the PBX was initially set up.
- Selecting **Disable** as the connection mode for the built-in router disables it.

Conditions

- Only a single session is available for PPPoE.
- If the protocol for setting the IP address is changed, you must perform a System Reset and restart the PBX before the setting can be applied.
- When the built-in router is active, it serves as the default gateway on the LAN-side of the network. The gateway address distributed by the DHCP feature will be changed to the LAN port's IP address.
- For details about what values to use for configuring the protocol for specifying an IP address, consult the network administrator.
- This PBX supports the PPPoE protocol in conformance with RFCs 1332, 1334, 1661, 1877, 1994, and 2516.
- The WAN IP address of the router must be a global address, and the WAN IP address of the Master unit must be a fixed address. If you need to change the WAN IP address of the Master unit, change the Master unit IP address setting at the Slave units first, and then change the WAN IP address of the Master unit. Otherwise, you will lose One-look network functionality.

PC Programming Manual References

- 27.1 Router Configuration—Setup—[1-1] Router Information
27.2.1 Router Configuration—Setup—[1-2-1] WAN—Connection Settings

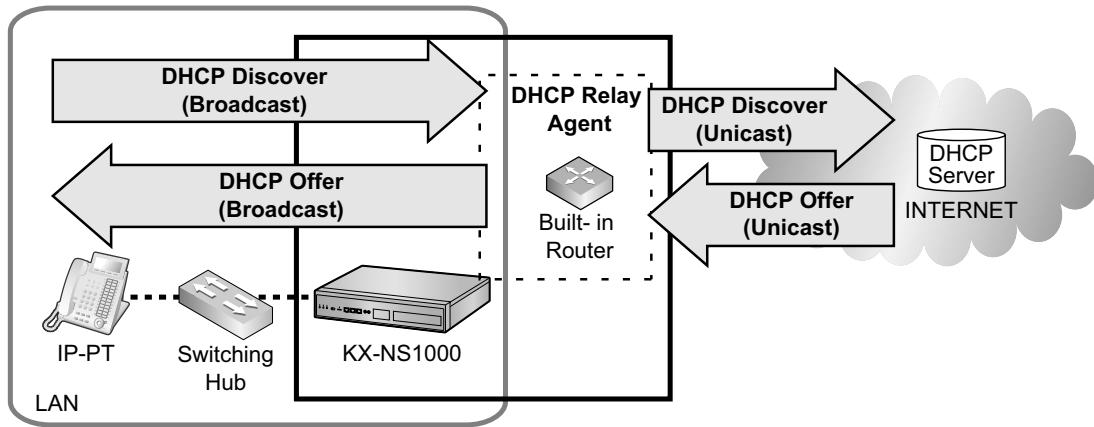
8.6.3 DHCP Relay Agent

Description

The built-in router relays DHCP messages to a specified server. DHCP messages (e.g., DHCP discover) broadcast within a network segment are sent and received as unicast messages with the DHCP server set as the relay destination.

8.6.4 Dynamic DNS

You can enable/disable the DHCP relay agent and specify the relay destination DHCP server.



Conditions

- This PBX supports RFC 1542 (Clarifications and Extensions for the Bootstrap Protocol).
- To enable sending multicast packets on the WAN side, the DHCP relay agent feature can be used only when the built-in router feature is enabled.
- When the built-in router feature is enabled, the PBX must act as the network gateway for the LAN. Therefore, the default gateway address that the DHCP server distributes is changed to the IP address of the PBX's LAN port.
- This feature cannot be configured if the method for acquiring IP addresses on the LAN side is DHCP mode.

PC Programming Manual References

28.2.1 Network Service—[2-1] Server Feature—DHCP

8.6.4 Dynamic DNS

Description

If the PBX's WAN-side IP address is assigned dynamically, the PBX can notify the DNS server of its current IP address. Since the PBX updates its DNS record each time it connects to the network, other devices can always connect to the PBX using the same hostname, even if the PBX's WAN-side IP address changes each time the PBX reconnects to the network.

You can enable/disable the Dynamic DNS feature and specify the dynamic DNS server.

Conditions

- The Dynamic DNS feature differs from the dynamic DNS defined in RFC 2136. It uses HTTP to update the DNS record. The update method differs depending on the DNS server operator. Although some operators may support FTP or e-mail for updating the DNS record, this PBX only supports HTTP.
- The KX-NS1000 supports only type A records.
- For details about what values to use for the DNS server settings, consult the network administrator.

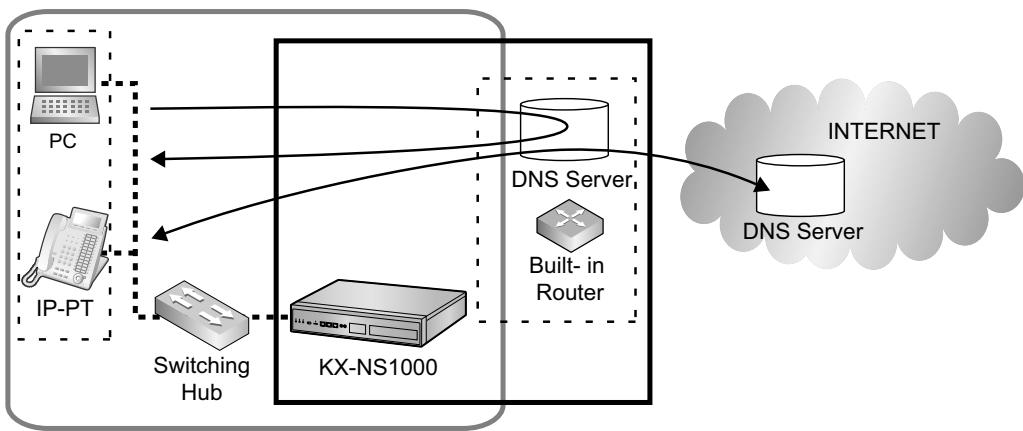
PC Programming Manual References

27.2.4 Router Configuration—Setup—[1-2-4] WAN—Dynamic DNS

8.6.5 DNS Client

Description

When a device on the LAN requests a domain name resolution, the DNS client queries an outside DNS server and then forwards the results to the requesting device. With this feature, devices on the LAN can convert domain names into IP addresses, and determine what domain name is associated with an IP address. Once a domain name has been resolved, this information is temporarily stored in a local cache. If a query is made for the same information, the PBX responds with the information stored in its cache.



Conditions

- A primary and secondary DNS server can be specified in the WAN-side network settings. The PBX will query the primary DNS server first. If that query fails, the PBX queries the secondary server.
- For details about what values to use for the DNS client settings, consult the network administrator.
- When the built-in router is enabled, it is not possible to access a DNS server at a different site over a VLAN. Since communication over a VPN will not be possible, do not set a destination IP address in the VPN for the following settings:
 - 27.2.1 Router Configuration—Setup—[1-2-1] WAN—Connection Settings
 - ◆ Preferred DNS IP Address
 - ◆ Alternative DNS IP Address
 - 28.1 Network Service—[1] IP Address/Ports
 - ◆ DNS Setting—Preferred DNS IP Address
 - ◆ DNS Setting—Alternative DNS IP Address

Either set up a DNS server at each site, or specify a DNS server on the WAN side.

