

Chapter 1 System Description.....	1-1
1.1 Overview of the Product	1-1
1.1.1 Product Position	1-1
1.1.2 System Applications.....	1-1
1.1.3 Product Features	1-3
1.2 Hardware Structure	1-4
1.2.1 Hardware Configurations	1-4
1.2.2 Functional Principles.....	1-5
1.2.3 Configuration Relationship with Other Devices.....	1-7
1.3 Software Structure.....	1-8
1.3.1 Overall Software Structure.....	1-8
1.3.2 Service Processes	1-9
1.4 System Functions	1-11
1.4.1 Service Functions	1-11
1.4.2 Operation and Maintenance Functions.....	1-11
1.5 Technical Specifications.....	1-12
1.5.1 System Specifications	1-12
1.5.2 Environment Specifications.....	1-13
1.5.3 Reliability Specifications	1-13
Chapter 2 System Installation	2-1
2.1 Overview of Installation	2-1
2.1.1 Installation Steps.....	2-1
2.1.2 Installation Preparations	2-3
2.2 Installing Hardware Components	2-4
2.2.1 Structure and Appearance of IBM Server	2-4
2.2.2 Installing Server Cables	2-6
2.3 Installing Operating System	2-7
2.3.1 Setting iGWB Hard Disk to "RAID5 + HostSpare" Mode	2-7
2.3.2 Installing Windows 2000 Server.....	2-11
2.3.3 Installing Windows 2000 Service Pack 4	2-20
2.3.4 Installing Windows 2000 Hotpatches.....	2-24
2.3.5 Installing Drivers for iGWB Network Adapter and RAID Adapter ...	2-28
2.3.6 Partitioning iGWB Hard Disk.....	2-34
2.3.7 Setting IP Address for iGWB Network Adapter.....	2-45
2.3.8 Setting Automatic Logon to Windows 2000 Server.....	2-48
2.4 Installing Billing Interface.....	2-48
2.4.1 Installing FTAM Protocol.....	2-49
2.4.2 Installing FTP Protocol.....	2-56
2.4.3 Setting User Authority	2-59

2.5 Installing iGWB Server Software	2-60
2.5.1 Installing Server Software	2-60
2.5.2 Modifying Server Software Settings	2-67
2.5.3 Modifying Software Watchdog Settings	2-73
2.6 Installing iGWB Client Software	2-75
2.6.1 Installing Operating System	2-75
2.6.2 Installing Client Software	2-75
2.6.3 Modifying Client Settings	2-82
2.7 Modifying iGWB Factory Settings.....	2-83
2.7.1 Checklist of iGWB Factory Settings	2-83
2.7.2 Modifying Computer Name and Workgroup.....	2-84
2.7.3 Modifying IP Address of Network Adapter	2-87
2.7.4 Modifying Administrator Password.....	2-87
2.7.5 Installing iGWB Server Software.....	2-90
2.7.6 Modifying Software Watchdog Settings	2-90
2.7.7 Setting Automatic Logon to Windows 2000 Server.....	2-90
2.8 Checking Installed Hardware and Software	2-90
2.8.1 Checking Installed Hardware	2-90
2.8.2 Checking Windows 2000 Server.....	2-90
2.8.3 Checking Server Software	2-93
2.8.4 Checking Client Software.....	2-94
Chapter 3 Basic Operations.....	3-1
3.1 Introduction to CDR Console.....	3-1
3.1.1 Graphical User Interfaces	3-1
3.1.2 Menu Bar	3-2
3.1.3 Toolbar	3-3
3.2 System Management	3-3
3.2.1 CDR Console Management	3-3
3.2.2 Office Management.....	3-7
3.2.3 System Customization	3-9
3.2.4 View Functions.....	3-10
3.3 Service Operations.....	3-10
3.3.1 CDR Management	3-10
3.3.2 State Query.....	3-15
3.3.3 Log Management.....	3-17
3.3.4 User Management	3-21
3.3.5 Other Functions	3-24
3.4 System Debugging	3-25
3.4.1 Debugging Information.....	3-26
3.4.2 Protocol Trace Information.....	3-30

3.4.3 Workflow Information	3-31
Chapter 4 System Maintenance.....	4-1
4.1 System User	4-1
4.2 Routine Maintenance	4-1
4.3 Software Upgrade	4-4
4.3.1 Overview of Software Upgrade	4-4
4.3.2 Ordinary Upgrade	4-5
4.3.3 Special Upgrade	4-6
4.4 Troubleshooting.....	4-7
4.4.1 Introduction to Fault Positioning Information.....	4-7
4.4.2 Collection of Fault Positioning Information.....	4-12
4.4.3 Common Trace Information and Related Maintenance	4-13
4.4.4 Frequently Asked Questions	4-18
Appendix A iGWB Configuration Instance.....	A-1
A.1 Configuration for Single-host Mode	A-1
A.1.1 Networking Diagram	A-1
A.1.2 IP Address Configuration of Network Adapters	A-2
A.1.3 Configuration of iGWB.....	A-3
A.2 Configuration for Cluster Mode	A-4
A.2.1 Networking Diagram	A-4
A.2.2 IP Address Configuration of Network Adapters	A-4
A.2.3 Configuration of iGWB.....	A-5
A.3 Port Usage	A-10
Appendix B Software Directory Description	B-1
B.1 Disk Directory Structure of iGWB Server	B-1
B.2 Structure of Client Software Directory.....	B-5
Appendix C Acronyms and Abbreviations.....	C-1

HUAWEI

U-SYS iGateway Bill
User Manual

V200R002

U-SYS iGateway Bill

User Manual

Manual Version T2-010162-20041012-C-2.25

Product Version V200R002

BOM 31014262

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. Please feel free to contact our local office or company headquarters.

Huawei Technologies Co., Ltd.

Address: Administration Building, Huawei Technologies Co., Ltd.,

Bantian, Longgang District, Shenzhen, P. R. China

Postal Code: 518129

Website: <http://www.huawei.com>




Email: support@huawei.com

Copyright © 2004 Huawei Technologies Co., Ltd.

All Rights Reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks

, HUAWEI, C&C08, EAST8000, HONET, , ViewPoint, INtess, ETS, DMC, TELLIN, InfoLink, Netkey, Quidway, SYNLOCK, Radium,  M900/M1800, TELESIGHT, Quidview, Musa, Airbridge, Tellwin, Inmedia, VRP, DOPRA, iTELLIN, HUAWEI OptiX, C&C08iNET, NETENGINE, OptiX, iSite, U-SYS, iMUSE, OpenEye, Lansway, SmartAX, infoX, TopEng are trademarks of Huawei Technologies Co., Ltd.

All other trademarks mentioned in this manual are the property of their respective holders.

Notice

The information in this manual is subject to change without notice. Every effort has been made in the preparation of this manual to ensure accuracy of the contents, but all statements, information, and recommendations in this manual do not constitute the warranty of any kind, express or implied.

About This Manual

Release Notes

The manual applies to the U-SYS iGateway Bill V200R002 (hereinafter referred to as the iGWB).

Organization

The manual presents the principle, installation, operation, and maintenance of the product in the following structure.

The manual contains four chapters and two appendixes

- **Chapter 1 System Description** introduces the iGWB's networking model, hardware structure, software structure, functional features, and technical specifications.
- **Chapter 2 System Installation** details two installation processes regarding the iGWB: the complete installation process and the on-site installation process.
- **Chapter 3 Basic Operations** presents the basic operations performed on the iGWB, including system management, service operations, and system debugging.
- **Chapter 4 System Maintenance** describes the maintenance tasks about the iGWB, software upgrade steps of the iGWB, and troubleshooting knowledge regarding the iGWB.
- **Appendix A iGWB Configuration Instance** describes the configuration in single-host mode or cluster mode of iGWB.
- **Appendix B Software Directory Description** provides a clear illustration of software directory of the iGWB server and client.
- **Appendix C Acronyms and Abbreviations** lists the full names of the acronyms and abbreviated used in the manual.

Intended Readers

The manual is intended for the following readers:

- Installation engineers
- Project engineering technicians
- Operation & maintenance specialists

Conventions

The manual uses the following conventions:

I. General conventions

Convention	Description
Arial	Normal paragraphs are in Arial.
Arial Narrow	Warnings, Cautions, Notes and Tips are in Arial Narrow.
Boldface	Headings are in Boldface .
Courier New	Terminal Display is in Courier New.

II. GUI conventions

Convention	Description
< >	Button names are inside angle brackets. For example, click the <OK> button.
[]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

III. Keyboard operation

Format	Description
<Key>	Press the key with the key name inside angle brackets. For example, <Enter>, <Tab>, <Backspace>, or <A>.
<Key1+Key2>	Press the keys concurrently. For example, <Ctrl+Alt+A> means the three keys should be pressed concurrently.
<Key1, Key2>	Press the keys in turn. For example, <Alt, A> means the two keys should be pressed in turn.

IV. Mouse operation

Action	Description
Click	Press the left button or right button quickly (left button by default).
Double Click	Press the left button twice continuously and quickly.
Drag	Press and hold the left button and drag it to a certain position.

V. Symbols

Eye-catching symbols are also used in the manual to highlight the points worthy of special attention during the operation. They are defined as follows:



Caution Means reader be extremely careful during the operation.



Note Means a complementary description.

Environmental Protection

This product has been designed to comply with the requirements on environmental protection. For the proper storage, use and disposal of this product, national laws and regulations must be observed.

Table of Contents

Chapter 1 System Description	1-1
1.1 Overview of the Product	1-1
1.1.1 Product Position	1-1
1.1.2 System Applications	1-1
1.1.3 Product Features.....	1-3
1.2 Hardware Structure.....	1-4
1.2.1 Hardware Configurations	1-4
1.2.2 Functional Principles	1-5
1.2.3 Configuration Relationship with Other Devices.....	1-7
1.3 Software Structure	1-8
1.3.1 Overall Software Structure	1-8
1.3.2 Service Processes	1-9
1.4 System Functions	1-11
1.4.1 Service Functions.....	1-11
1.4.2 Operation and Maintenance Functions	1-11
1.5 Technical Specifications	1-12
1.5.1 System Specifications	1-12
1.5.2 Environment Specifications.....	1-13
1.5.3 Reliability Specifications.....	1-13
Chapter 2 System Installation	2-1
2.1 Overview of Installation.....	2-1
2.1.1 Installation Steps	2-1
2.1.2 Installation Preparations.....	2-3
2.2 Installing Hardware Components.....	2-4
2.2.1 Structure and Appearance of IBM Server	2-4
2.2.2 Installing Server Cables	2-6
2.3 Installing Operating System.....	2-7
2.3.1 Setting iGWB Hard Disk to "RAID5 + HostSpare" Mode	2-7
2.3.2 Installing Windows 2000 Server.....	2-11
2.3.3 Installing Windows 2000 Service Pack 4	2-20
2.3.4 Installing Windows 2000 Hotpatches	2-24
2.3.5 Installing Drivers for iGWB Network Adapter and RAID Adapter.....	2-28
2.3.6 Partitioning iGWB Hard Disk	2-34
2.3.7 Setting IP Address for iGWB Network Adapter	2-45
2.3.8 Setting Automatic Logon to Windows 2000 Server.....	2-48
2.4 Installing Billing Interface	2-48
2.4.1 Installing FTAM Protocol	2-49

2.4.2	Installing FTP Protocol	2-56
2.4.3	Setting User Authority	2-59
2.5	Installing iGWB Server Software	2-60
2.5.1	Installing Server Software	2-60
2.5.2	Modifying Server Software Settings	2-67
2.5.3	Modifying Software Watchdog Settings	2-73
2.6	Installing iGWB Client Software	2-75
2.6.1	Installing Operating System	2-75
2.6.2	Installing Client Software	2-75
2.6.3	Modifying Client Settings	2-82
2.7	Modifying iGWB Factory Settings	2-83
2.7.1	Checklist of iGWB Factory Settings	2-83
2.7.2	Modifying Computer Name and Workgroup	2-84
2.7.3	Modifying IP Address of Network Adapter	2-87
2.7.4	Modifying Administrator Password	2-87
2.7.5	Installing iGWB Server Software	2-90
2.7.6	Modifying Software Watchdog Settings	2-90
2.7.7	Setting Automatic Logon to Windows 2000 Server	2-90
2.8	Checking Installed Hardware and Software	2-90
2.8.1	Checking Installed Hardware	2-90
2.8.2	Checking Windows 2000 Server	2-90
2.8.3	Checking Server Software	2-93
2.8.4	Checking Client Software	2-94
Chapter 3	Basic Operations	3-1
3.1	Introduction to CDR Console	3-1
3.1.1	Graphical User Interfaces	3-1
3.1.2	Menu Bar	3-2
3.1.3	Toolbar	3-3
3.2	System Management	3-3
3.2.1	CDR Console Management	3-3
3.2.2	Office Management	3-7
3.2.3	System Customization	3-9
3.2.4	View Functions	3-10
3.3	Service Operations	3-10
3.3.1	CDR Management	3-10
3.3.2	State Query	3-15
3.3.3	Log Management	3-17
3.3.4	User Management	3-21
3.3.5	Other Functions	3-24
3.4	System Debugging	3-25
3.4.1	Debugging Information	3-26
3.4.2	Protocol Trace Information	3-30

3.4.3 Workflow Information	3-31
Chapter 4 System Maintenance	4-1
4.1 System User	4-1
4.2 Routine Maintenance	4-1
4.3 Software Upgrade	4-4
4.3.1 Overview of Software Upgrade	4-4
4.3.2 Ordinary Upgrade.....	4-5
4.3.3 Special Upgrade.....	4-6
4.4 Troubleshooting	4-7
4.4.1 Introduction to Fault Positioning Information.....	4-7
4.4.2 Collection of Fault Positioning Information.....	4-12
4.4.3 Common Trace Information and Related Maintenance	4-13
4.4.4 Frequently Asked Questions	4-18
Appendix A iGWB Configuration Instance	A-1
A.1 Configuration for Single-host Mode.....	A-1
A.1.1 Networking Diagram	A-1
A.1.2 IP Address Configuration of Network Adapters	A-2
A.1.3 Configuration of iGWB	A-3
A.2 Configuration for Cluster Mode	A-4
A.2.1 Networking Diagram	A-4
A.2.2 IP Address Configuration of Network Adapters	A-4
A.2.3 Configuration of iGWB	A-5
A.3 Port Usage.....	A-10
Appendix B Software Directory Description	B-1
B.1 Disk Directory Structure of iGWB Server	B-1
B.2 Structure of Client Software Directory	B-5
Appendix C Acronyms and Abbreviations	C-1

Chapter 1 System Description

1.1 Overview of the Product

1.1.1 Product Position

The U-SYS iGateway Bill (hereinafter referred to as the iGWB) is a large-capacity billing gateway developed by Huawei. With advanced software and hardware techniques, the iGWB provides powerful CDR storage and conversion capabilities and supports the interconnection with a billing center through File Transfer Protocol (FTP) or File Transfer Access Management protocol (FTAM). The iGWB cooperates with the U-SYS SoftX3000 SoftSwitch System (hereinafter referred to as the SoftX3000), and provides a large-capacity CDR storage medium and billing interface for the SoftX3000.

1.1.2 System Applications

The SoftX3000 is the core of the Next Generation Network (NGN) and resides at the network control layer of the NGN. The SoftX3000 provides the functions of call control and connection management of voice, data, and multimedia services based on Internet Protocol (IP) packet network. For each call, the SoftX3000 must perform the charging processing in addition to call control, media gateway access control, resource allocation, protocol processing, routing, and authentication. In other words, the SoftX3000 must record the call related information, such as the calling number, called number, answer time, and on-hook time, in a particular format.

The charging tickets (also named original CDRs) generated by the SoftX3000 are buffered in the memory (usually called CDR pool) of its main processing unit. Limited by the capacity and security of the CDR pool, however, the original CDRs stored in the CDR pool must be transferred to a reliable storage medium in time. In addition, the contents and formats of the original CDRs are different from those required by the billing center, the CDR files must be pre-processed before being transmitted to the billing center.

The iGWB is a gateway-like device placed between the SoftX3000 and the billing center, used to implement the CDR receiving, pre-processing, buffering, and billing interfacing functions. Figure 1-1 shows the position of the iGWB in system networking.