PC Programming Manual References

9.11 PBX Configuration—[1-1] Configuration—Slot—V-SIPGW—Port Property—Main—★ SIP Server Name
 9.11 PBX Configuration—[1-1] Configuration—Slot—V-SIPGW—Port Property—Register—★ Registrar Server Name
 9.11 PBX Configuration—[1-1] Configuration—Slot—V-SIPGW—Port Property—NAT—★ STUN Server—Name

8.6.7 Protocol Bridge—PPPoE Bridge

- 27.2.1 Router Configuration—Setup—[1-2-1] WAN—Connection Settings—Static IP
 - ◆ Preferred DNS IP Address
 - ◆ Alternative DNS IP Address
- 27.2.1 Router Configuration—Setup—[1-2-1] WAN—Connection Settings—DHCP
 - ◆ Preferred DNS IP Address
 - ◆ Alternative DNS IP Address
- 27.2.1 Router Configuration—Setup—[1-2-1] WAN—Connection Settings—PPPoE
 - ◆ Preferred DNS IP Address
 - ◆ Alternative DNS IP Address
- 27.3.2 Router Configuration—Setup—[1-3-2] LAN—DNS Server
- 28.1 Network Service—[1] IP Address/Ports—◆ DNS Setting—Preferred DNS IP Address
- 28.1 Network Service—[1] IP Address/Ports—◆ DNS Setting—Alternative DNS IP Address
- 28.2.5 Network Service—[2-6] Server Feature—SMTP—◆ SMTP server for relay—SMTP server address
- 28.3.1 Network Service—[3-1] Client Feature—FTP—◆ Name
- 28.3.2 Network Service—[3-2] Client Feature—Syslog—◆ Remote Syslog server—IP address / Host name
- 28.3.3 Network Service—[3-3] Client Feature—SNMP Agent—SNMP Manager #1 / SNMP Manager #2—◆ Host name
- 28.4.2 Network Service—[4-2] Other—NAS—◆ NAS Setting—NAS Address—Name

8.6.6 Protocol Bridge—IPv6 Bridge

Feature

Use this feature if a device on the LAN uses IPv6 to communicate directly with a device on the WAN also using IPv6. This feature allows an IPv6 frame (protocol number: 0x86dd) to bridge the WAN–LAN boundary. If IPv6 is disabled, it is still possible to use the PBX to provide IPv6 services to users.

You can enable/disable the IPv6 Bridge feature.

Conditions

- For details about devices that are compatible with IPv6 Bridge, consult the network administrator.

PC Programming Manual References

- 27.2.3 Router Configuration—Setup—[1-2-3] WAN—Protocol Bridge

8.6.7 Protocol Bridge—PPPoE Bridge

Description

This feature is used when a PPPoE client device on the LAN wants to establish a separate PPPoE session. Even if the PPPoE Bridge feature is enabled, a PPPoE frame received on the WAN interface of the PBX will be processed by the PBX without being bridged. This feature allows PPPoE frames (protocol numbers 0x8863 and 0x8864) to bridge the WAN–LAN boundary.

You can enable/disable the PPPoE Bridge feature.

Conditions

- PPPoE frames (protocol numbers 0x8863 and 0x8864) are bridged according to the following conditions:
 - If PPPoE Bridge is enabled
PPPoE frames from the WAN side addressed to the PBX are processed by the PBX.

(Normally, PPPoE frames from the LAN side are not addressed to the PBX. PPPoE frames addressed to a device other than the PBX are bridged (both WAN → LAN and LAN → WAN)).

- If PPPoE Bridge is disabled
PPPoE frames are not bridged.
- For details about devices that are compatible with PPPoE Bridge, consult the network administrator.

PC Programming Manual References

27.2.3 Router Configuration—Setup—[1-2-3] WAN—Protocol Bridge

8.6.8 MAC Address Clone

Description

This feature allows the MAC address of the WAN interface to be changed. If this feature is disabled, the factory-set MAC address is used. If this feature is enabled, you can specify a MAC address manually.

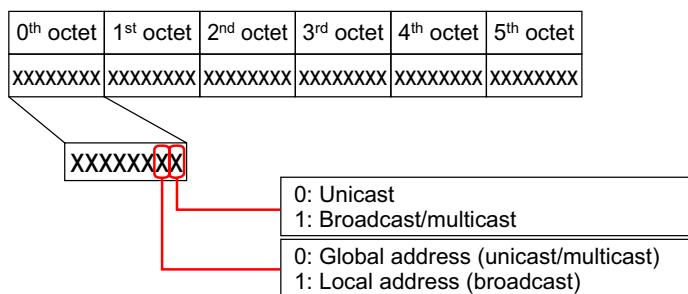
Note

Some ISPs register the MAC address of the PC used for initial setup for connecting to the internet. In this case, if you install a new router, the MAC address will be different from the one used in the initial setup with the ISP and the connection may be rejected.

Although you may be able to have the ISP update the registered MAC address, the MAC Address Clone feature is provided so you can avoid this time-consuming process.

Conditions

- The following types of MAC addresses cannot be set:
 - An address that violates the MAC address format
 - An address whose 0th bit in the first octet is 1 (broadcast/multicast MAC)



- An address already being used in the PBX (LAN interface, MNT interface, DSP, etc.)
- The same MAC address as another device on the same LAN segment
- This feature is applied only once when the system is started. To reflect any changes to the MAC address, the PBX must be restarted.
- For details about what MAC addresses you can use, consult the network administrator.

PC Programming Manual References

27.6 Router Configuration—Setup—[1-6] MAC Address

8.6.9 Routing

Description

The built-in router supports routing over the WAN–LAN boundary using IPv4. This PBX supports static routing only. It does not support dynamic routing through RIP (Routing Information Protocol).

Static Routing

- Up to 64 entries can be entered.
- To determine how packets are routed, a static routing destination can be specified for each entry.
- You can specify either "next hop (gateway address)" or "PPPoE session ID" for the routing destination.
- You can specify the default route (the route specified packets that do not match the routing information).
- You can specify the distance for each entry.

Dynamic Routing

- Not supported.

Conditions

- This feature conforms to RFC 1812: Requirements for IP Version 4 Routers.
- For details about routing rules, consult the network administrator.

PC Programming Manual References

27.4 Router Configuration—Setup—[1-4] Routing

8.6.10 Firewall

Description

The built-in router includes a firewall for inspecting packets at the WAN–LAN boundary and rejecting unauthorised packets. The firewall can also sense unauthorised access and DoS attacks and take appropriate measures. This feature applies only to packets routed via IP.

This feature does not apply to data routed through a tunnel, such as with IPsec.

Conditions

- **Filter priority**

If multiple security settings are enabled, such as Packet Filtering, SPI, and DoS Protection, some filter settings may conflict with one another. To avoid this, the following priorities are applied to the filters. In the table, priority 1 has the highest priority, and priority 13 has the lowest priority.