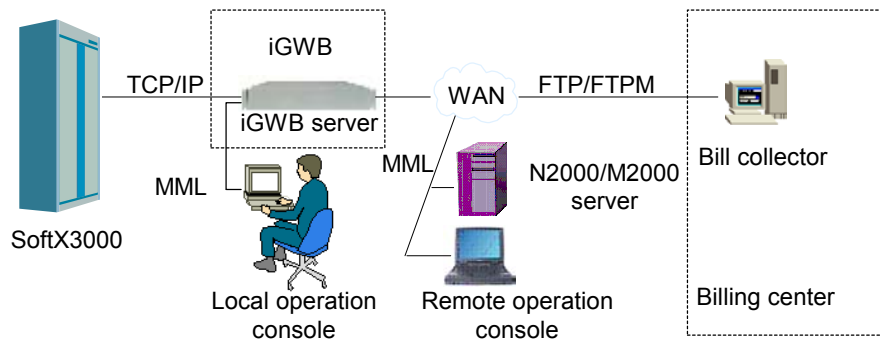


Figure 1-1 Position of iGWB in system networking

As shown in Figure 1-1, the external devices taking part in the iGWB networking model include SoftSwitch system (SoftX3000), billing center, and operation & maintenance system.

I. SoftSwitch system

SoftX3000 is responsible for call setup and control, producing original CDRs and storing them in its CDR pool temporarily. The iGWB server is connected to the SoftSwitch system through a separate network adapter, and receives the original CDRs from the SoftSwitch system.

II. Billing center

Generally, online billing is adopted between the SoftX3000 and the billing center. In this case, it is a basic function of the iGWB to provide a network interface to the billing center. The CDR collector, a component of the billing center, has direct communication with the iGWB. The CDR collector and the iGWB are interconnected through Wide Area Network (WAN), and communicate with each other through FTP or FTAM. In the case of FTP, the iGWB acts as the server, and the CDR collector acts as the client. In the case of FTAM, the iGWB acts as the responder, and the CDR collector acts as the initiator in a way similar to FTP communication. The iGWB provides a separate network adapter for communication with the billing center.

III. Network management system and CDR console

The iGWB is one of the devices managed by the network management system (NMS), and thus needs to provide a network interface to the NMS. The iGWB includes server and client. The iGWB client is managed by the NMS. Typically, it is required to configure a computer in the equipment room to function as a local maintenance console of the iGWB. A remote maintenance console can be configured as required. The iGWB provides a separate network adapter for communication with the NMS.

1.1.3 Product Features

I. High reliability

1) Dual-system

Because of the special position of the billing system in networking, high reliability of the iGWB is demanded. To achieve that, the iGWB adopts a dual-system design in both hardware and software. In addition, the iGWB provides an automatic switchover protection mechanism between the dual systems to ensure the operation reliability and service continuity.

2) Hard disk sub-system adopting redundant arrays of inexpensive disks (RAID) mode

Based on the experience of using server and mini computer, it is known that hard disk sub-system is prone to errors and failures. Therefore, the iGWB adopts RAID5 plus HotSpare. The purpose is to ensure that data will not be lost in the event of a fault occurring to one of the hard disks.

3) Network backup

The iGWB can automatically back up CDR files to another server through WAN or LAN, to further improve the data security.

4) Software auto-startup and restart after exit

A monitor module is designed in the software. The monitor module can automatically start up the iGWB in case of a power failure. The purpose is to ensure the normal running of the system when unattended.

II. Multi-access

The iGWB can receive and process CDRs in different formats, for example, CDRs generated by a mobile system or fixed network system. The CDRs in different formats are stored separately and provided respectively to the billing center.

III. Flexible CDR format conversion

The charging system of telecom carriers might have special requirements for CDR format. For example, they might need the iGWB to convert an original CDR in a binary format to a final CDR in another format such as text format or Abstract Syntax Notation One (ASN.1) format and abstract particular fields from an original CDR to generate a new CDR for the billing center. The iGWB provides flexible CDR format configuration and conversion functions to meet the diversified requirements of telecom carriers.

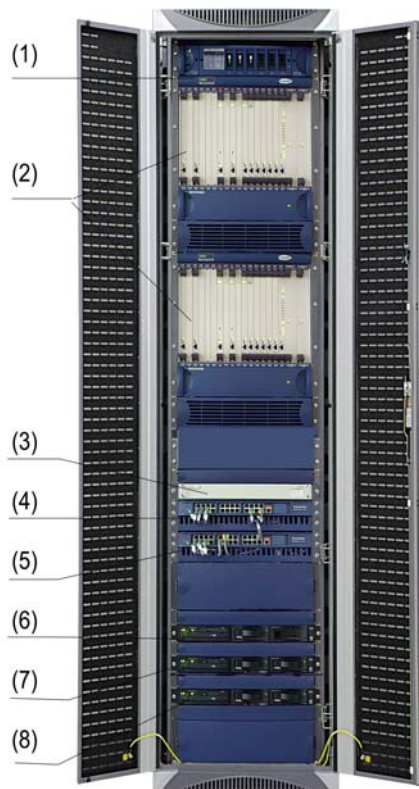
IV. Large capacity

The available capacity of the hard disks configured in the iGWB determines its CDR buffering capability. With greater CDR buffering capability, the iGWB can store more CDRs on itself and archive fewer CDRs in the billing center, which enhances the security of CDRs. Currently, the hard disks configured in the iGWB provide a sufficient valid capacity to store the CDRs that are generated by the SoftX3000 in at least seven days in the case of maximum subscriber quantity. In addition, the iGWB is scalable in hard disk capacity.

1.2 Hardware Structure

1.2.1 Hardware Configurations

In the SoftX3000, the iGWB and the basic service processing frame are configured in the same cabinet (integrated configuration cabinet). The related hardware components include active and standby iGWB servers, core Local Area Network (LAN) Switches, and an integrated converter, as shown in Figure 1-2.



- | | | | |
|------------------------------|--------------------------------|--------------------------|------------------|
| (1) Power distribution frame | (2) Service processing frame | (3) Integrated converter | (4) LAN Switch 1 |
| (5) LAN Switch 0 | (6) Back administration module | (7) Standby iGWB | (8) Active iGWB |

Figure 1-2 Cabinet configuration

I. iGWB server

The iGWB server is the core device of the iGWB system and adopts a dual-system design. Currently, two IBM X343 servers are employed. (Because server might be updated, the server module might be different from the actually delivered server model.) Each server provides four network adapters: two for communication with the SoftX3000, one for the billing center, and one for the NMS. In addition, the iGWB server has a built-in hard disk array.

The iGWB server communicates with the SoftX3000 to implement CDR storage, format conversion, and pre-processing functions.

II. Integrated converter

The active iGWB, the standby iGWB, and a back administration module (BAM) are configured in the integrated configuration cabinet. An integrated converter is thus configured in the cabinet, used to achieve operation control and switch of input and output devices, such as liquid crystal display (LCD), keyboard, and mouse.

III. LAN Switch

LAN Switch is the communication channel between the iGWB and the SoftX3000. Generally, Huawei's Quidway series products are selected for this purpose. Two LAN Switches are configured in the integrated configuration cabinet.

1.2.2 Functional Principles

The iGWB adopts a dual-system design. Two servers are operating in the active and standby mode. Heartbeat link is set up between the servers. Handshake messages are exchanged between them for each server to monitor the operating status of the other. Whenever the active server becomes faulty, the standby server automatically becomes active. The purpose is to ensure the continuity of the provided services. In addition, each server provides network adapters for communication with the SoftSwitch, the billing center, and the NMS. Consequently, the system has a dual-plane structure, which further improves the reliability of the system. Figure 1-3 illustrates the operating environments of the iGWB.

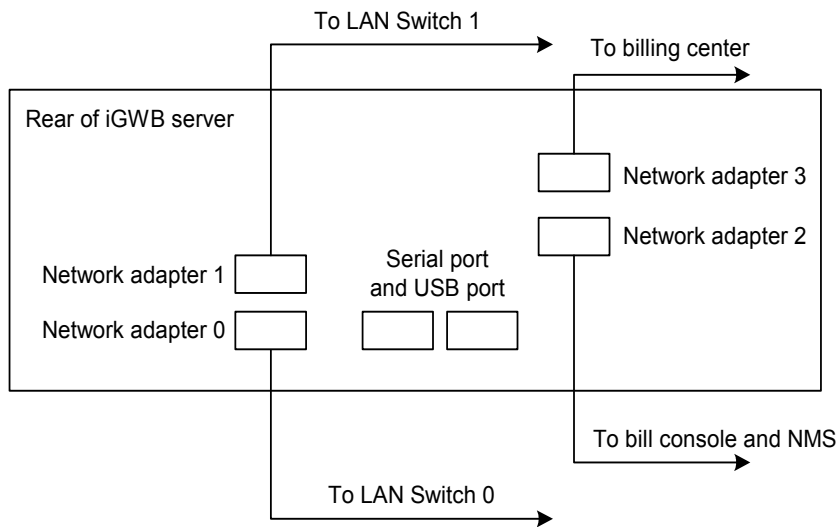


Figure 1-3 Operating environments of iGWB

I. iGWB network adapters

The iGWB server provides four network adapters for communication with outside. For easy description purposes, we number the network adapters as shown in Table 1-1.

Table 1-1 Network adapters of iGWB server

No.	Identifier	Function
0	Netcard0 to 0#LAN Switch	Connected to the LAN Switch 0 for communication with the SoftX3000 on the active plane.
1	Netcard1 to 1#LAN Switch	Connected to the LAN Switch 1 for communication with the SoftX3000 on the standby plane.
2	Netcard2 to Office LAN	Connected to the CDR console and NMS, also functioning as the first heartbeat path of the dual-system iGWB.
3	Netcard3 to Billing Center	Connected to the billing center, providing a billing interface.

II. Communication with the SoftSwitch system

The iGWB server communicates with the SoftX3000 by using network adapters 0 and 1. The active plane of the SoftSwitch system is connected through the core LAN Switch 0 to network adapters 0 of the active and standby iGWB servers. The standby plane of the SoftX3000 is connected through the core LAN Switch 1 to network adapters 1 of the active and standby iGWB servers. The two core LAN Switches interwork with each other through concatenation cable.

Network adapters 0 of the active and standby iGWB servers must be set with the same virtual IP address, which is in the same network segment as the active plane of the SoftX3000. Similarly, network adapters 1 of the active and standby iGWB servers must also be set with the same virtual IP address, which is in the same network segment as the standby plane of the SoftX3000. The virtual IP addresses are achieved by software configuration.

III. Communication with the billing center

The iGWB server communicates with the billing center by using network adapter 3 for the billing center to collect CDRs. The communication protocol can be FTP or FTAM.

Normally, the billing center simultaneously logs in to the active and standby iGWB servers. The active and standby iGWB servers provide different IP addresses to the billing center.

IV. Communication with the bill console and NMS

Network adapter 2 is used for connection between the NMS and the bill console, providing a man-machine interface. In addition, network adapter 2 acts as the first heartbeat path between the active and standby iGWB servers.

Network adapters 2 of the active and standby iGWB servers must be set with the same virtual IP address, which is in the same network segment as the CDR console (NMS). The virtual IP address is achieved by software configuration. For more information, refer to Chapter 2 “System Installation”.

V. Heartbeat paths

Heartbeat paths are configured between the active and standby iGWB servers to exchange handshake messages. With the heartbeat paths, each iGWB server can monitor the operating status of the other and back up the status for future switchover usage. The status backed up includes CDR sequence number, front disk state, back disk state, and so on. The system provides two heartbeat paths, which are in the “private network” inside the system. The first heartbeat path is the LAN that is formed by network adapters 2. The second heartbeat path passes through serial ports. When the first heartbeat path is broken, the iGWB servers use the second heartbeat path for communication.

1.2.3 Configuration Relationship with Other Devices

The following serving devices need be configured to ensure the normal running of the iGWB and facilitate maintenance.

I. Power supply

The power distribution box in the integrated management cabinet supplies power for the iGWB. The nominal voltage is -48 VDC.

II. Integrated converter

The active and standby iGWB servers are connected to the integrated converter through C2T line. The integrated converter achieves input/output control and other operations on the servers.

III. Client

The iGWB also includes a computer as the client. The computer must be installed in the same LAN as network adapter 2 of the iGWB server. The client is used for device debugging, CDR browse, CDR query, and routine maintenance purposes.

1.3 Software Structure

1.3.1 Overall Software Structure

The iGWB is a multi-process and multi-threaded system in the client/server mode.

The iGWB software is designed to be several thread modules based on independent services. The thread modules that have the closest relationship to a particular service function are incorporated to be a specific process. In this way, the software is structured in multi-process and multi-threaded manners. Client/server mode is employed for communication between the processes. In other words, a particular process is the kernel, and the other processes act as sub-processes. The kernel process schedule and monitor the service sub-processes.

Figure 1-4 illustrates the overall structure of the iGWB software.

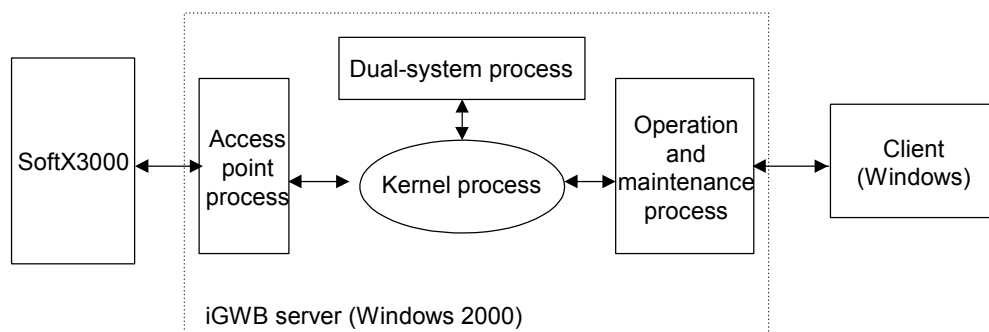


Figure 1-4 Structure of iGWB software

1.3.2 Service Processes

As shown in Figure 1-4, the iGWB server is composed of a kernel process, a dual-system process, an access point process, and an operation and maintenance process. Each process contains several service thread modules that are relatively independent of each other.

I. Kernel process

The kernel process is the core of the whole software. It acts as the Transmission Control Protocol/Internet Protocol (TCP/IP) server for the other processes. It is responsible for starting, stopping, and monitoring the access point process and the operation and maintenance process. This process is composed of a dual-system monitor module and a dual-system interface module.

II. Access point process

The access point process incorporates the main service functions of the iGWB, including CDR reception, CDR processing, and CDR storage. The service functions are integrated to be a network module, a front disk module, a CDR processing module, and a back disk module. The four modules constitute a CDR processing flow, in which the service log is uni-directional and can be cut down. See Figure 1-5. (The arrows stand for the transmission directions of the CDR data.)

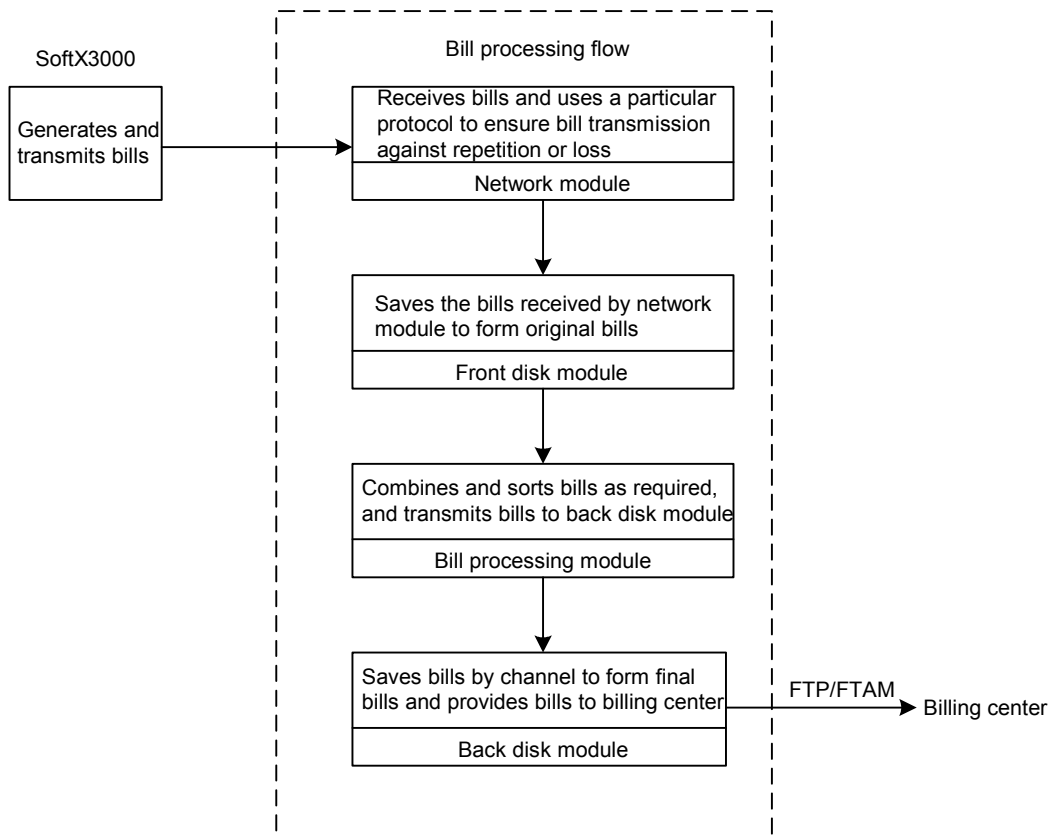


Figure 1-5 CDR processing flow

III. Operation and maintenance process

The operation and maintenance process integrates the operability and maintainability functions of the iGWB. In terms of functionality, the incorporated service modules include a log module, a backup module, a CDR browse and query module, a man-machine language (MML) server module, a performance module, and an alarm module. The modules are relatively independent of each other.