Priority	Security rule	Destination			
		KX-NS1000 to WAN	WAN to KX-NS1000	WAN to LAN	LAN to WAN
1	DoS Protection	–	✓	✓	✓
2	Stateful Packet Inspection Drop	–	✓	✓	✓
3	IPv4 Packet Filtering (Filter) ¹	✓	✓	✓	✓
4	Automatic filtering system reservation port ²	✓	✓	✓	✓

Priority	Security rule	Destination			
		KX-NS1000 to WAN	WAN to KX-NS1000	WAN to LAN	LAN to WAN
5	VoIP Port Dynamic Settings	—	—	✓	✓
6	NET BIOS Packet Filtering	—	—	—	—
7	Private IP Address Filtering	—	✓	✓	✓
8	ICMP Echo Request Packet Filtering	—	✓	—	—
9	Stateful Packet Inspection Accept	—	—	✓	✓
10	Port Forward	—	—	✓	✓
11	Pass Through	—	—	✓	✓
12	DMZ Host	—	—	✓	✓
13	IPv4 Packet Filtering (LAN->WAN Basic Policy) (WAN->LAN Basic Policy)	✓	✓	✓	✓

✓: Applicable for prioritising

—: Not applicable

¹ Setting the IPv4 Packet Filtering (Filter) to allow full access, may leave your system open to network attacks. Consider this carefully before configuring this setting.

² Depending on system operation, specific ports can be set to allow or disallow network traffic. For details, consult the system administrator.

- For details about the security policy for the built-in router, consult the network administrator.

8.6.11 Firewall—Packet Filtering

Description

This feature filters IPv4 packets (e.g., user IP data and IP data addressed to the PBX). You can configure the LAN → WAN basic policy and WAN → LAN basic policy, which are system wide.

You can also configure filter settings for each entry. If the system-wide and entry-specific settings conflict, the entry filter is prioritised.

LAN → WAN Basic Policy, WAN → LAN Basic Policy

- Defines the basic policy for IPv4 packets travelling from the LAN to the WAN (allow/deny). This policy applies to the entire system. If you select "deny", all packets travelling from the LAN to the WAN will be discarded.
- Defines the basic policy for IPv4 packets travelling from the WAN to the LAN (allow/deny). This policy applies to the entire system. If you select "deny", all packets travelling from the WAN to the LAN will be discarded. This policy applies to packets addressed to the PBX itself.

Filter

- You can configure up to 64 entries. For each entry, you can specify whether it is enabled or disabled.
- Filter rules are prioritised by entry order.
- The following table shows which settings can be configured for a filter rule.

8.6.13 Firewall—DoS Protection

Setting	Description
Protocol number	Specify a protocol number directly (0–255) Specify a protocol type (ICMP, TCP, UDP, TCP&UDP)
Originating IP address	By specifying a subnet, you can apply the filter to a range of addresses.
Destination IP address	By specifying a subnet, you can apply the filter to a range of addresses.
TCP/UDP originating port	You can specify a range.
TCP/UDP destination port	You can specify a range.
Direction	LAN->WAN, WAN->LAN
Operation	Allow/Deny
Log	Record in log or do not record in log

PC Programming Manual References

27.8 Router Configuration—Firewall—[2-2] Packet Filtering

8.6.12 Firewall—Stateful Packet Inspection

Description

Stateful Packet Inspection (SPI) is a feature where the firewall inspects the contents of a packet and determines dynamically whether to allow or deny the packet. If SPI is enabled, packets determined to be "INVALID" (packets that do not apply to any other state) are denied. On this PBX, SPI applies to both incoming (WAN → LAN) and outgoing (LAN → WAN).

Using the following "TCP flag state" as the detection criteria, packets that do not match the TCP state change are discarded by the SPI feature.

This feature remembers each transmission state, and by predicting the next packet that will arrive, it can detect unauthorised access and discard packets accordingly.

PC Programming Manual References

27.7 Router Configuration—Firewall—[2-1] One Touch Security

8.6.13 Firewall—DoS Protection

Description

The DoS Protection feature protects the system against DoS (Denial of Service) attacks. Security rules for protecting against port scans and DoS attacks can be set with one touch.
You can enable and disable DoS Protection.

Conditions

- For details about whether the DoS Protection feature is necessary, consult the network administrator.

PC Programming Manual References

27.7 Router Configuration—Firewall—[2-1] One Touch Security

8.6.14 Firewall—Other Security Settings

Description

The following additional filtering settings are available.

Other Security Settings	Description
Private IP Address Filtering	Block private IP addresses
ICMP Echo Request Packet Filtering	Block ICMP echo requests
ICMP Redirect Settings	Settings for sending and receiving ICMP redirect packets.
NET BIOS Packet Filtering	Block external sharing packets from NetBIOS.

Private IP Address Filtering

- This setting is a filter for private IP addresses. It blocks private IP addresses in both directions.
- If the WAN interface is connected to an edge, communication using the WAN's private IP addresses is not allowed. Therefore, if this feature is enabled, the following types of packets will be discarded.
 1. Packets travelling from the LAN to the WAN whose destination IP address is a private IP address
 2. Packets travelling from the WAN to the LAN whose source IP address is a private IP address
 However, if the WAN interface's IP address is a private IP address, this feature will be automatically disabled. Also, communication over an IPsec VPN is exempt from this filter.

ICMP Echo Request Packet Filtering

- This setting determines whether the PBX responds to ICMP echo requests on either the WAN interface or LAN interface.

ICMP Redirect Settings

- Depending on the settings, the PBX will send ICMP redirect packets and notify the sender of changes to the route.
- Depending on the settings, the PBX will receive ICMP redirect packets and will update its routing table based on the content of the received packet.

NET BIOS Packet Filtering

- This setting filters packets so that Windows services such as DCE and RPC, NetBIOS, Direct Hosting, SMB, etc., are limited to the LAN and do not travel onto the WAN.
 In particular, it is necessary to filter RPC packets, since several vulnerabilities have been found in the Windows RPC interface.
- By using a filter rule to discard packets for these ports travelling from the LAN to the WAN, traffic for external Windows sharing features (NetBIOS) will be blocked.

Conditions

- For details about which security settings should be enabled, consult the network administrator.

PC Programming Manual References

27.7 Router Configuration—Firewall—[2-1] One Touch Security

8.6.15 Dynamic NAPT (IP masquerade)

Description

This feature dynamically changes the address and port of packets accessing the WAN from the LAN. This makes it possible for multiple devices to connect to the outside. You can enable and disable this feature for each built-in router.

Note

The PBX must remember the mapping of IP addresses and ports for packets leaving the LAN. Therefore, it is not possible to directly access a LAN-side device from the WAN side. This acts as a security measure, preventing unauthorised access from outside the LAN.

Conditions

- This PBX supports only dynamic NAPT (IP masquerade). It does not support dynamic NAT.
- Protocols that can use this feature are: TCP(6), UDP(17), and ICMP (1). For ICMP, the ICMP query ID is changed instead of the port number.
- If the router is being used as an edge router, the dynamic NAPT feature will be enabled. If the router is being used as a local router, the dynamic NAPT feature will be disabled.
- Conforming RFCs
 - RFC 1631: The IP Network Address Translator (NAT)
 - RFC 2391: Load Sharing using IP Network Address Translation (LSNAT)

PC Programming Manual References

27.3.1 Router Configuration—Setup—[1-3-1] LAN—IPv4

8.6.16 Static NAPT (Port Forwarding)

Description

By mapping a specific port on the WAN side (for example 80 for HTTP) to a device on the LAN side (IP address and port), packets that arrive on the WAN side at the specified port can be forwarded to the device. The static NAPT (port forwarding) feature can be enabled and disabled for each built-in router.

Conditions

- This PBX supports only static NAPT (port mapping/static IP masquerade). It does not support static NAT.
- A maximum of 64 entries can be registered.
- Protocols that can use this feature are: TCP(6), UDP(17), and ICMP (1).
- You can set a range of ports using the condition that the WAN-side port number and LAN-side port number be the same number.
- A maximum of 4096 sessions can be managed. This session number includes dynamic NAPT settings.
- Conforming RFCs:
 - RFC 1631: The IP Network Address Translator (NAT)
 - RFC 2391: Load Sharing using IP Network Address Translation (LSNAT)

PC Programming Manual References

27.3.1 Router Configuration—Setup—[1-3-1] LAN—IPv4

8.6.17 DMZ Host

Description

This PBX supports the DMZ (De-Militarised Zone) Host (or simply DMZ) function, but not the strictly defined DMZ function. It will forward all incoming access to a specified IP address on the LAN.

The DMZ is a segment on the network protected by a firewall. It prevents unauthorised access from the internet and keeps threats from proliferating within the internal network.

Packets addressed to the PBX's WAN-side IP address are forwarded to the LAN-side device specified as the DMZ host. However, traffic that accesses previously used ports will be handled by the appropriate application. Only 1 device can be specified as the DMZ host.

Note

If the DMZ host feature is enabled, the DMZ host device and other devices on the LAN are on the same network segment, which can pose a security risk.

PC Programming Manual References

27.5 Router Configuration—Setup—[1-5] DMZ

8.6.18 VoIP Port Dynamic Setting

Description

This feature allows NAPT settings to be configured automatically for communication protocols that require NAT traversal settings (e.g., SIP). These protocols are used by devices such as SIP phones and IP-PTs.

When using protocols like SIP that require NAT traversal, the necessary parameters, such as the RTP port number and the port number for the protocol in use, are configured automatically.

Conditions

- When an extension is connected to an outside destination using P2P and the parties are directly exchanging RTP packets, this feature is applicable only to SIP trunks.
- When the built-in router is enabled, all communication over IP trunks and remote extensions will be directed to the WAN interface of the built-in router. To direct communication to an external router, you must set the applicable address and routing information to divert communication to the PBX LAN interface.
- When the KX-NS1000 is the RTP terminal**

Specify the port range for RTP to a port range that is not applicable to the dynamic NAPT feature. By doing so, the port numbers of RTP packets sent from the LAN are not changed by dynamic NAPT, and RTP packets can use the port number negotiated by SIP.

The RTP port number is different from the ports set in the static NAPT settings, and the port will be opened for the first time when an RTP packet is sent from the LAN, so it is secure. However, the port will be opened only when a packet is sent from the LAN, so any WAN traffic received at the port before it is opened will be discarded.

When the built-in router is used as an edge router and dynamic NAPT is enabled, this feature operates associating the DSP's IP address and the RTP port range settings.

- When an extension is the RTP terminal (P2P)**

With RTP/RTCP communication, NAT traversal problems will arise when performing voice communication via P2P. Therefore, the PBX will automatically configure the NAPT settings for RTP and RTCP as necessary from the SDP information.

Installation Manual References

- 5.9.3 Installing SIP Phones at a Remote Site
- 5.9.4 Installing IP Phones at a Remote Site with a Built-in Media Relay Gateway

Feature Guide References

- 5.2.3 Peer-to-Peer (P2P) Connection

8.6.19 IPsec Pass-through

Description

For VPN packets that use IPsec and are sent and received from a specified device on the LAN, you can configure settings so that (1) the port number is not changed when these packets are sent and received and (2) these packets are allowed to cross the LAN–WAN boundary uninhibited.

Only 1 device on the LAN can be designated as the IPsec pass-through device.

Setting	Description
Application	IPsec
Protocol/Protocol number	ESP ^{*1} / 50
Port number	UDP/500: ISAKMP ^{*2} UDP/4500: NAT-T ^{*3}

A VPN that uses IPsec is a tunnelling protocol, so the send/receive port number for packets additionally indicates which tunnelling protocol the packets are using. If the port number is changed by the dynamic NAPT (IP masquerade) feature, the information that indicates the tunnelling protocol will be lost, and end-to-end communication will be impossible.

To allow end-to-end communication, specified packets from a specified device are allowed to pass through the WAN–LAN boundary without having their port number changed.

Conditions

- The IPsec pass-through feature cannot be used together with the PBX's IPsec feature or the VPSS feature. This is because when IPsec packets pass through to the LAN, they cannot be distinguished from VPN (IPsec) packets for the KX-NS1000.
- Communication across the WAN–LAN boundary is subject to the following conditions:
 - IKE^{*4} must be able to be initiated from the WAN side.
 - The first ESP^{*1} packet must be able to be sent from either the LAN side or the WAN side.

^{*1} ESP: Encapsulating Security Payload

^{*2} ISAKMP: Internet Security Association Key Management Protocol

^{*3} NAT-T: NAT Traversal

^{*4} IKE: Internet Key Exchange

PC Programming Manual References

- 27.11 Router Configuration—VPN—[3-3] Pass Through

8.6.20 PPTP Pass-through

Description

For VPN packets that use PPTP and are sent and received from a specified device on the LAN, you can configure settings so that (1) the port number is not changed when these packets are sent and received and (2) these packets are allowed to cross the LAN–WAN boundary uninhibited.

Only 1 device on the LAN can be designated as the PPTP pass-through device (acting as either a server or a client).

Setting	Description
Application	PPTP
Protocol/Protocol number	GRE ¹ / 47
Port number	TCP/1723: PPTP

A VPN that uses PPTP is a tunnelling protocol, so the send/receive port number for packets additionally indicates which tunnelling protocol the packets are using. If the port number is changed by the dynamic NAPT (IP masquerade) feature, the information that indicates the tunnelling protocol will be lost, and end-to-end communication will be impossible.

To allow end-to-end communication, specified packets from a specified device are allowed to pass through the WAN–LAN boundary without having their port number changed.

Conditions

- Communication across the WAN–LAN boundary is subject to the following conditions:
 - One server–client pair is limited to 1 session.
 - A PPTP-controlled connection can be established from either the LAN side or the WAN side.
 - The GRE¹ tunnel's first packet can be sent from either the LAN side or the WAN side.
 - You must set the LAN-side client's IP address.

¹ GRE: Generic Route Encapsulation

PC Programming Manual References

27.11 Router Configuration—VPN—[3-3] Pass Through

8.6.21 L2TP Pass-through

Description

For VPN packets that use L2TP (Layer 2 Tunnelling Protocol) and are sent and received from a specified device on the LAN, you can configure settings so that (1) the port number is not changed when these packets are sent and received and (2) these packets are allowed to cross the LAN–WAN boundary uninhibited.

Only 1 device on the LAN can be designated as the L2TP pass-through device (LENS¹).

Setting	Description
Application	L2TP
Protocol/Protocol number	—
Port number	UDP/1701: L2TP

8.6.22 Quality of Service (QoS)

L2TP is a tunnelling protocol for layer 2 (data link layer) of the OSI model. The send/receive port number for packets additionally indicates which tunnelling protocol the packets are using.

If the port number is changed by the dynamic NAPT (IP masquerade) feature, the information that indicates the tunnelling protocol will be lost, and end-to-end communication will be impossible.

To allow end-to-end communication, specified packets from a specified device are allowed to pass through the WAN–LAN boundary without having their port number changed.