IV. Dual-system process

The design of the iGWB aims at the cross-platform dual systems. The dual-system design greatly varies with different platforms. Consequently, the dual-system process is used to mask the details of the dual-system functionality at different platforms. The dual-system process enables the processes interacting with it to ignore the differences of the platforms. This process has only one service module—a dual-system management module.

Each of the preceding four processes has a management module and a message transfer module. The management module manages and schedules the various

modules inside the process. The message transfer module is responsible for communication and message transfer between the processes.

1.4 System Functions

The iGWB system provides two categories of functions: system service, and operation and maintenance.

1.4.1 Service Functions

I. CDR processing function

The iGWB system sorts the original CDRs as required. The different types of CDRs can be sorted to different storage directories in accordance with the pre-defined sorting conditions, for example, sorting by CDR type.

II. Flexible billing interface

The iGWB system can communicate with the billing center through FTP or FTAM. The iGWB system supports configuring CDR file name, file size, and file generation time. The iGWB system supports flexibly converting CDR format.

III. Reliable dual-system function

The iGWB system supports automatic switchover and manual switchover of the dual systems. The iGWB system supports auxiliary upgrade.

IV. Optimized alarming function

The iGWB system provides a variety of alarms, such as medium space alarm, file read/write error alarm, dual-system switchover alarm, CDR collection timeout alarm, and heartbeat interruption alarm.

V. CDR backup over network

The iGWB system can back up the CDRs in real time to another computer over the network. The purpose is to improve the security of the data.

1.4.2 Operation and Maintenance Functions

I. User management functions

The system provides functions to add and delete an operator account, and modify and query operator information.

II. Software management functions

The system provides functions to query information about the software version of the iGWB server and the client.

III. CDR storage setting functions

What can be set includes storage paths for original CDRs and final CDRs, size of a final CDR file, generation duration of a final CDR file, and buffer expiration of CDRs.

IV. Routine maintenance functions

- Log management function

The system provides log browse and query functions. Log of a specified user in specified time can be queried. The system log can be queried.

- CDR browse and query function

CDRs can be queried according to CDR type, date, subscriber number, and conversation duration.

- Performance monitor function

The system supports monitoring the memory space, hard disk space, and heartbeat state in real time.

- Commissioning function

The running status of the system can be displayed in real time.

- Protocol trace function

The system provides functions to trace message flow inside the system and message flow between the iGWB and the SoftX3000.

1.5 Technical Specifications

1.5.1 System Specifications

Technical parameter		Specification
Hard disk capacity	Standard configuration	432 GB
	Maximum configuration	730 GB
CDR processing capability		2,300 CDR/s
Cabinet dimensions (Width x depth x height)		600 mm × 800 mm × 2,200 mm
Weight of server		42 kg
Power consumption of server		700 W

1.5.2 Environment Specifications

Technical parameter		Specification
Power supply	Nominal voltage	-48 V
	Allowed range	-52 V to -40 V
Operating temperature	Long-term operation	0 to +45 °C
	Short-term operation	-40 to +60°C

1.5.3 Reliability Specifications

Technical parameter	Specification
Mean time between failure (MTBF)	40,000 hours
Mean time to repair (MTTR)	0.25 hours

Chapter 2 System Installation

2.1 Overview of Installation

2.1.1 Installation Steps

A complete installation process of the iGWB includes preparation, hardware installation, server software installation, and client software installation, as shown in Figure 2-1.

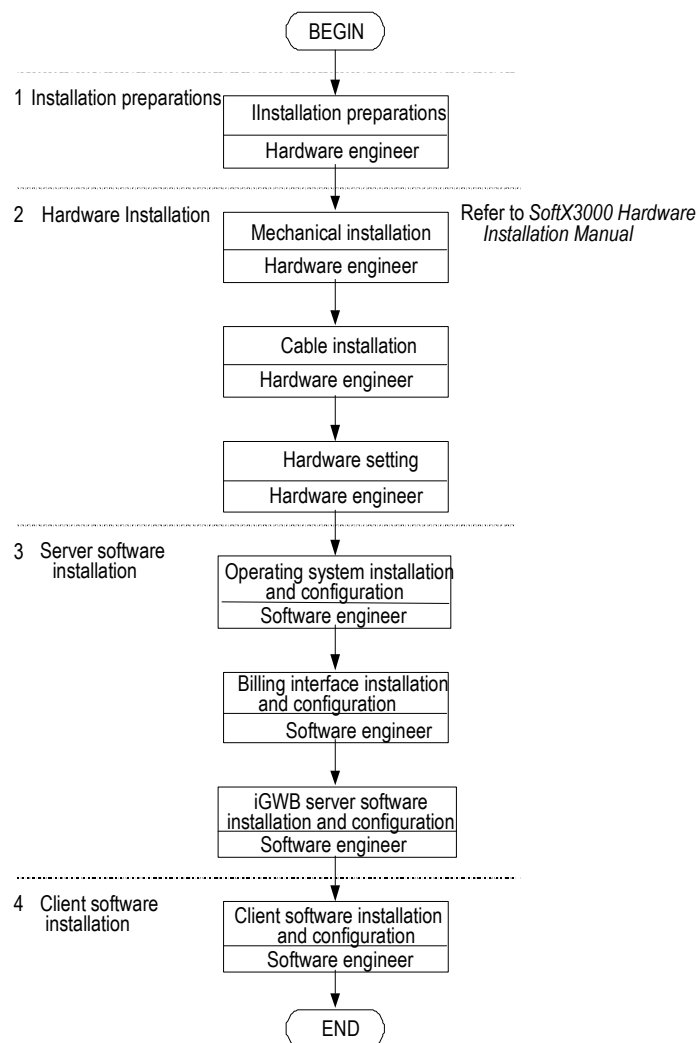


Figure 2-1 Complete installation process of iGWB

Usually, the server software has been installed and debugged before the delivery of the iGWB. After the debugging, the iGWB server software is uninstalled in the factory for version matching and deployment convenience purposes. Therefore, only the iGWB server software needs to be installed and partial settings have to be modified at the site. The operation steps are illustrated in Figure 2-2.

For the on-site installation process of the server, refer to section 2.7 Modifying iGWB Factory Settings.

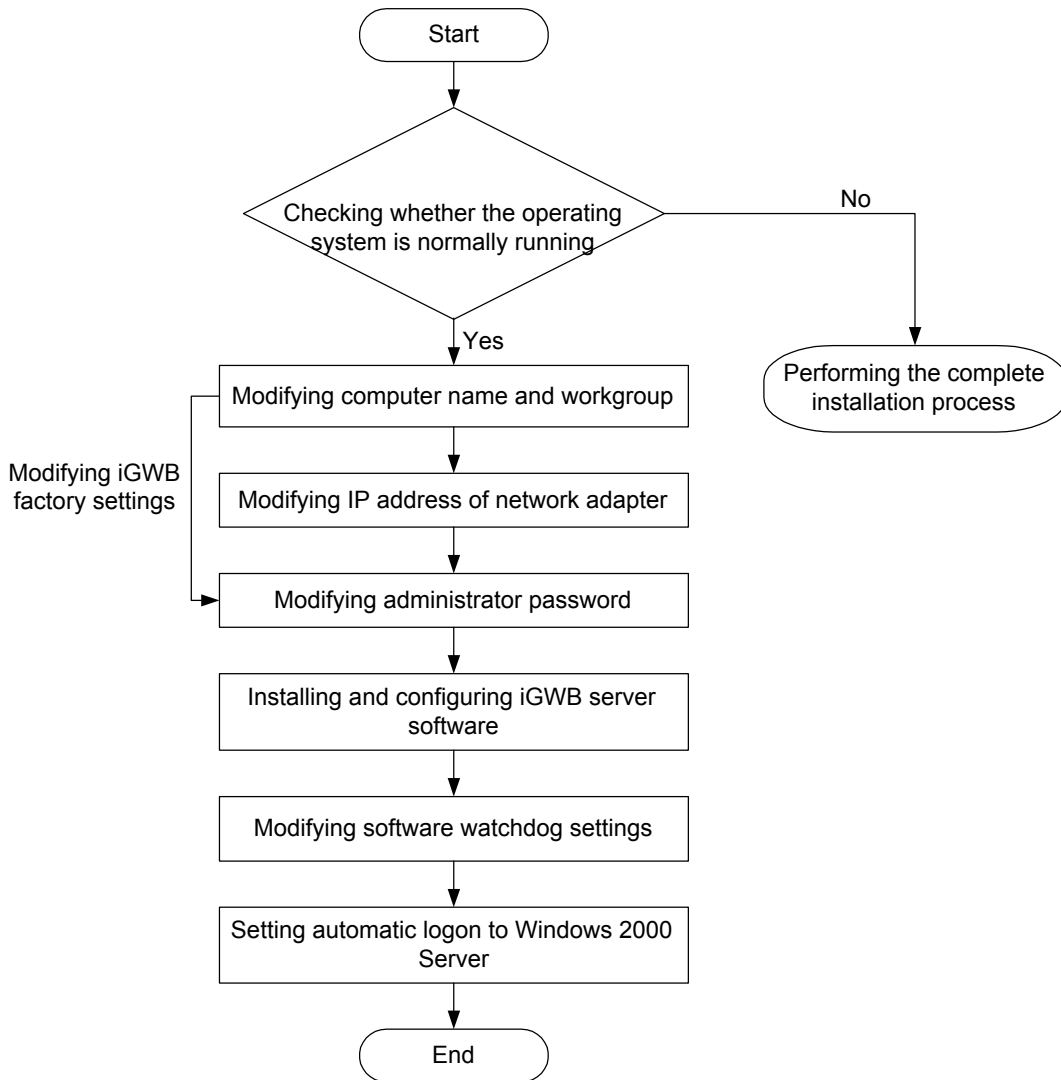


Figure 2-2 On-side installation process of server

2.1.2 Installation Preparations

I. Preparing installation tools

Ensure that one straight screwdriver and one cross screwdriver are available.

II. Checking server hardware configurations

With reference to the related server configuration checklist, check the basic hardware components of the servers one by one. Ensure that the configurations of both servers are the same. Currently, the IBM x343 model is used as the server. Each server has the basic configurations as shown in Table 2-1.

Table 2-1 Basic server configurations

Item	Configuration
CPU	Two Intel Pentium III 1.26 GHz or higher processors
Hard disk	One 34 GB hard disks (10 KB RPM SCSI hard disks) Five 73 GB hard disks (hard disk array)
Memory	Two 1 GB memories
Network adapter	Four 10/100 MB network adapters
RAID adapter	Single ServeRAID-4L adapter

Each hard disk array consists of ten 73 GB hard disks. The five hard disks one the left are controlled by one iGWB, while the five hard disks on the right are controlled by the other iGWB.

 **Note:**

The hardware configuration of the iGWB server may be updated; so the preceding configuration is for reference only.

III. Checking required installation software

The following lists the installation software required:

- ServeRAID Support CD (used to set the hard disks of server to be RAID5 mode)
- ServeRAID 5.10 Driver for Windows 2000 Server floppy disk (used to install the driver for SCSI controller)

- IBM 10/100 Ethernet Server Adapters Family Device Drivers and Installation CD (used to install the driver of iGWB extended network adapter)
- Windows 2000 Server CD (used to install Windows 2000 Server including Windows 2000 Service Pack 3.0)
- Microsoft Windows 2000 Service Pack4 CD (used to install)
- Vertel UTS-FTAM installation software (optional)
- iGWB software installation CD (including server and client installation software)

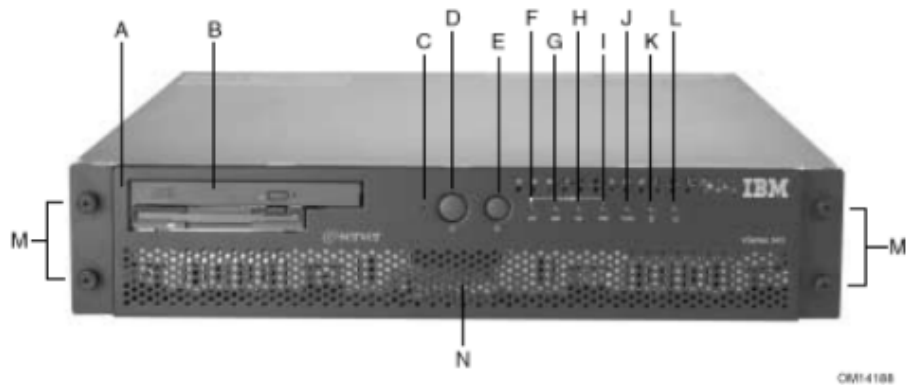
2.2 Installing Hardware Components

The iGWB server is installed in the integrated configuration cabinet of the SoftX3000. The iGWB hardware installation is carried out during the SoftX3000 hardware installation. This chapter details cable connection after the cabinet and the components are installed. For the mechanic installation of the iGWB server, refer to *U-SYS SoftX3000 SoftSwitch System Hardware Installation Manual*.

2.2.1 Structure and Appearance of IBM Server

I. Front view

Figure 2-3 shows the front view of the iGWB server with the bezel.



A Bezel	B Peripheral bay	C NMI switch
D Power switch	E Reset switch	F Critical alarm indicator
G Major alarm indicator	H Minor alarm indicator	I Power alarm indicator
J Network adapter status indicator	K Hard disk status indicator	L Power supply status indicator
M Bezel removal thumbscrews	N Hard drive tray	

Figure 2-3 Front view of iGWB server with bezel

Figure 2-4 shows the front view of the server with the bezel removed.

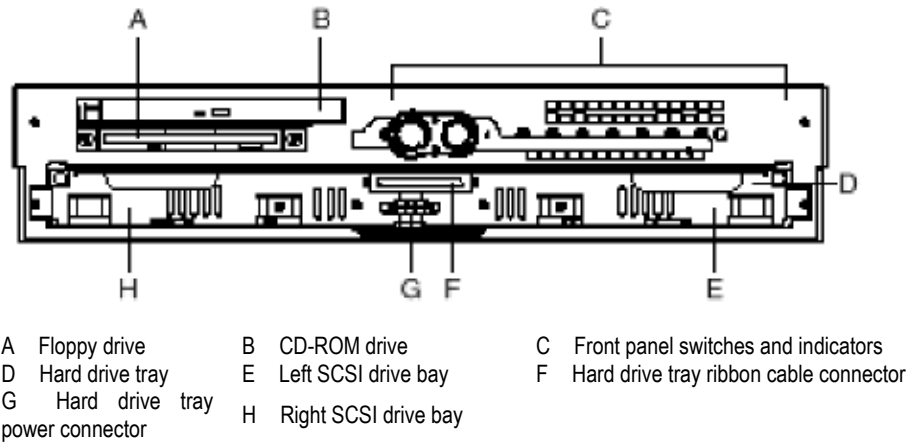
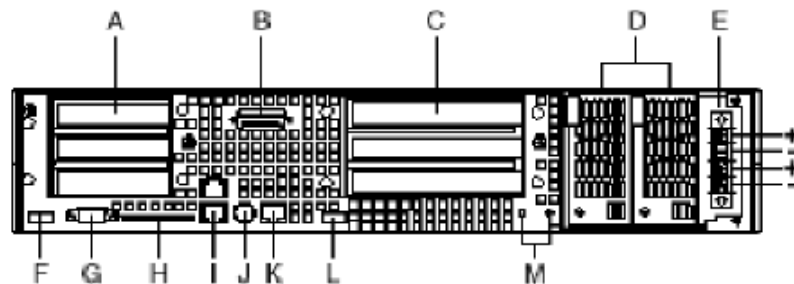


Figure 2-4 Front view of iGWB server with bezel removed

II. Back view

Figure 2-5 shows the back view of the iGWB server.