Conditions

- Communication across the WAN–LAN boundary is subject to the following conditions.
 - Access from a LAC² on the LAN side to the LENS¹ on the WAN side:
 - Operate according to the dynamic NAPT settings
 - Access from a LAC² on the WAN side to the LENS¹ on the LAN side:
 - Only 1 LENS¹ can be installed on the LAN side.
 - The L2TP tunnel is established from the WAN side.
 - The L2TP tunnel's first packet can be sent from either the LAN side or the WAN side.
 - You must set the LAN-side LENS's IP address.

¹ LENS: L2TP Network Server

² LAC: L2TP Access Concentrator

PC Programming Manual References

27.11 Router Configuration—VPN—[3-3] Pass Through

8.6.22 Quality of Service (QoS)

Description

This PBX supports the following QoS (Quality of Service) mechanisms.

You can enable and disable the QoS feature and configure the specific QoS settings.

Setting	Description
QoS Service	Priority control
Auto QoS VoIP	Automatically prioritise VoIP packets (SIP, H.323, MGCP, RTP)
Upstream Bandwidth	Set a limit on the number of frames sent of a specified type

If the WAN line is narrow, sending packets at the link up-speed can cause overflow at the exit point (modem, etc.) and result in packet loss. To avoid this, the sending bandwidth should be restricted to match the speed of the WAN line.

This, combined with priority control can allow efficient communication.

Conditions

- Only PQ¹ is supported for priority control. WRR² and SP³+WRR⁴ are not supported.

- For bandwidth control, the PBX supports setting an upper limit on the number of frames sent of a specified type. However, a bandwidth guarantee, where the number of frames of a specified type is guaranteed to be sent, is not supported.

¹ PQ: Priority Queuing

² WRR: Weighted Round Robin

³ SP: Strict Priority

⁴ WFQ: Weighted Fair Queuing

PC Programming Manual References

27.12 Router Configuration—QoS Settings—[4] QoS Service

8.6.23 VPN—IPsec

Description

There are 2 VPN communication modes: transport mode and tunnel mode.

Transport Mode

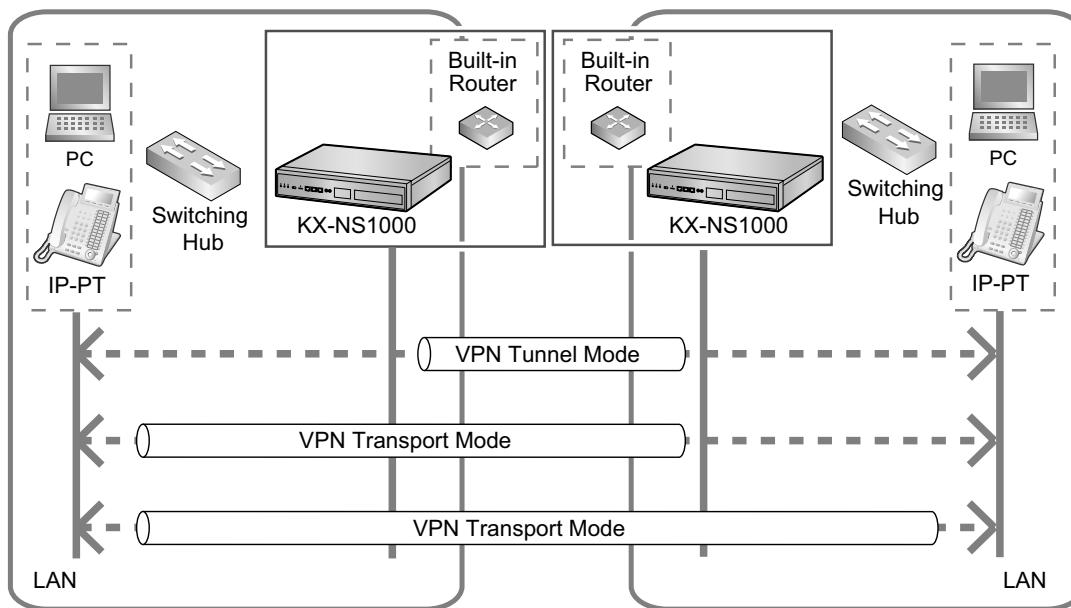
This mode is used when IPsec is applied between hosts or between a host and site. It is useful for remote access. In this mode, the host itself encrypts the packet before sending it.

Tunnel Mode

This mode is used when IPsec is applied between sites.

In this mode, an SA (Security Association) is created between devices (called secure gateways) that support IPsec. Data from other clients connected to these devices is encrypted and sent. A host's data is encrypted by a security gateway and sent to the corresponding security gateway.

The receiving security gateway decrypts the data and sends it to the destination host.



VPN connection procedure overview

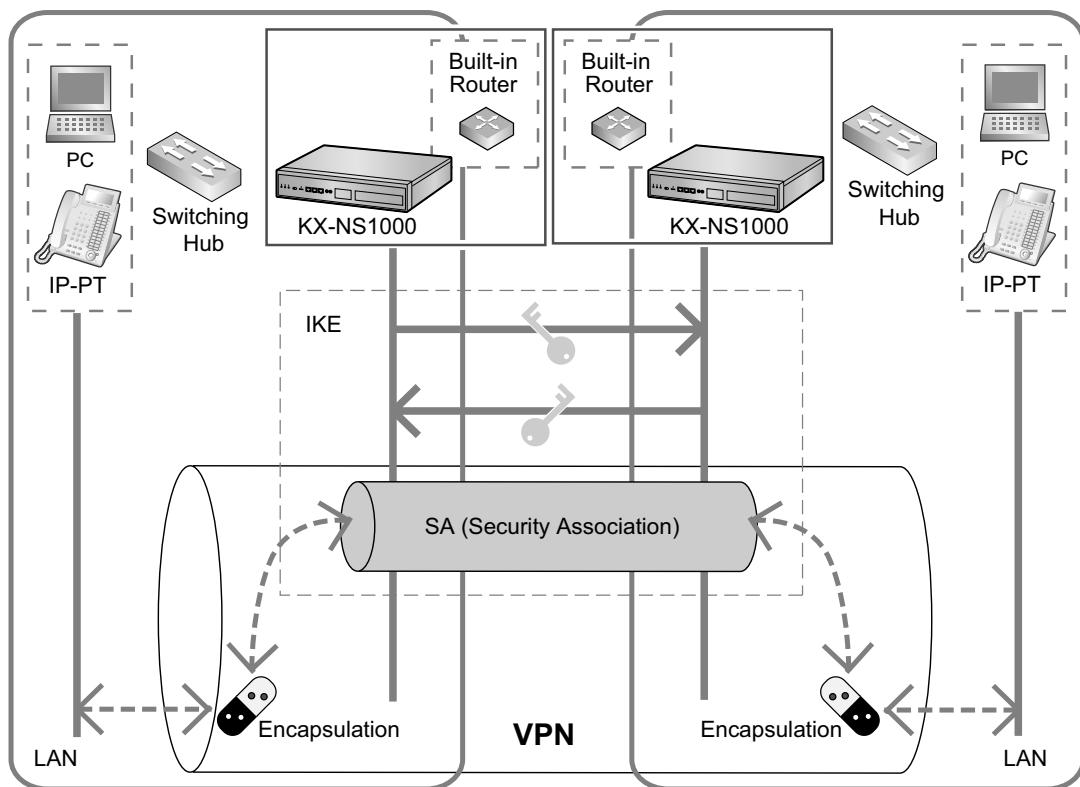
1. Establish a security association (SA)

An SA refers to the agreed upon results of encryption key exchange and encryption method negotiated by the devices that will communicate over a VPN.