- A Three half-length 64-bit, 66 MHz PCI add-in board slots (3.3 V riser board)
- B DB-15 male connector for front panel alarm relay contacts
- C Three full height, full length 64-bit, 33 MHz PCI add-in board slots (5 V riser board), upper one of which is used for RAID adapter (with SCSI interfaces and disk array cables), and the other two of which are used for network adapters 2 and 3
- D Redundant, hot-plug power supplies
- E Four-terminal DC input power connector for DC input power supply cage
- F USB port 1
- G Video connector
- H External wide SCSI Ultra160 68-pin connector
- I Dual NIC 10/100 E/N RJ45 connectors NIC 1 (lower) and NIC 2 (upper), of which the upper one is used for network adapter 1 and the lower one is used for network adapter 0.
- J The PS/2 port can accept both keyboard and mouse. Use the included “Y” splitter cable to connect a mouse and a keyboard to the PS/2 port at the same time.
- K Serial port (COM2), 8-pin RJ45 connector
- L USB port 0
- M Two grounding plugs for attachment of grounding wire to chassis

Figure 2-5 Back view of iGWB server

2.2.2 Installing Server Cables

I. Connecting power cables

The power input to the IBM x343 server is –48 VDC. Dual redundant power supplies are adopted, and thus the server can keep running normally when only one power supply is available.

When connecting power cables, note that the positive pole of the power terminal of the server should be connected to the grounding terminal of –48 VDC power supply, and that the negative pole should be connected to the “–48V” terminal of –48 VDC power supply.

II. Connecting network cables

The IBM x343 server provides four network ports. The network ports are numbered as shown in Table 2-2 for description purposes. Network cables must be strictly installed based on the correspondence.

Table 2-2 Numbering plan of server network adapters

Position	Number	Usage
Lower network port on integrated network adapter	0	Connected to the LAN Switch 0 for communication with the SoftX3000 on the active plane.
Upper network port on integrated network adapter	1	Connected to the LAN Switch 1 for communication with the SoftX3000 on the standby plane.
Lower network port of PCI network adapter (PCI network adapter 2)	2	Connected to the bill console and NMS, also functioning as the first heartbeat path of the dual-system iGWB.
Upper network port of PCI network adapter (PCI network adapter 3)	3	Connected to the billing center, providing a billing interface.

III. Connecting serial port cables

The serial port cable is used to connect the serial ports of two servers as the second heartbeat connection between the active and standby iGWB servers. Figure 2-5 shows the position of the serial port.

IV. Connecting C2T cables

C2T cables are used to connect the servers with display, keyboard, and mouse. To save space, two iGWB servers and the BAM server will share one set of display, keyboard, and mouse, which are switched by the integrated converter. The servers are connected to the KVM/LCD converter through C2T cables.

One end of the C2T cable is connected to the corresponding port of the server. The other end of the C2T cable is connected to the correct channel port of the KVM/LCD converter.

V. Connecting disk array cables

The disk array is configured in IBM x343 server with ten hard disks. The disk array is divided into two parts, each of which provides a signal cable. Connect the left disk array to iGWB0 and the right disk array to iGWB1.

VI. Binding cables

The iGWB related cables should be bound with the other cables in the integrated configuration cabinet. For details, refer to *U-SYS SoftX3000 SoftSwitch System Hardware Installation Manual*.

If the installed softswitch system is not the SoftX3000, read the related manuals for installation.

2.3 Installing Operating System

The installation steps for the operating system of the active and standby iGWBs are the same. The following presents the installation steps of the active one and provides the specific settings of the standby one when different.

Before the installation of Windows 2000, conduct the RAID configuration of the server. The built-in hard disk array of the iGWB server should be set to be "RAID5 + HostSpare" (3+1+1) mode.

Installation of Windows 2000 Server requires two CDs: ServeRAID Support CD for RAID5 setting and Windows 2000 Server CD (with Windows 2000 Service Pack 4.0 contained) for Windows 2000 Server installation.

2.3.1 Setting iGWB Hard Disk to "RAID5 + HostSpare" Mode



Caution:

Re-setting of the RAID5 mode of the hard disks will cause all data on the disks lost. Be careful to perform this operation.

The hard disks of the iGWB server employ the “RAID5 + HostSpare” redundant and error tolerance techniques for data security purposes.

RAID5 is a disk-striping strategy with a dedicated check disk. Data is allocated on several disks to improve the read/write speed. Check data is also allocated on several disks instead of being stored on a dedicated check disk. When one of the disks becomes faulty, the controller can restore or create the lost data from other disks without influence on the availability of the data.

RAID5 requires a minimum of three disks. The availability ratio of the disk space is about $(N-1)/N$, in which N is the number of the disks in the hard disk array.

Compared with the “RAID5” mode, the “RAID5 + HostSpare” mode adds one disk as the hot spare disk.

When the iGWB uses the IBM server, the hard disk array is usually configured (with ten hard disks). DIP switch of the hard disk array can be set so that the active and standby servers manage five hard disks respectively. (Four hard disks are set to the RAID5 mode and the left one is configured to hot spare.) Set the first bit of the DIP switch SW4 of the hard disk array to “ON”, and retain the factory settings of the other switches.

Note:

The hard disks of the iGWB have been set to the RAID5 mode before the delivery. Confirm the RAID5 mode at the site.

The IBM server provides a dedicated tool, ServeRAID Manager, to manage and configure ServeRAID. The graphical interface of the ServeRAID Manager is shown in Figure 2-6.

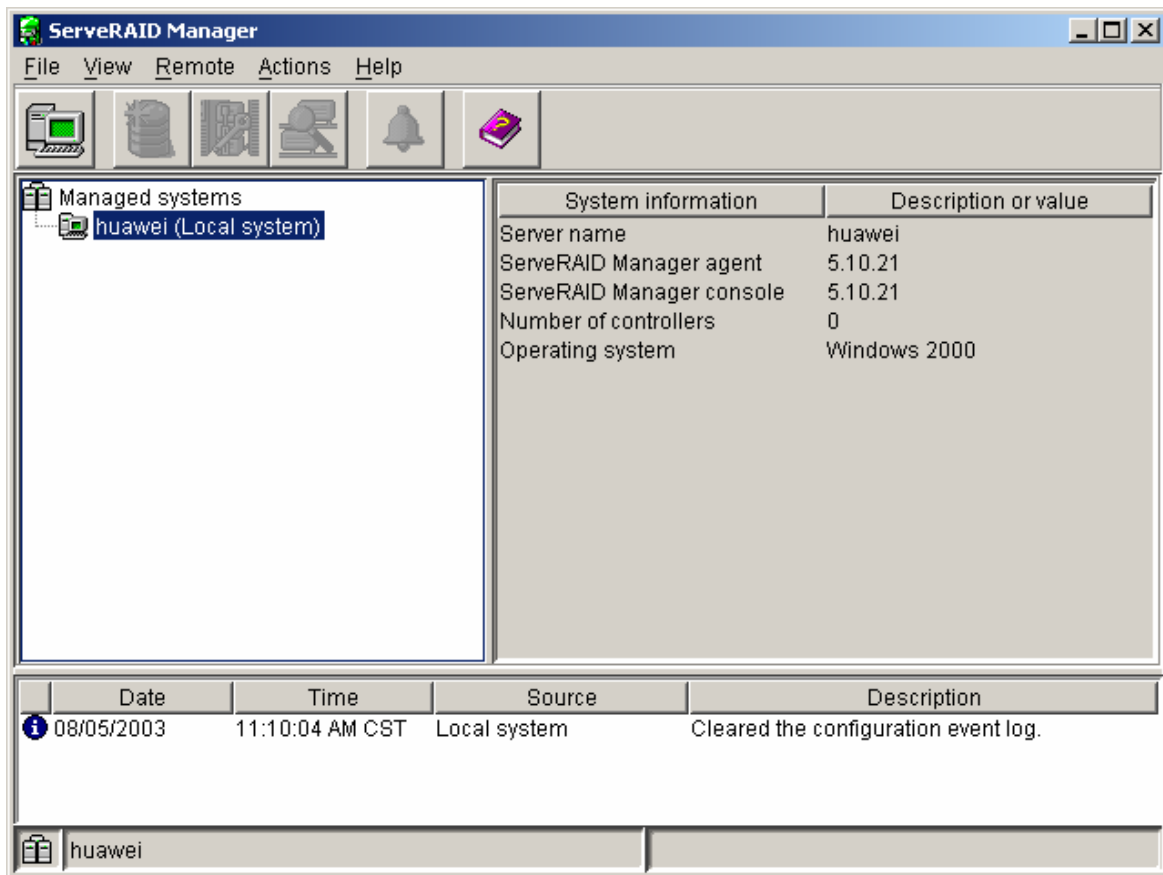


Figure 2-6 Graphical interface of ServeRAID Manager

To set the RAID5 mode by using ServeRAID program, proceed as follows:

I. Setting the server to boot from the CD-ROM

- 1) Power on the server. When the startup screen is displayed after the self-test of the system, press <F2> to enter the BIOS setting program.
- 2) In the [BIOS SETUP UTILITY] screen, select the [Boot] menu by using the arrow keys.
- 3) In the [Boot] menu, set [Boot Device Priority] according to the displayed guide. Set the first boot device to be "ATAPI CD-ROM". Press <F10> to save the settings and exit.

II. Booting the server from the ServeRAID Support CD

Insert the ServeRAID Support CD into the CD-ROM drive. Boot the server from the CD. After the boot, the [ServeRAID Manager] window is displayed.

III. Checking whether logical drives and RAID5 mode are configured

The ServeRAID Manager detects all ServeRAID controllers of the system. Check whether logical drives and RAID5 mode are configured in the system.

- 1) The following are the criteria, for Figure 2-7, for judging that logical drives and RAID5 mode are configured and all devices are operating well:
 - All node icons are green, indicating that the devices are operating well. (Red indicates faulty. Yellow indicates abnormal state.)
 - After all nodes are expanded, the hierarchical structure of the nodes and the number of the nodes are consistent with the display in the left pane as shown in Figure 2-7. For example, one 210018 MB logical drive is created. Six physical drives are available, among which four are in the online state, one is in the hot spare state, and one is in the enclosure state.

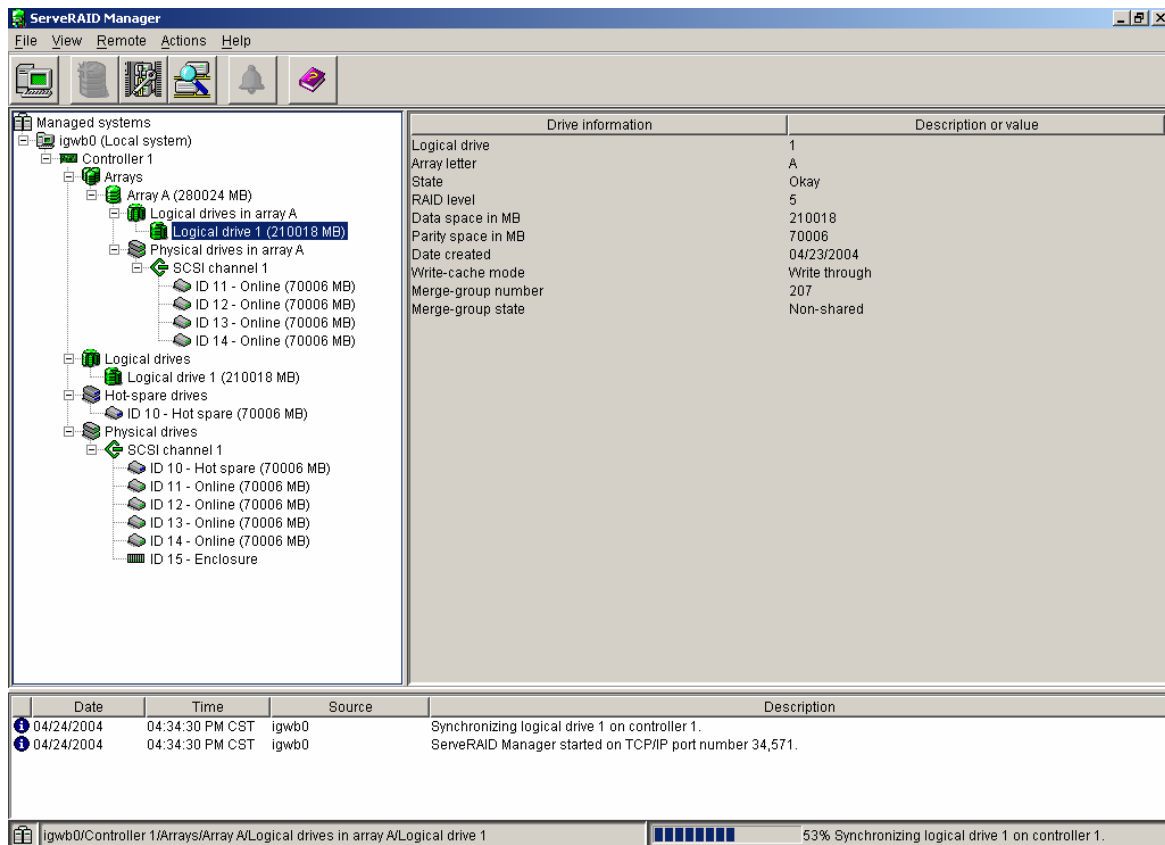


Figure 2-7 Interface with successful RAID5 configuration

- 2) If the system displays information or state that is inconsistent with the preceding description, it indicates that logical drives or RAID5 mode is not configured or, even configured, the operating status of the devices are abnormal. In these cases, proceed as follows. If the system is successfully configured with the RAID5 mode, skip the following setting of RAID and go to the installation of Windows 2000 Server.

IV. Restoring the working mode of the hard disks to factory-default settings

Before setting the hard disks of the iGWB to the RAID5 mode, restore the working mode of the hard disks to the factory settings. Proceed as follows:

- 1) Right-click the [Controller 1] node. Select [Restore to factory-default settings] from the displayed menu.
- 2) Click <Yes> to confirm the restoration.
- 3) The system begins the initialization. After about one minute, the content of the [Controller 1] node is displayed as "Controller 1(not configured)". It indicates that the RAID5 mode is not configured.

V. Setting the hard disks of the iGWB to the RAID5 mode

- 1) Right-click the [Controller 1 (not configured)] node. Select [Configure RAID] from the displayed menu. The [Configure the ServeRAID controller] window is displayed.
- 2) In the [Configure the ServeRAID controller] window, select [Custom configuration for controller 1] in the [Configuration paths] area. Click <Next>.
- 3) In the following window, the currently installed physical disks are displayed on the [System LocalHost, Controller 1] tab in the half pane.
- 4) Click <Add> in the middle to add four of the hard disks to the [New array A] area and the fifth to the [Spares] area. Click <Next>.
- 5) The current RAID configurations are displayed. Click <Next>.
- 6) The current RAID5 configurations are displayed. Click <Apply>. Click <Next> to confirm the modification.
- 7) You are prompted to restart the server to make the configurations effective. Click <Restart>.

Now, the configuration is completed. After the system is restarted, it is strongly recommended to check again whether the logical drives and RAID5 mode are configured according to the preceding operations.

2.3.2 Installing Windows 2000 Server

I. Setting the server to boot from the CD-ROM

- 1) Power on the server. When the startup screen is displayed after the self-test of the system, press <F2> to enter the BIOS setting program.
- 2) In the [BIOS SETUP UTILITY] screen, select the [Boot] menu by using the arrow keys.
- 3) In the [Boot] menu, set [Boot Device Priority] according to the displayed guide. Set the first boot device to be "ATAPI CD-ROM". Press <F10> to save the settings and exit.

II. Booting the system from the Windows 2000 Server CD

- 1) Insert the Windows 2000 Server CD into the CD-ROM drive.
- 2) Insert the ServeRAID 5.10 Driver for Windows 2000 Server floppy disk into the floppy disk drive.

If the ServeRAID 5.10 Driver for Windows 2000 Server floppy disk is lost, read the following. Otherwise, skip the following creation process.

If the ServeRAID 5.10 Driver for Windows 2000 Server floppy disk is lost, create one as follows:

Insert a formatted floppy disk into the floppy drive and the ServeRAID Support CD into the CD-ROM drive.

In the DOS mode, execute the command: **X:\diskette\tools\dsk4w32.exe X:\diskette\winsrv img a:**, where X represents the CD-ROM drive letter.

After the execution is completed, the specified driver is copied to the floppy disk.

- 3) After the server is restarted, you are prompted to "Press any key to boot from CD". Press any key to boot the server from the CD.

III. Copying installation files (pressing <F6> required)

The [Windows 2000 Setup] screen is displayed. The following information is also displayed at the bottom:

```
Press F6 if you need to install a third party SCSI or RAID driver...
```

Press <F6> before this information disappears. The system begins copying the installation files. (If the prompt information disappears before you press <F6>, the system will not install a third party SCSI controller driver. Interrupt the current installation and restart the installation program again.)

IV. Installing SCSI controller driver

- 1) After about five minutes, the following information is displayed:
Setup could not determine the type of one or more mass storage devices installed in your system, or you have chosen to manually specify an adapter. Currently, Setup will load support for the following mass storage device(s):

```
<none>
```

* To specify additional SCSI adapters, CD-ROM drives, or special disk controllers for use with Windows 2000, including those for which you have a device support disk from a mass storage device manufacturer, press S.

* If you do not have any device support disks from a mass storage device manufacturer, or do not want to specify additional mass storage device for use with Windows 2000, press ENTER.

Press <S> to add a SCSI controller.

- 2) You are prompted to insert the driver disk. Insert the ServeRAID 5.10 Driver for Windows 2000 Server floppy disk into the floppy disk drive. Press <Enter> to continue.
- 3) The system searches the SCSI controllers in the server and displays the information about the found SCSI controllers. The first controller is automatically positioned and looks highlighted. Press <Enter> to select it.
- 4) You are prompted whether to add more SCSI controllers. In this case, press <Enter> to continue. The system continues to copy the installation files.

V. Selecting the setup mode

After the initial installation files are copied, the Windows 2000 Server Setup program is started, as shown in Figure 2-8.

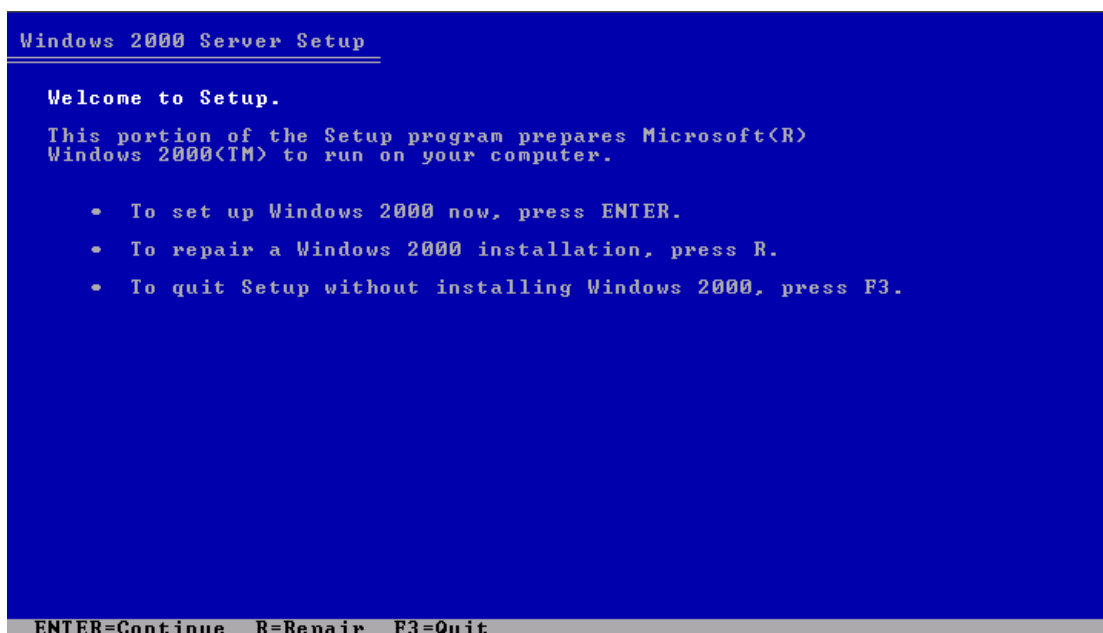


Figure 2-8 Selecting setup mode

Press <Enter> to set up Windows 2000.

VI. Confirming the licensing agreement

Read carefully the Windows 2000 Licensing Agreement. To accept it, press <F8>. Otherwise, press <ESC> to quit the setup.

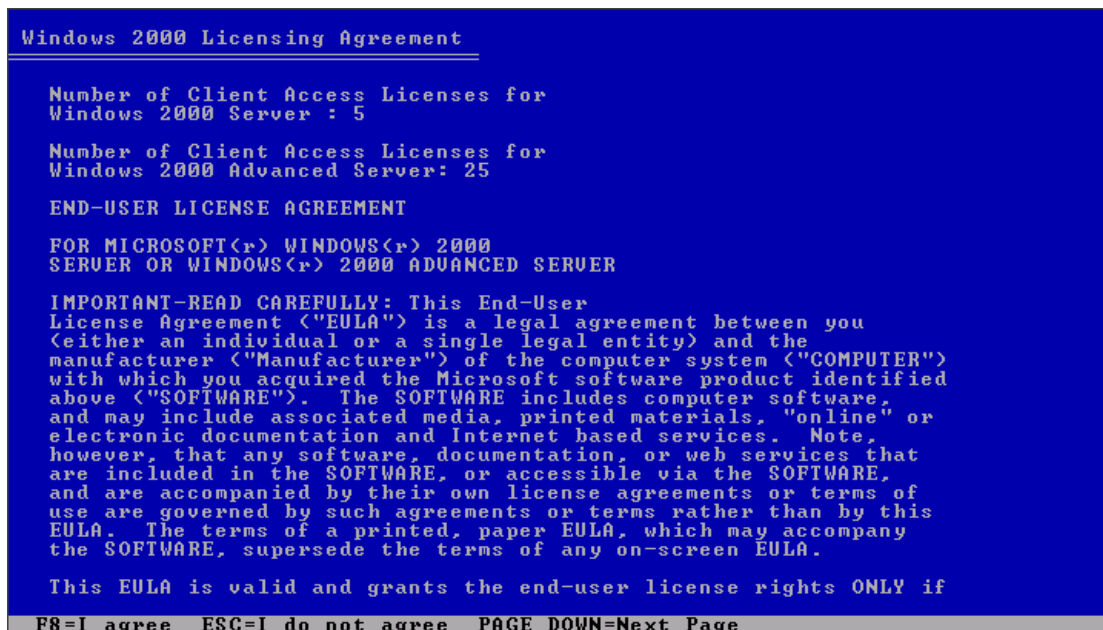


Figure 2-9 [Windows 2000 Licensing Agreement] screen

VII. Creating partitions and continuing copying installation files

- 1) The system searches and displays the partitions on the hard disks. Press <C> to create a partition (that is, drive C). The partition is used to install the program files of Windows 2000 Server.
- 2) You are prompted to enter the capacity of the partition. Select the maximum value of the current system disk (about 8GB).
- 3) Press <Enter> to continue.
- 4) The capacity of drive C is displayed. Press <Enter> to continue.
- 5) You are prompted to select a file system format for the partition, as shown in Figure 2-10. Select the NTFS file system. Press <Enter> to continue.

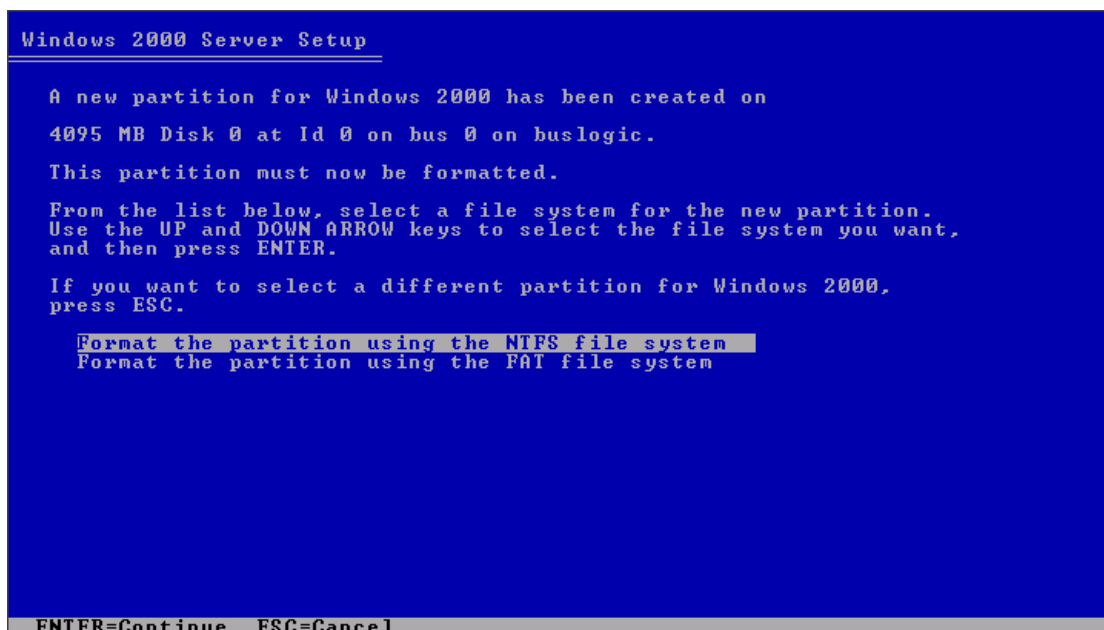


Figure 2-10 Selecting file system format

- 6) The system begins to format drive C. After the formatting, the system continues to copy the installation files. The copying progress bar is displayed in the middle of the screen.

VIII. Running the setup program and configuring the hardware

- 1) After the files are copied, the system is automatically restarted.
- 2) After the restart of the server, the setup program continues to run and the hardware is automatically configured. This takes about 10 minutes.

IX. Customizing country (region), language, and keyboard layout

In the [Regional Settings] dialog box, you are prompted to customize the country (region), language, and keyboard layout. See Figure 2-11. Select the default settings. Click <Next> to continue.

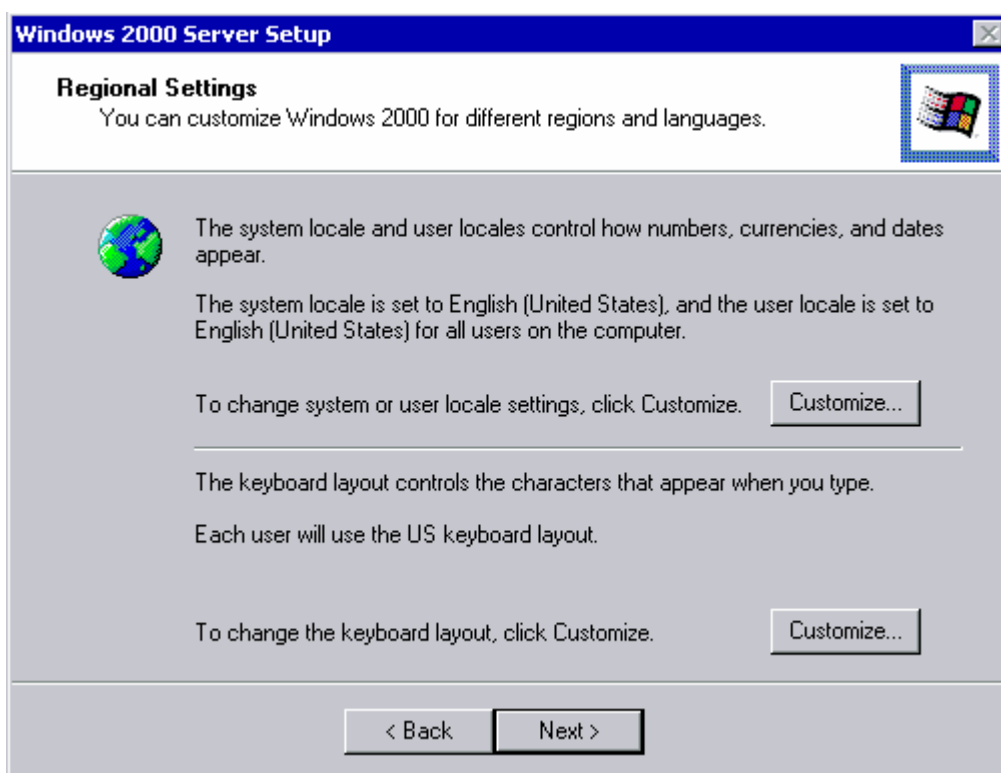


Figure 2-11 [Regional Settings] dialog box

X. Entering user information

In the [Personalize Your Software] dialog box, enter the username **“huawei”** in the [Name] box.

Enter the organization name **“Huawei Technologies Co., Ltd”** in the [Organization] box.

Click <Next> to continue.

XI. Entering the product key

In the [Your Product Key] dialog box as shown in Figure 2-12, enter the product key in the [Product Key] boxes. (The product key is printed on the Windows 2000 Server CD or user manual.) Click <Next> to continue.

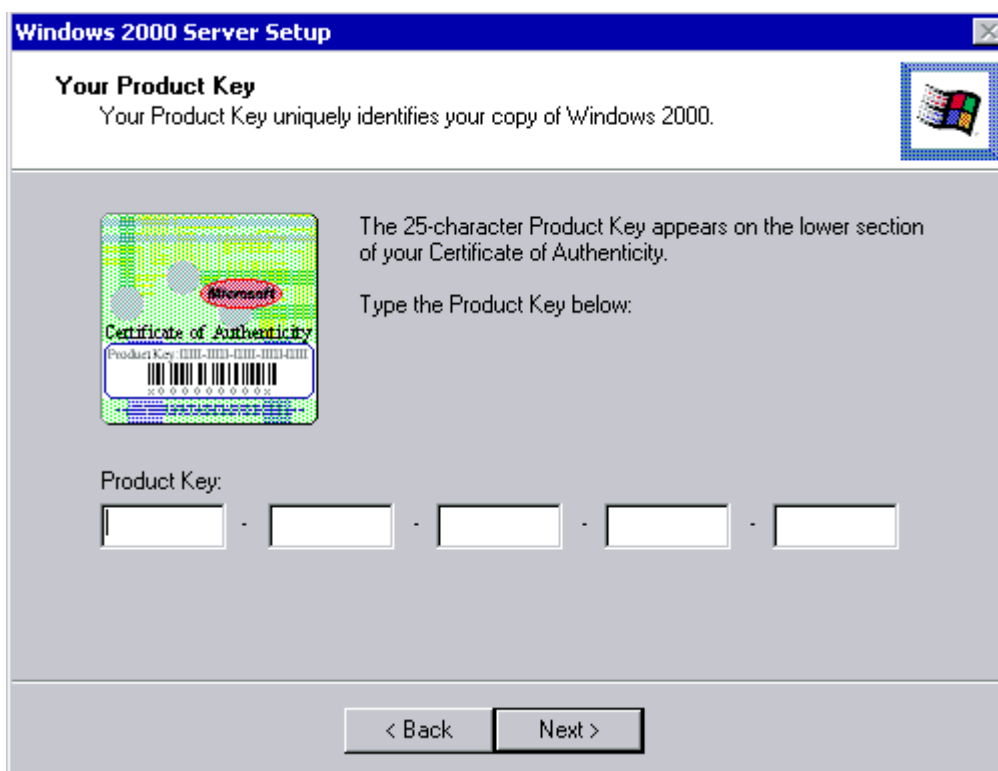


Figure 2-12 [Your Product Key] dialog box

XII. Setting the license mode

In the [License Modes] dialog box, select “Per server”.

Enter “5” of allowed users.

Click <Next> to continue.

XIII. Setting the computer name and the administrator password

In the [Computer Name and Administrator Password] dialog box, enter the computer name and the administrator password.