From this process, a secure communication channel is established. An SA is automatically constructed using the IKE (Internet Key Exchange) protocol (although depending on the settings, the SA can be established manually).

2. After an SA is established, encapsulate packets and transmit them securely.

Example: Establishing a VPN in transport mode



Features

The following settings are available to modify establishing a VPN connection over IPsec.

Setting	Description
IKE Settings	IKE (Internet Key Exchange) settings
Security	Security settings for SA
ISAKMP SA	ISAKMP (Internet Security Association Key Management Protocol) settings for SA
IKE Proposal	Settings for the PBX's IKE proposal. VPN negotiations are performed according to these settings.
IPsec SA	IPsec settings for SA
IPsec Proposal	Settings for the PBX's IPsec proposal. VPN negotiations are performed according to these settings.
Optional Function	Settings for other optional functions, such as XAUTH authentication mode settings.

Conditions

- IPsec (VPN) connection using a non-Panasonic router is not guaranteed.
- KX-NSN216 (16-channel IPsec Activation Key) is required to use this feature.
- This PBX supports only IKE version 1.
- This PBX supports only IPsec version 2.
- IPsec NAT Traversal, Mode Config (IKE-CFG), IPsec DHCP are not supported.
- Since it is assumed the VPN will be used for remote access, this PBX supports XAUTH.
- This PBX supports the following packet encapsulation protocols:
 - Authentication Header (AH)
 - Encapsulating Security Payload (ESP)
- The maximum number of VPNs that can be established between sites on a One-look network and between KX-NS1000 PBXs and Android/iOS devices is shown in the following table:

Connecting Device	Maximum Number of VPN Connections
KX-NS1000	16 sites (VPN connections with 15 sites)
Android (4.0 or later) / iOS 6.0 or later	32 devices (VPN connections with 32 devices)

- IKE standard reference: RFC 2401–2409, 4109
- For each established SA, the number of IPsec connections enabled by the activation key decrements by 1. When the number reaches 0, no more SAs can be established.
- The necessary activation key for an IPsec connection must be enabled.
- The following authentication methods are supported for connection with an Android™ (version 4.0 or later) or iOS device:

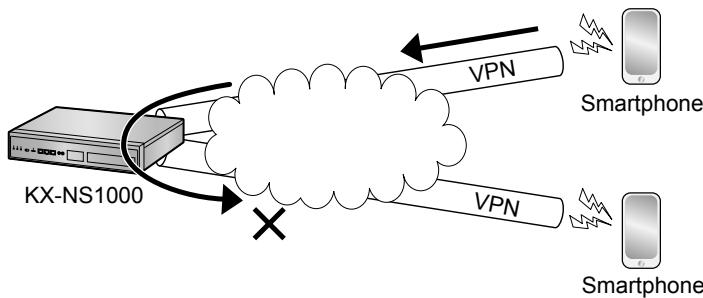
Authentication method	Description
IPsec XAUTH PSK	Method based on X Window authentication using a pre-shared encryption key
IPsec XAUTH RSA	Method based on X Window authentication using an RSA encryption key

- You can confirm the current VPN connection status in Web Maintenance Console.
- If a smartphone is connected to the PBX via a VPN using the built-in router, a global IP address must be provided by the carrier. Smartphones cannot be used without a global IP address.
- When you connect IP devices such as smartphones to the PBX via a VPN using the built-in router, the connected device must be registered to the PBX that is providing the VPN connection.
- The PBX assigns a fixed IP address (10.99.99.xxx) to IP devices, such as smartphones, for the VPN connection. Please do not assign a 10.99.99.xxx IP address to other IP equipment connected to the PBX and the underlying the network because there is a possibility that IP addresses will overlap.
- The PBX may migrate to Backup Master mode or Isolated mode if the keep-alive timer between PBXs expires while connected to the VPN. To avoid this issue, adjust the value for the keep alive timer through PBX system programming. Refer to "9.4 PBX Configuration—[1-1] Configuration—Slot—System Property—Multisite—◆ Multisite Keepalive Time-out time" in the PC Programming Manual. If the system does not enter Backup Master mode or Isolated mode, please change the system mode to **Normal** via Web Maintenance Console.
- When you change the system mode from Backup Master mode to Normal mode, the Master unit and Backup Master unit must be connected via a VPN. You can confirm the VPN connection status via Web Maintenance Console. Refer to "27.1.3 Router Configuration—Setup—[1-1-3] Router Information—VPN Status" in the PC Programming Manual.

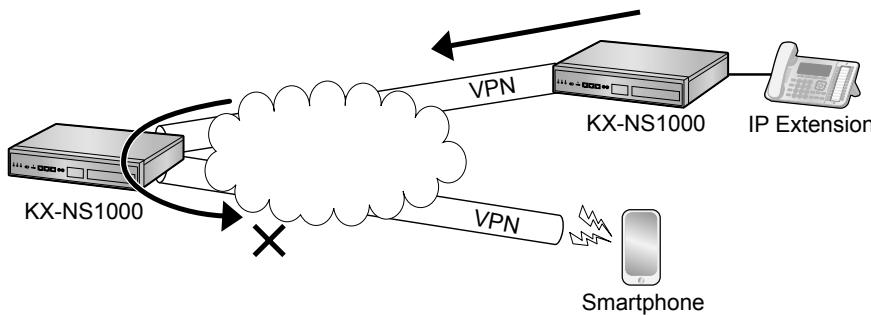
8.6.24 VPN—VPSS Setting

- If you change the router configuration (refer to "27.10 Router Configuration—VPN—[3-2] IPSec" in the PC Programming Manual), the affected unit's system must be restarted in order to rebuild the VPN connection. At that time, service will be temporarily unavailable.
- It is not possible to use VPN connections using the built-in router for P2P connection as shown in the following diagrams. In this case, separate P2P groups must be used (refer to "5.2.3 Peer-to-Peer (P2P) Connection" in the Feature Guide).

Example 1



Example 2



PC Programming Manual References

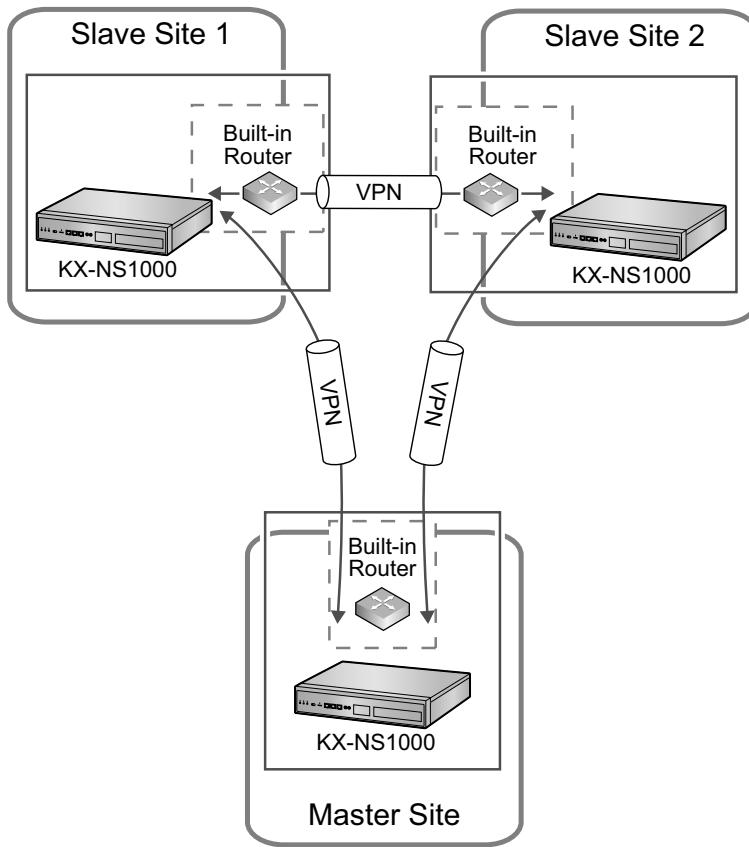
- 27.1.3 Router Configuration—Setup—[1-1-3] Router Information—VPN Status
27.10 Router Configuration—VPN—[3-2] IPSec