The preceding information has been preset as follows before the delivery:

- The computer name of the active iGWB server is set to “iGWB0”. The computer name of the standby iGWB server is set to “iGWB1”.
- The administrator password is set to “igwb”.

Click <Next> to continue.

XIV. Selecting Windows 2000 components

In the [Windows 2000 Components] dialog box as shown in Figure 2-13, select the Windows 2000 components to be installed. In this case, use the default settings. Click <Next> to continue.

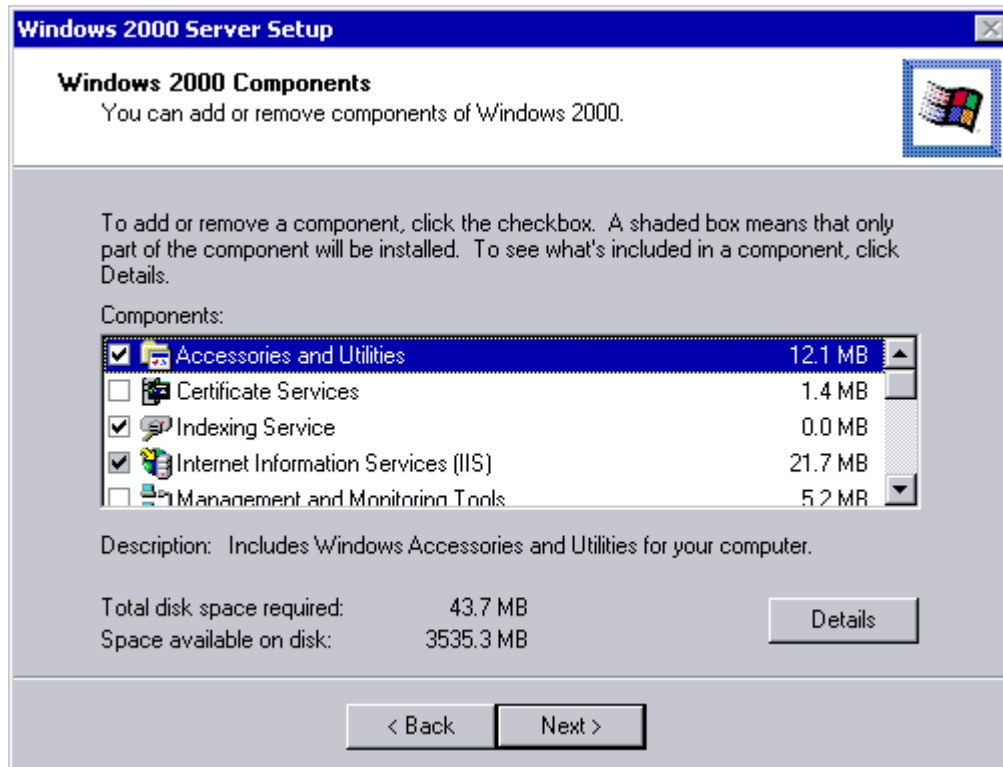


Figure 2-13 [Windows 2000 Components] dialog box

XV. Setting the date and time

In the [Date and Time Settings] dialog box as shown in Figure 2-14, set the current date and time. Click <Next> to continue.

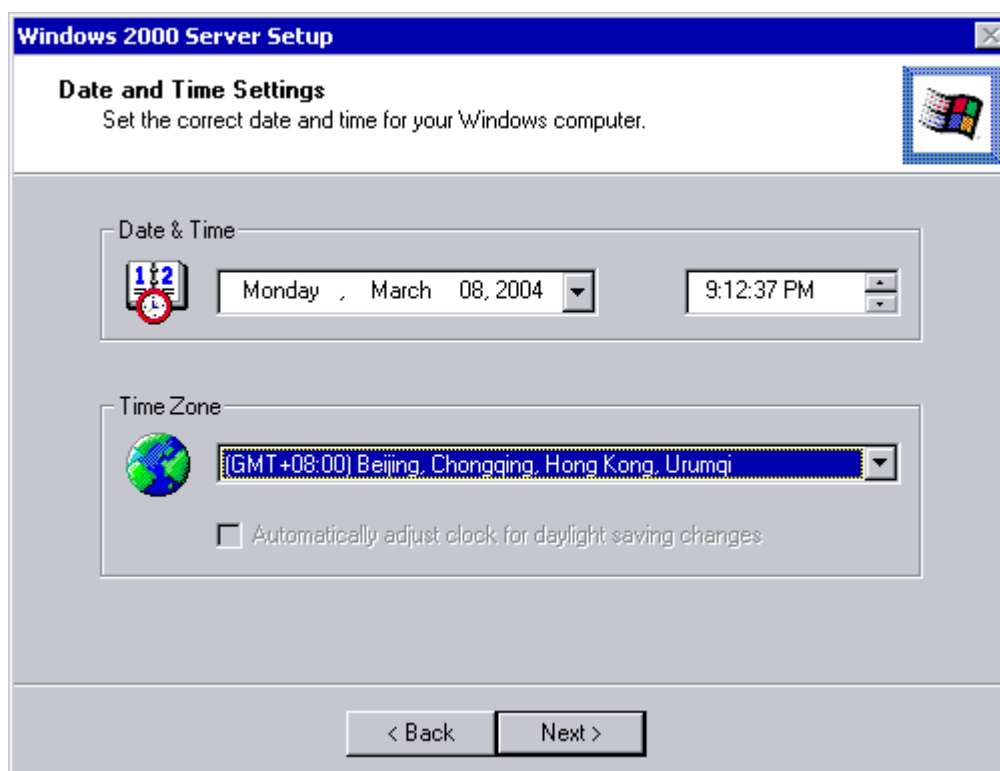


Figure 2-14 [Date and Time Settings] dialog box

XVI. Continuing the installation

The system continues the installation, including setting the network, installing the program components, setting the start menu, registering the program components, saving the configurations, and deleting the temporary files. This takes about 20 minutes.

XVII. Completing the installation

After the preceding installation, a prompt dialog box is displayed. Click <Finish> to complete the installation. The system will be restarted.

XVIII. Removing the CD and setting to boot the server from hard drive

- 1) After the server is restarted, remove the Windows 2000 Server CD from the CD-ROM drive.
- 2) Set the server to boot from the hard drive. In other words, set the first boot device to "Hard Drive".

Now, the installation of Windows 2000 Server is completed.

2.3.3 Installing Windows 2000 Service Pack 4

I. Overview of Installing Windows 2000 Service Pack 4

To ensure the security and the normal operation of the iGWB, you have to install the service pack 4 of Windows 2000 server.

II. Initializing setup

Proceed as follows:

Put the "Microsoft Windows 2000 Service Pack 4" CD into CDROM.

Double-click the file W2KSP4-EN.exe.

The setup wizard starts verifying files in the installation process, as shown in Figure 2-15.

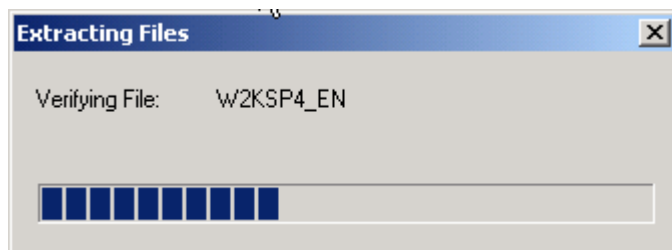


Figure 2-15 Extracting files

After the verification completes, the welcome dialog box appears as shown in Figure 2-16.



Figure 2-16 Welcome dialog box

Click <Next>.

III. Confirming license agreement

The [License Agreement] dialog box appears as shown in Figure 2-17.

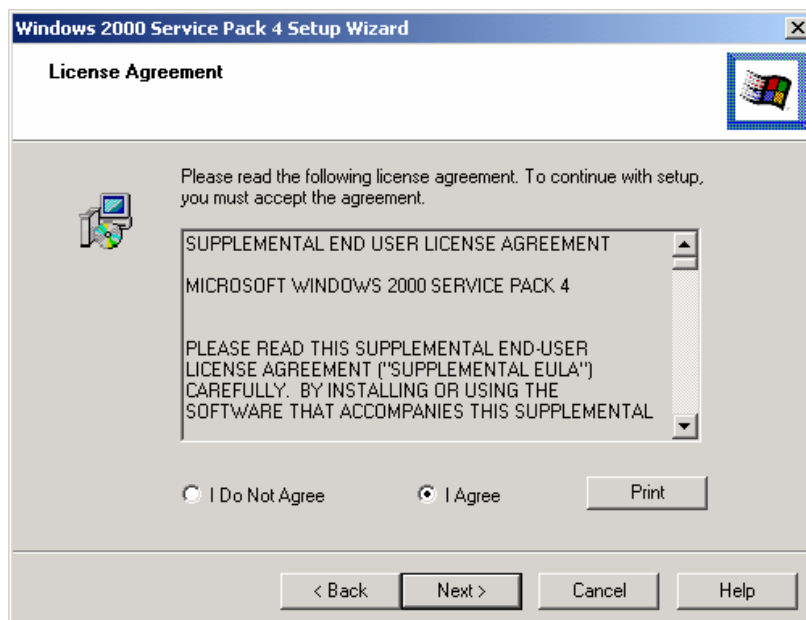


Figure 2-17 License agreement

Read it carefully, and proceed as follows:

Select [I Agree].

Click <Next>.

IV. Select options

The [Select Options] dialog box appears, as shown in Figure 2-18.

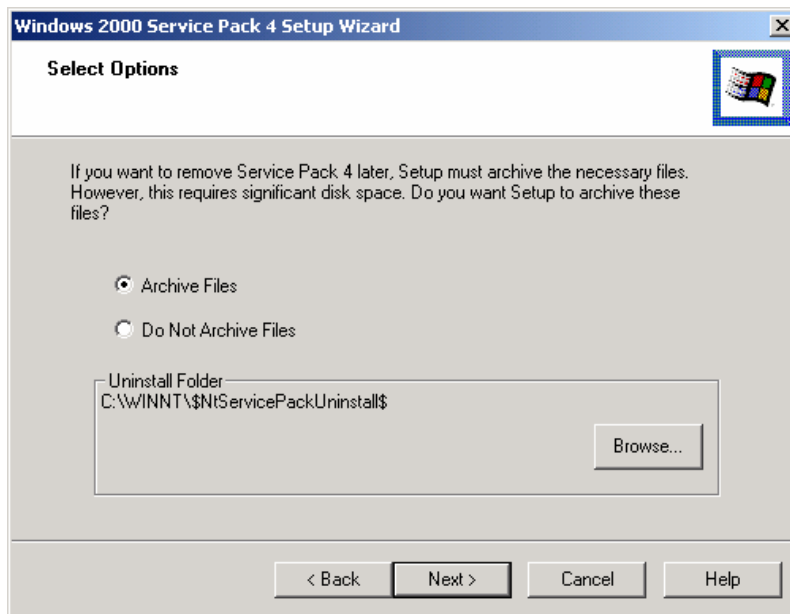


Figure 2-18 Select Options

Proceed as follows:

Select [Archive files]

Click <Next>.

V. Updating system

The setup wizard starts updating the system, as shown in Figure 2-19.

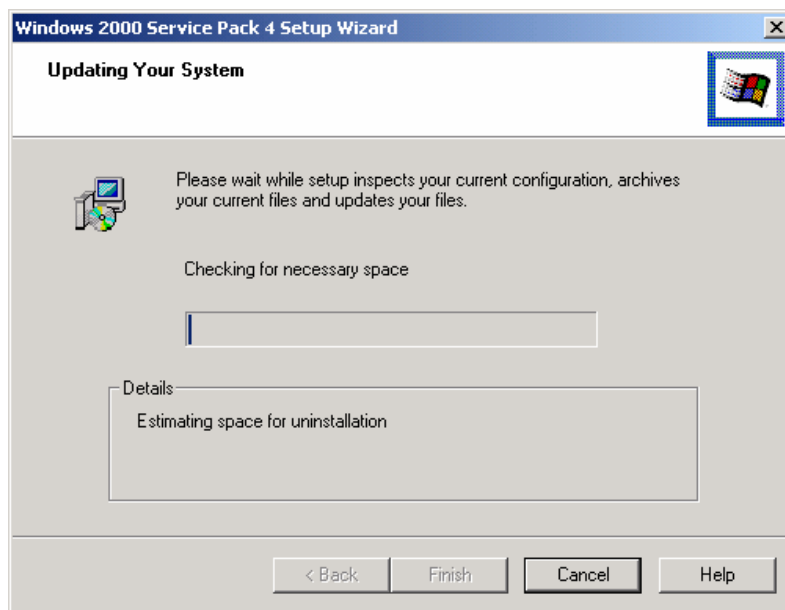


Figure 2-19 Updating your system

The installation covers three processes:

- Checking for necessary space
- Backing up files
- Installing files

The complete process takes about five minutes.

VI. Completing setup

After the updating process completes, the [Completing the Windows 2000 Service Pack 4 Setup Wizard] dialog box appears, as shown in Figure 2-20.



Figure 2-20 Completing the windows 2000 service pack 4 setup wizard

Click <Finish>.

The system will restart, and the installation of Windows 2000 service pack 4 is completed.

2.3.4 Installing Windows 2000 Hotpatches

I. Overview of installing Windows 2000 Hotpatches

To ensure the security of the iGWB, you need to install the following hotpatches (released by Microsoft) in sequence:

KB823980

KB824146

KB828741

KB828749

KB835732

KB837001



Caution:

- This section is for reference only. If possible, please refer to the release notice of the hotpatches on Microsoft homepage.
- Before installing the hotpatches, make sure that the Service Pack 4 has been installed.

II. Log in Windows 2000 Server as administrator

After you have installed Windows 2000 Server and Service Pack4, the iGWB will restart.

Log in as administrator.

III. Initializing setup

Proceed as follows:

Double-click the hotpatch file **Windows2000-KB823980-x86.exe**, a welcome dialog box appears as shown in Figure 2-21.

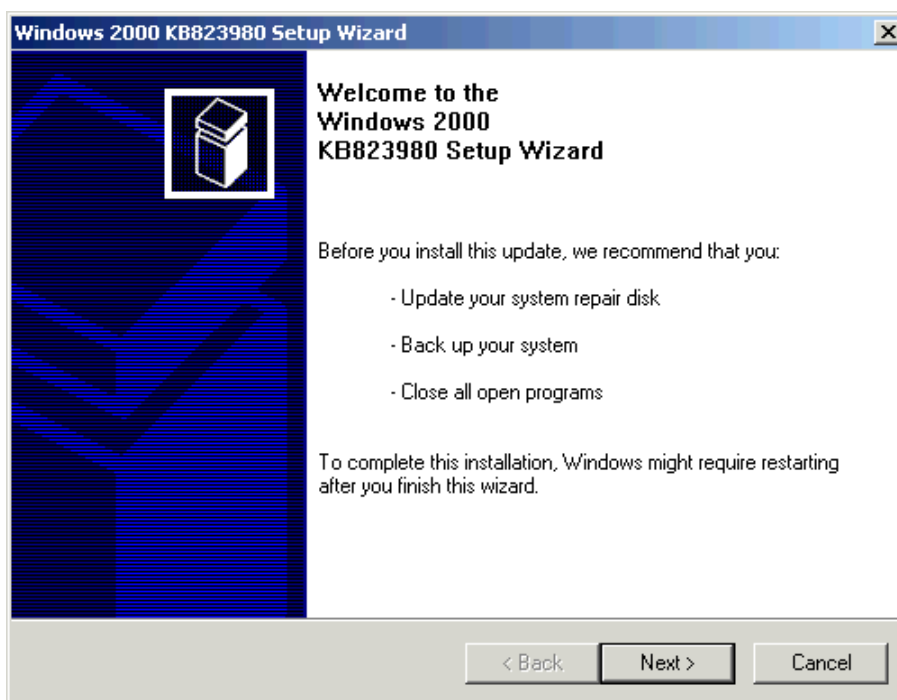


Figure 2-21 KB23980 Setup welcome dialog box

Click <Next>.

IV. Confirming license agreement

The license agreement dialog box appears as shown in Figure 2-22.

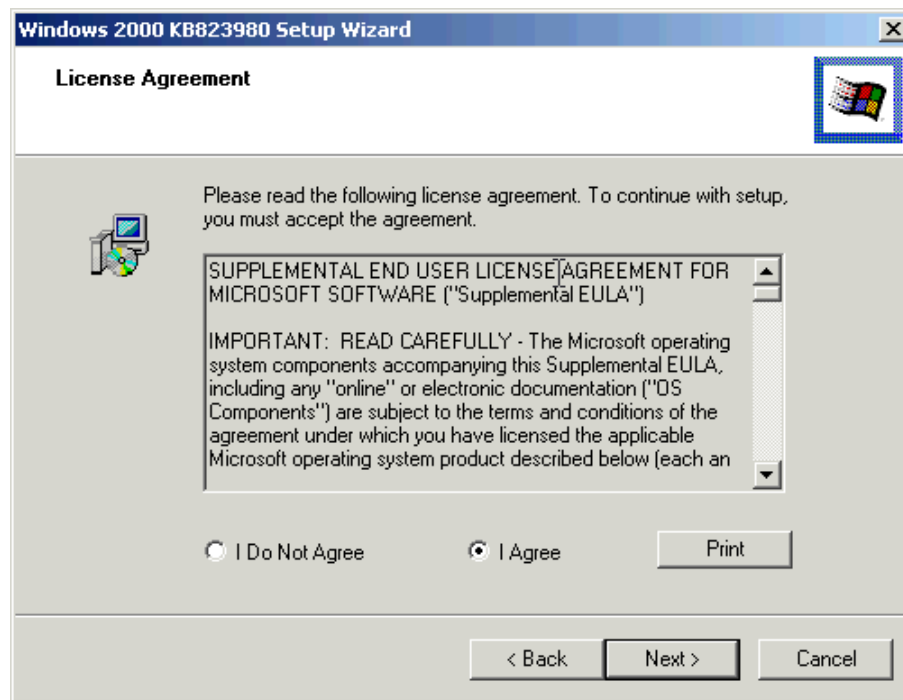


Figure 2-22 License agreement

Read it carefully, and proceed as follows:

Select [I Agree].

Click <Next>.

V. Updating your system

The setup wizard starts updating the system, as shown in Figure 2-23.

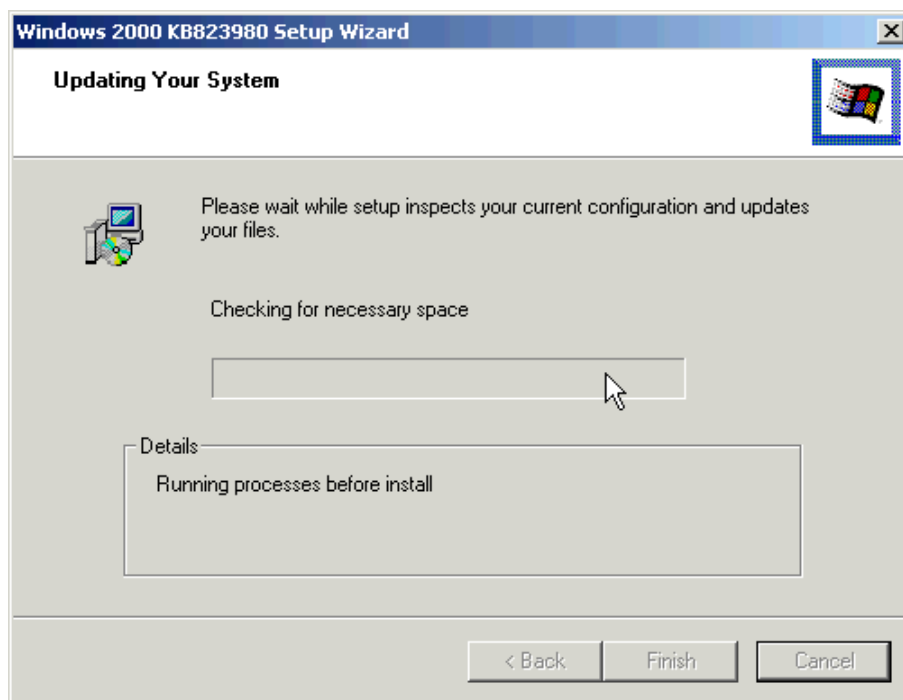


Figure 2-23 Updating your system

The hotpatch starts to update your system. The process will take some 30 seconds.

VI. Completing setup

After the updating process completes, the [Completing the Windows 2000 KB823980 Setup Wizard] dialog box appears, as shown in Figure 2-24.

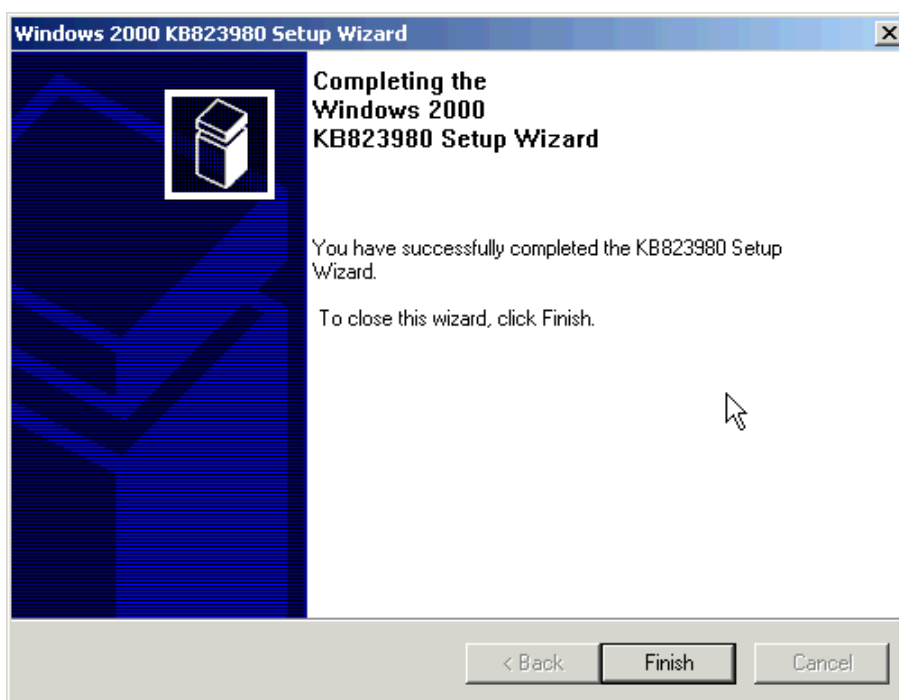


Figure 2-24 Completing the Windows 2000 KB823980 setup wizard

Repeat the above steps to complete the installation of other hotpatches.

2.3.5 Installing Drivers for iGWB Network Adapter and RAID Adapter

After Windows 2000 Server is installed, network adapter and RAID adapter should be installed for the iGWB server. Proceed as follows:

- 1) At the Windows 2000 Server desktop, right-click the My Computer icon. Select [Properties] from the shortcut menu. The [System Properties] dialog box is displayed.
- 2) In the [System Properties] dialog box, select the [Hardware] tab. See Figure 2-25.

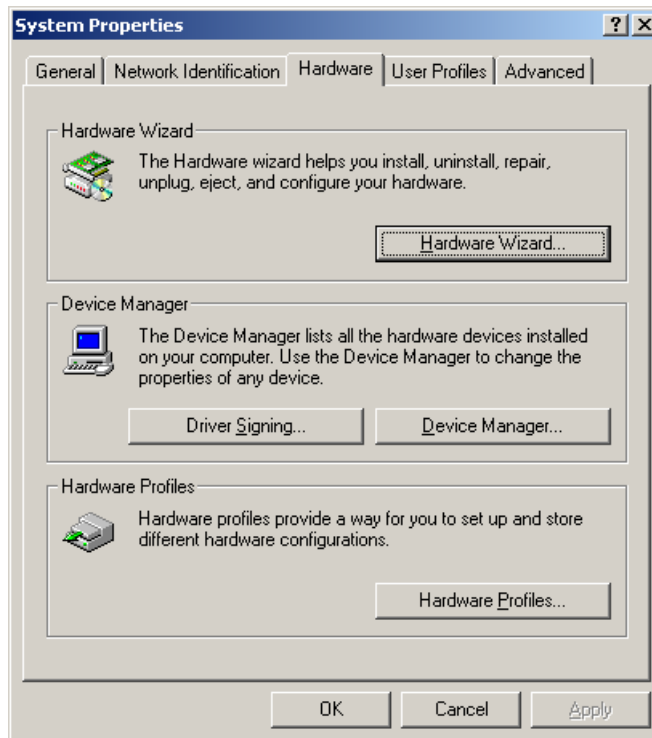


Figure 2-25 [System Properties] dialog box

- 3) Click <Device Manager...>. The [Device Manager] window is displayed. All Ethernet adapters and RAID adapters that are found but not operating well are displayed under the [Other devices] node. See Figure 2-26.

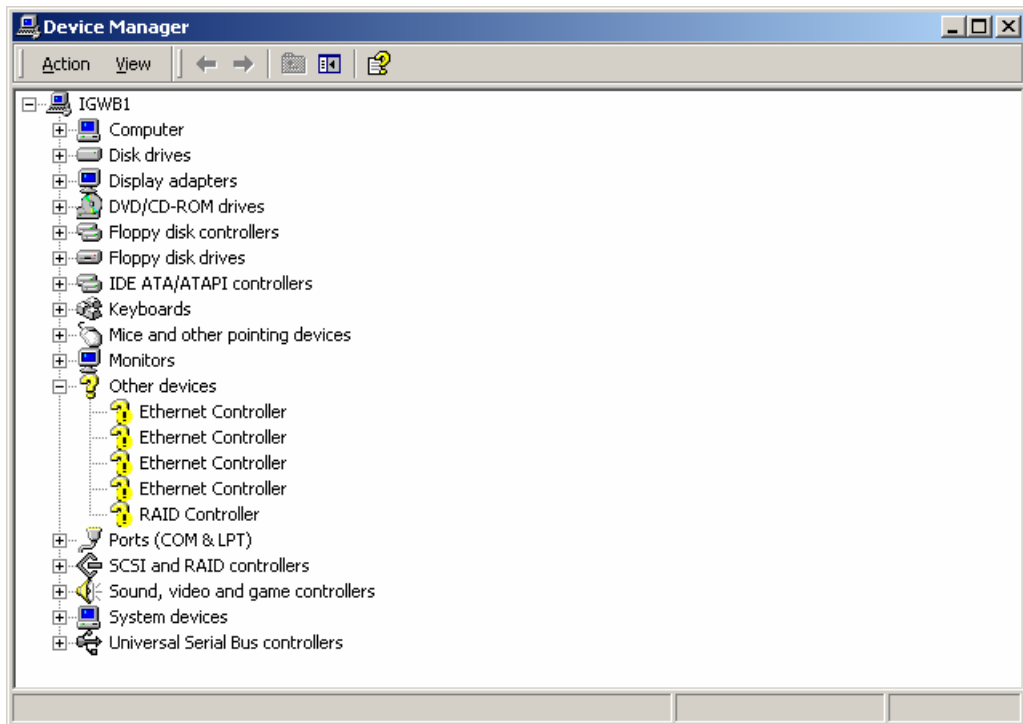


Figure 2-26 [Device Manager] window

- 4) Double-click a network adapter. The [Ethernet Controller Properties] dialog box is displayed. Select the [Driver] tab. See Figure 2-27.

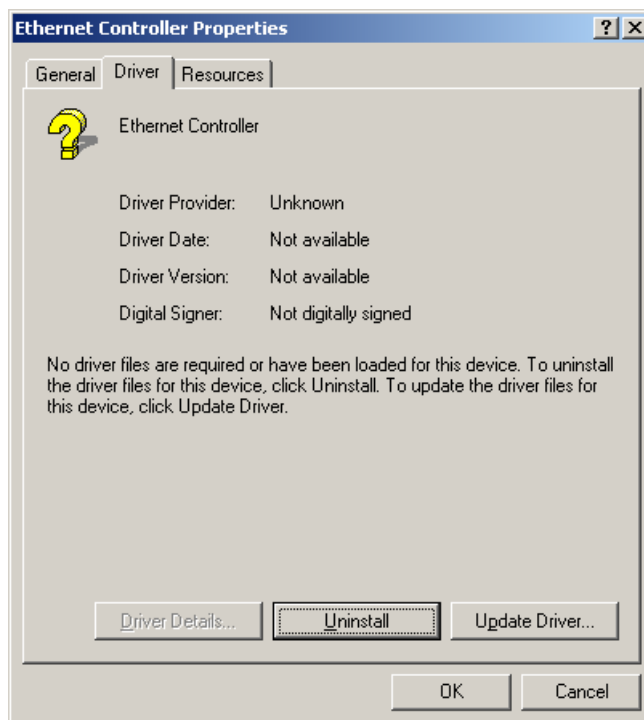


Figure 2-27 [Ethernet Controller Properties] dialog box

- 5) Click <Update Driver...>. The [Update Device Driver Wizard] dialog box is displayed. Click <Next> to continue. See Figure 2-28.



Figure 2-28 [Update Device Driver Wizard] dialog box

- 6) In the [Install Hardware Device Drivers] dialog box, select [Search for suitable driver for my device]. Click <Next> to continue. See Figure 2-29.

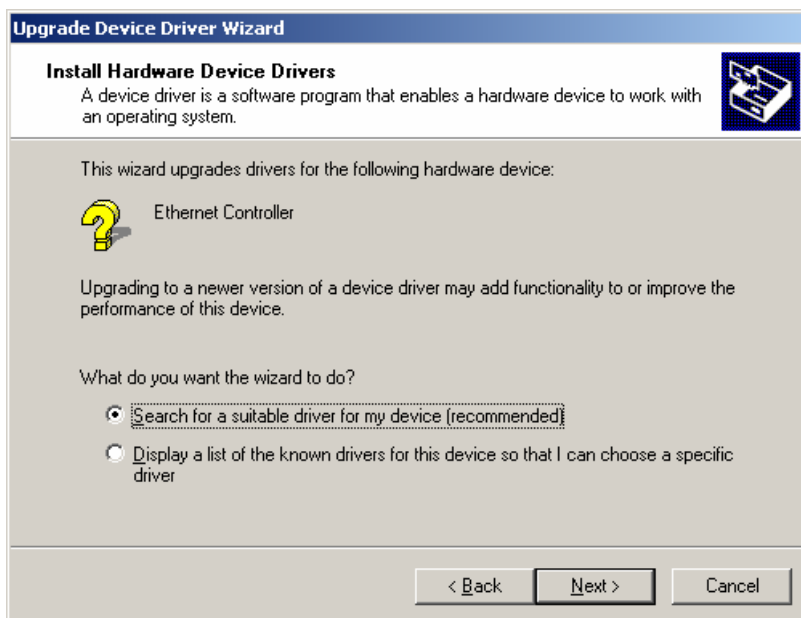


Figure 2-29 [Install Hardware Device Drivers] dialog box

- 7) In the [Locate Driver Files] dialog box, select [CD-ROM drivers] in the [Optional disk locations] area. Insert the network adapter driver CD into the CD-ROM drive. Click <Next> to continue. See Figure 2-30.

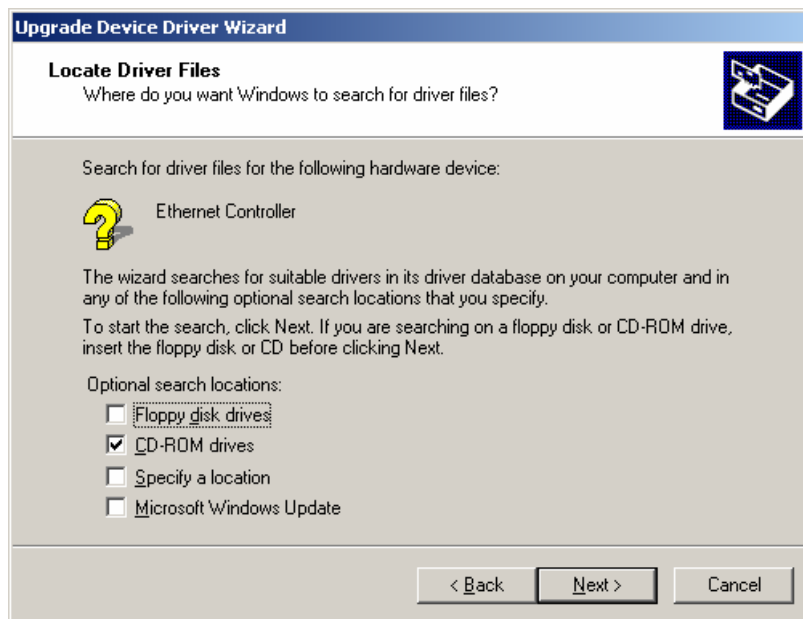


Figure 2-30 [Locate Driver Files] dialog box

- 8) The system searches the CD for the driver of the network adapter. The [Driver Files Search Results] dialog box is displayed with the path to the driver, for example, d:\neti557x.inf. Click <Next> to continue. See Figure 2-31.