8.6.24 VPN—VPSS Setting

Description

The VPSS (VPN Simple Setting) feature allows you to automatically create a complex, full-mesh VPN. When constructing a multi-site system with KX-NS1000 PBXs, you can create a VPN with IPsec to ensure secure communication between sites, but with VPSS, a complex, full-mesh VPN can be created automatically, as shown in the following figure. This VPN between sites can be easily created and maintained.

The VPSS information path refers to the information path that makes VPSS possible. Information is encrypted with SSL, IPsec, etc., and exchanged securely.



Features

- VPN Simple Settings can be activated in the Easy Setup Wizard.
For details, refer to "5.4.1 Easy Setup Wizard" in the Installation Manual.
- The following settings relating to VPSS can be changed manually.

Setting	Description
VPSS	Enabling/disabling VPSS
Per-site settings	Specify a site number, and you can change whether VPSS is enabled or disabled, the Slave unit's name, and other detailed VPSS settings.

Conditions

- KX-NSN216 (16-channel IPsec Activation Key) is required to use this feature.
- To connect PBXs over a VPN, the Master unit and backup Master unit must both have static IP addresses.
- Users cannot use the VPSS function when more than one KX-NS1000 is on the same local network. In this type of configuration, the user must perform custom settings in whole or in part for a VPN connection.
- Local address subnets on the LAN side that overlap are not detected by VPSS.

8.6.26 WAN Port Mirroring

- When using VPSS, opposing subnets of KX-NS1000 PBXs are automatically configured. However, subnets created by subsequent external routers are not taken into account.
- In routing settings for crossing subnets, a maximum of 4 network addresses for adjacent segments, satellite offices, etc., can be configured for each site. These settings are configured in the VPSS Advanced Settings.

PC Programming Manual References

27.9 Router Configuration—VPN—[3-1] VPSS

8.6.25 Router Command

Description

You can enter router commands from Web Maintenance Console. You can reference the built-in router's settings in the commands' results.

The following commands are available.

Command	Description
ROUTE	Display the connected route information cache.
NETSTAT	Display the status for each interface.
ARP	Display the ARP table state.
DNSFLUSH	Clear the DNS cache.

Conditions

- Users with User (Admin) privileges or higher can access this feature.

PC Programming Manual References

7.8.2 Utility—Command—Router Command

8.6.26 WAN Port Mirroring

Description

This feature mirrors the contents of packets sent and received on the WAN interface on the MNT port. With WAN port mirroring, you can analyse the contents of packets that pass through the WAN port. You can enable/disable WAN port mirroring.

Conditions

- Users with User (Admin) privileges or higher can access this feature.

PC Programming Manual References

28.1 Network Service—[1] IP Address/Ports—Advanced Settings—◆ Port Mirroring—Packet kind for mirroring

Section 9

Appendix

This section provides information about PBX Region Suffix Codes and Areas, System Prompt Languages, and the revision history.

9.1 PBX Region Suffix Codes and Areas

According to the following table, select the appropriate Suffix Code and Area for your PBX to localise PBX settings to your location.

For KX-NS1000NE

Suffix Code	Area	Suffix Code	Area
G	Germany	CE	Poland
	Austria		Hungary
BL	Belgium		Czech
	Luxembourg		Slovakia
DK	Denmark		Romania
FI	Finland		Slovenia
FR	France		Croatia
JT	Italy		Yugoslavia
NL	Netherlands		Bosnia
NO	Norway		Lithuania
PT	Portugal		Latvia
SP	Spain		Estonia
SE	Sweden		Albania
SL	Switzerland		Bulgaria
TR	Turkey		Macedonia
GR	Greece		Other

For KX-NS1000XE

Suffix Code	Area
HK	Hong Kong
ML	Malaysia
SN	Singapore
TW	Taiwan
BX	Other

For KX-NS1000BX

Suffix Code	Area
SA	South Africa
BX	Other

For KX-NS1000AL

Suffix Code	Area
AL	Australia
NZ	New Zealand

9.2 System Prompt Languages

Note

- The following abbreviations are used in the language file names:
 - UK: United Kingdom
 - US: United States
 - LA: Latin America
 - CA: Canada
 - BR: Brazil
- No. 1 is set by default. For details, see "24.4 UM Configuration—[5-4] System Parameters—Parameters—Prompt Setting—Prompt Setting" in the PC Programming Manual.

System prompt languages stored in the Storage Memory Card (installed by default)

KX-NS1000 Suffix	NE	UK	AL	XE	BX
No. 1 (Primary)	UK-English	UK-English	UK-English	US-English	US-English
No. 2	Spanish	Spanish	-	LA-Spanish	LA-Spanish
No. 3	French	French	-	Mandarin	-
No. 4	German	German	-	Taiwan Mandarin	-
No. 5	Dutch	Dutch	-	Cantonese	-
No. 6	Italian	Italian	-	-	-
No. 7	Swedish	Swedish	-	-	-
No. 8	-	-	-	-	-

KX-NS1000 Suffix	AG	C	RU	UC	BR
No. 1 (Primary)	LA-Spanish	CA-English	Russian	Ukrainian	BR-Portuguese
No. 2	US-English	CA-French	Ukrainian	Russian	US-English
No. 3	-	-	US-English	US-English	-
No. 4	-	-	-	-	-
No. 5	-	-	-	-	-
No. 6	-	-	-	-	-
No. 7	-	-	-	-	-
No. 8	-	-	-	-	-

System prompt languages stored in optional Storage Memory Cards

KX-NS0135/ KX-NS0136/ KX-NS0137 Suffix	X
No. 1 (Primary)	UK-English
No. 2	German
No. 3	Spanish
No. 4	Italian
No. 5	Swedish
No. 6	Dutch
No. 7	CA-English
No. 8	CA-French

9.3 Revision History

9.3.1 PCMPR Software File Version 002.0xxxx

New Options

- Equipment Compatibility for KX-NS1000
 - KX-NS0130 Stacking Master Card (STACK-M)
 - KX-NS0131 Stacking Card for KX-NCP Series (STACK-S (NCP))
 - KX-NS0132 Stacking Card for KX-TDE Series (STACK-S (TDE))

New Contents

- 3.1.3 Using CTI Applications
- 4.6 Stacking Cards
- 5.9.3 Installing SIP Phones at a Remote Site
- 5.11 Programming E-mail Integration for UM Voice/Fax Messages
- 6.1 Information about Stacking PBXs
- 6.2 Methods of Stacking PBXs
- 8.4.2 One-look Networking Survivability

Changed Contents

- 2.1.1 System Configurations
- 2.1.2 System Connection Diagram
- 2.2.1 Optional Equipment
- 2.3.3 System Capacity
- 3.1.1 Type and Maximum Number of Activation Keys
- 4.2.1 Unpacking
- 4.2.7 Types of Connectors
- 4.3.1 Mother Board
- 5.2 PC Connection
- 5.3 Starting Web Maintenance Console
- 5.8.1 Assigning IP Addressing Information
- 7.1.1 Installation
- 7.1.6 Troubleshooting by Error Log
- 9.2 System Prompt Languages

9.3.2 PCMPR Software File Version 002.1xxxx

New Options

- Equipment Compatibility for KX-NS1000
 - KX-NS1020 Expansion Cabinet

New Contents

- 5.12 Automatic Configuration of Mailboxes

Changed Contents

- 2.1.1 System Configurations
- 2.3.3 System Capacity
- 3.1.1 Type and Maximum Number of Activation Keys
- 4.6.1 STACK-M Card (KX-NS0130)
- 5.3 Starting Web Maintenance Console
- 5.4.1 Easy Setup Wizard
- 5.9.3 Installing SIP Phones at a Remote Site

9.3.3 PCMPR Software File Version 003.0xxxx

New Contents

- 5.8.3 Setting LLDP Parameters
- 5.9.4 Installing IP Phones at a Remote Site with a Built-in Media Relay Gateway
- 8.6.1 Built-in Router Overview
- 8.6.2 WAN Connection
- 8.6.3 DHCP Relay Agent
- 8.6.4 Dynamic DNS
- 8.6.5 DNS Client
- 8.6.6 Protocol Bridge—IPv6 Bridge
- 8.6.7 Protocol Bridge—PPPoE Bridge
- 8.6.8 MAC Address Clone
- 8.6.9 Routing
- 8.6.10 Firewall
- 8.6.11 Firewall—Packet Filtering
- 8.6.12 Firewall—Stateful Packet Inspection
- 8.6.13 Firewall—DoS Protection
- 8.6.14 Firewall—Other Security Settings
- 8.6.15 Dynamic NAPT (IP masquerade)
- 8.6.16 Static NAPT (Port Forwarding)
- 8.6.17 DMZ Host
- 8.6.18 VoIP Port Dynamic Setting
- 8.6.19 IPsec Pass-through
- 8.6.20 PPTP Pass-through
- 8.6.21 L2TP Pass-through
- 8.6.22 Quality of Service (QoS)
- 8.6.23 VPN—IPsec
- 8.6.24 VPN—VPSS Setting
- 8.6.26 WAN Port Mirroring

Changed Contents

- System Components
 - Equipment Compatibility for Legacy Gateways
 - System Components for Legacy Gateways
- 1.4 Data Security
- 2.1.1 System Configurations
- 2.1.2 System Connection Diagram
- 2.2.1 Optional Equipment
- 2.3.1 General Description
- 2.3.3 System Capacity
- 3.1.1 Type and Maximum Number of Activation Keys
- 4.2.2 Names and Locations
- 4.3.1 Mother Board
- 4.4 Virtual Cards
- 4.6.1 STACK-M Card (KX-NS0130)
- 4.6.3 STACK-S (TDE) Card (KX-NS0132)
- 4.10 Connection of Peripherals
- 4.13 Starting the KX-NS1000

- 5.2 PC Connection
- 5.3 Starting Web Maintenance Console
- 5.3 Starting Web Maintenance Console
 - Converting KX-TDE, KX-NCP or KX-TDA100D System Data for Use with the KX-NS1000
 - KX-TVM System Prompt and Mailbox Data Import
- 5.4.1 Easy Setup Wizard
- 5.5 Programming a One-look Network
- 5.8.1 Assigning IP Addressing Information
- 5.10 Configuration of Users
- 5.12 Automatic Configuration of Mailboxes
- 6.1 Information about Stacking PBXs
- 8.1.2 DHCP (Dynamic Host Configuration Protocol) Server
- 8.1.3 VLAN (Virtual LAN)
- 8.1.6 Network Configuration
- 8.4.2 One-look Networking Survivability
- 8.4.2 One-look Networking Survivability
 - Recovering from Backup Master Operation to Master Operation
- 8.5 Port Security

9.3.4 PCMPR Software File Version 003.2xxxx

Changed Contents

- System Components
- Introduction
- 2.3.3 System Capacity
- 3.1.1 Type and Maximum Number of Activation Keys
- 4.11.1 LAN Connection for the Main Unit
- 4.11.2 LAN Connections for IP Telephones
- 5.2 PC Connection
- 5.3 Starting Web Maintenance Console
- 5.4.4 Installing Additional Activation Keys
- 5.8.1 Assigning IP Addressing Information
- 5.8.2 Setting VLAN Parameters
- 5.8.3 Setting LLDP Parameters
- 5.8.4 Setting Diffserv Parameters
- 5.8.5 Configuration of IP Ports
- 5.8.6 ECO mode (KX-NT500 series only)
- 5.9.1 Registering IP Telephones
- 5.9.4 Installing IP Phones at a Remote Site with a Built-in Media Relay Gateway
- 5.11 Programming E-mail Integration for UM Voice/Fax Messages
- 8.4.2 One-look Networking Survability
- 8.6.2 WAN Connection
- 8.6.13 Firewall—DoS Protection
- 8.6.23 VPN—IPsec
- 8.6.24 VPN—VPSS Setting



The KX-NS1000UK and KX-NS1000NE are designed to interwork with the:

- Analogue Public Switched Telephone Network (PSTN) of European countries
- Pan-European Integrated Services Digital Network (ISDN) using ISDN basic rate access
- Pan-European Integrated Services Digital Network (ISDN) using ISDN primary rate access

Panasonic System Networks Co., Ltd. declares that the KX-NS1000UK and the KX-NS1000NE are in compliance with the essential requirements and other relevant provisions of Radio & Telecommunications Terminal Equipment (R&TTE) Directive 1999/5/EC.

Declarations of Conformity for the relevant Panasonic products described in this manual are available for download by visiting:

<http://www.ptc.panasonic.eu>

Contact to Authorised Representative:

Panasonic Testing Centre
Panasonic Marketing Europe GmbH
Winsbergring 15, 22525 Hamburg, Germany

For Future Reference

Please print, record, and retain the following information for future reference.

Note

The serial number of this product can be found on the label affixed to the unit. You should record the model number and the serial number of this unit as a permanent record of your purchase to aid in identification in the event of theft.

MODEL NO.	_____
SERIAL NO.	_____
DATE OF PURCHASE	_____
NAME OF DEALER	_____
DEALER'S ADDRESS	_____

DEALER'S TEL. NO.	_____

Panasonic System Networks Co., Ltd.

1-62, 4-chome, Minoshima, Hakata-ku, Fukuoka 812-8531, Japan

Web Site: <http://www.panasonic.net/>

Copyright:

This material is copyrighted by Panasonic System Networks Co., Ltd., and may be reproduced for internal use only. All other reproduction, in whole or in part, is prohibited without the written consent of Panasonic System Networks Co., Ltd.

© Panasonic System Networks Co., Ltd. 2011

PNQX3640QA DD111HH9034