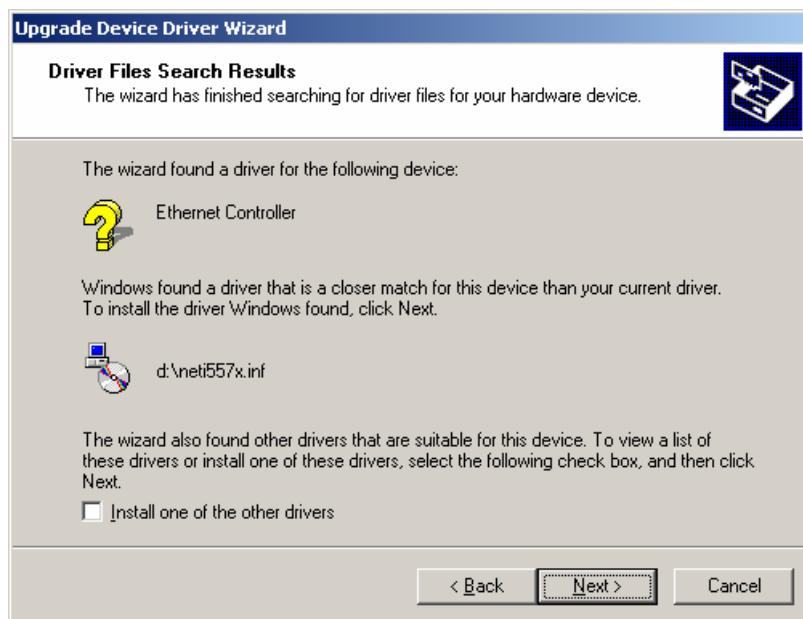


Figure 2-31 [Driver Files Search Results] dialog box

- 9) The system is installing the network adapter driver. After the installation, the [Update Device Driver Wizard] dialog box is displayed. Click <Finish> to complete the installation. See Figure 2-32.



Figure 2-32 [Update Device Driver Wizard] dialog box

10) The driver properties of the network adapter are displayed. See Figure 2-33.

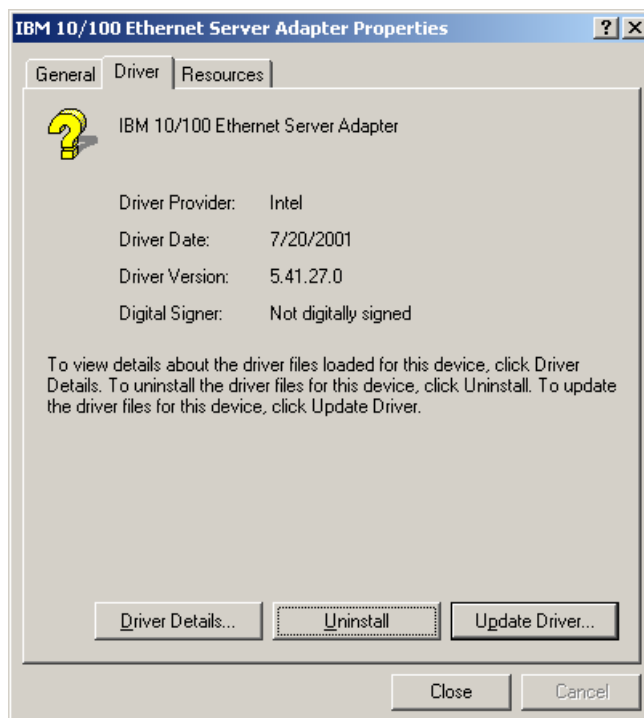


Figure 2-33 Adapter properties dialog box

Click <Close>. The driver of the network adapter is refreshed. Now, the installation of the driver of the first network adapter is completed.

- 11) Take the preceding steps to install the other network adapters and RAID adapter.

 **Note:**

- The installation process of the RAID adapter is the same as that of a network adapter, except that in the [Locate Driver Files] dialog box the floppy disk should be selected for searching the required driver.
 - The RAID adapter must have been installed before the hard disks are partitioned; otherwise, the hard disks in the array cannot be identified.
-

2.3.6 Partitioning iGWB Hard Disk

In consideration of the requirement of the iGWB server software on hard disk partitioning, the iGWB hard disks need be divided into three partitions. All the partitions should use the NTFS file system. It is recommended to set the letters of the partitions (logical drives) to “C”, “D”, and “E”, and the CD-ROM drive to “F”.

To ensure data security, the size of the partitions of the iGWB hard disks should be set to the following:

- Partition C: 8 GB, used to install the operating system and the iGWB server software.



Caution:

8 GB is allocated to drive C in the hard disk of the server (about 34 GB), and the left space (26 GB) is reserved for future use.

- Partition D: 105 GB, used to store the original bills, log files, and status files.
- Partition E: 105 GB, used to store the final bills and backup files.

According to the preceding requirements, you can use the disk management tool provided by Windows 2000 Server to partition the iGWB hard disks and set drive letters. To achieve that, proceed as follows:

I. Starting the Computer Management tool

- 1) At the Windows 2000 Server desktop, select [Start/Programs/Administrative Tools/Computer Management]. The [Computer Management] window is displayed, as shown in Figure 2-34.

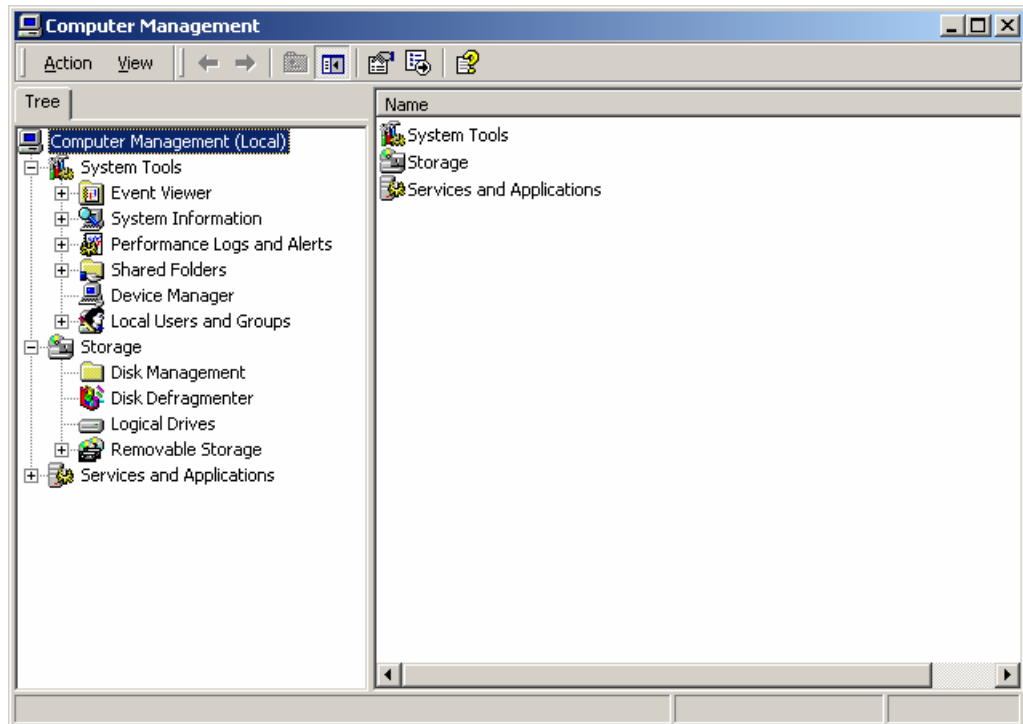


Figure 2-34 [Computer Management] window

- 2) As shown in Figure 2-34, select [Storage/Disk Management] in the tree pane. The partitions of the server are displayed in the right pane.

II. Changing driver letters

- 1) Right-click in the CD-ROM drive area. Select [Change Drive Letter and Path] from the shortcut menu, as shown in Figure 2-35.

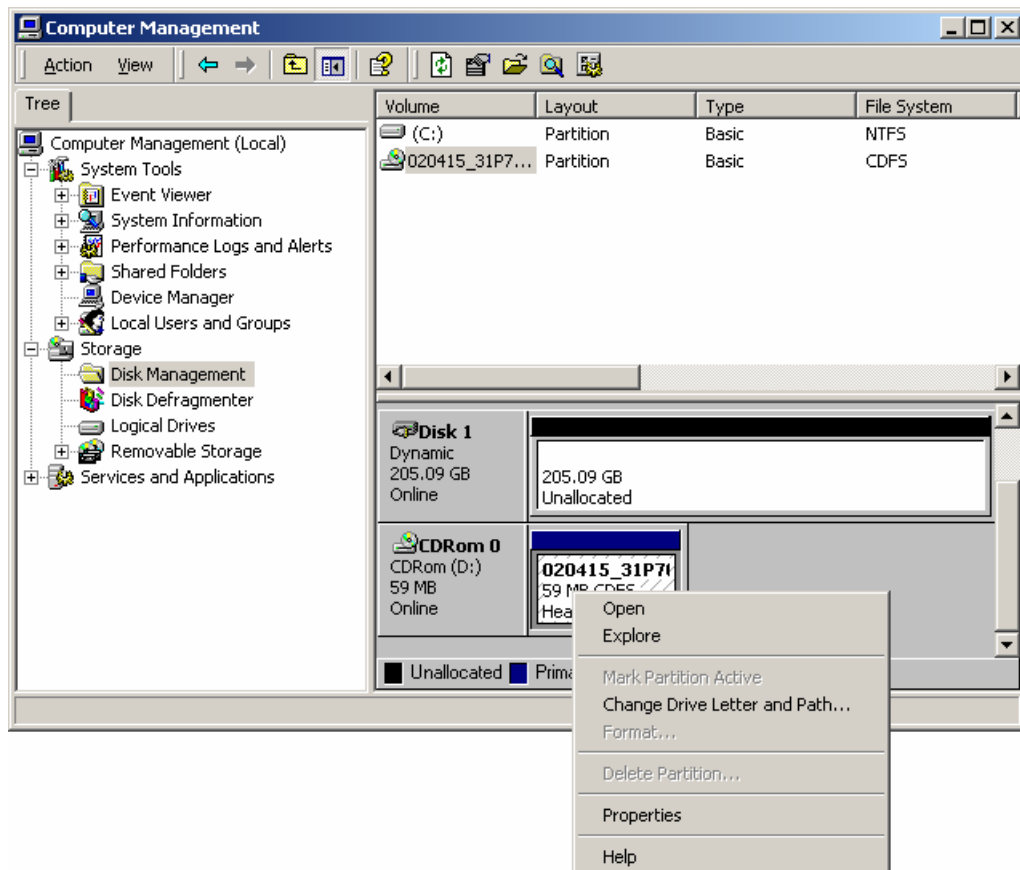


Figure 2-35 Right-click menu of CD-ROM drive

- 2) The [Change Drive Letter and Paths for (D:)] dialog box is displayed, as shown in Figure 2-36.

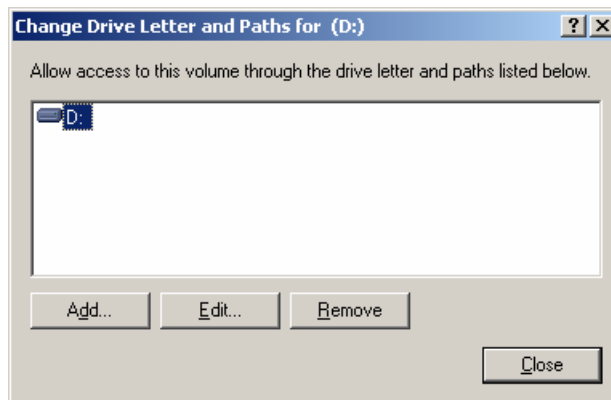


Figure 2-36 [Change Drive Letter and Paths for (D:)] dialog box

- 3) Click <Edit...>. The [Edit Drive Letter or Path] dialog box is displayed. Assign "F:" to the CD-ROM drive. Click <OK>. See Figure 2-37.

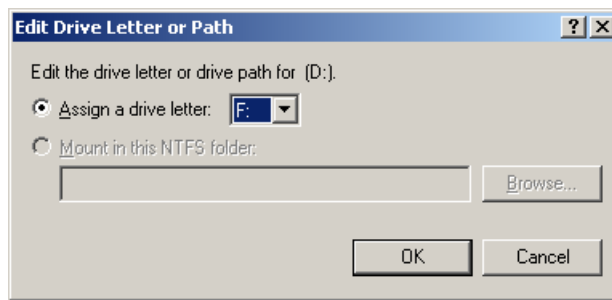


Figure 2-37 [Edit Drive Letter or Path] dialog box

- 4) The [Confirm] dialog box is displayed. Click <Yes>. See Figure 2-38.

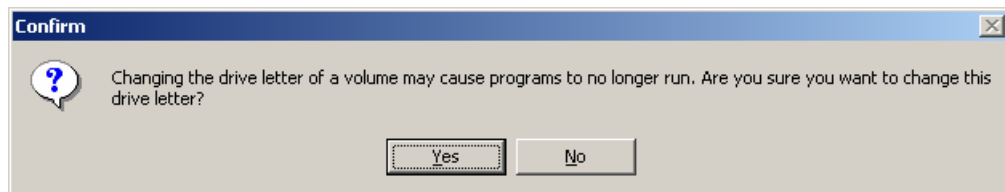


Figure 2-38 [Confirm] dialog box

III. Creating an extended partition

- 1) As shown in Figure 2-35, right-click in the [Unallocated] area in [Disk 1]. See Figure 2-39.

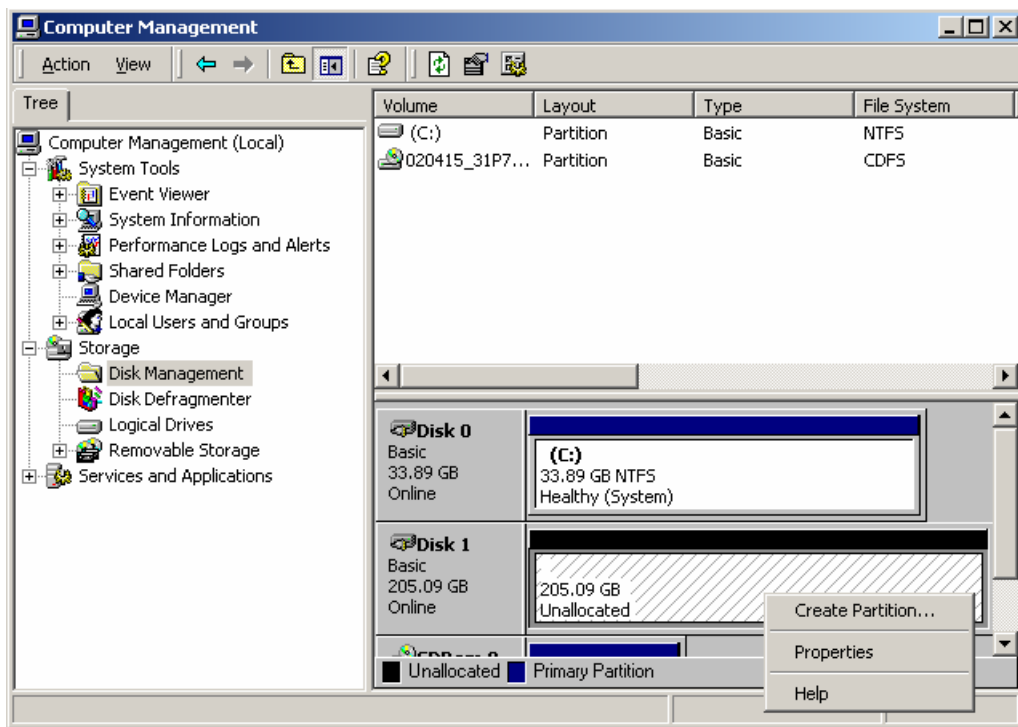


Figure 2-39 Creating extended partition

- 2) Select [Create Partition] from the shortcut menu. The [Create Partition Wizard] dialog box is displayed. Click <Next> to continue. See Figure 2-40.

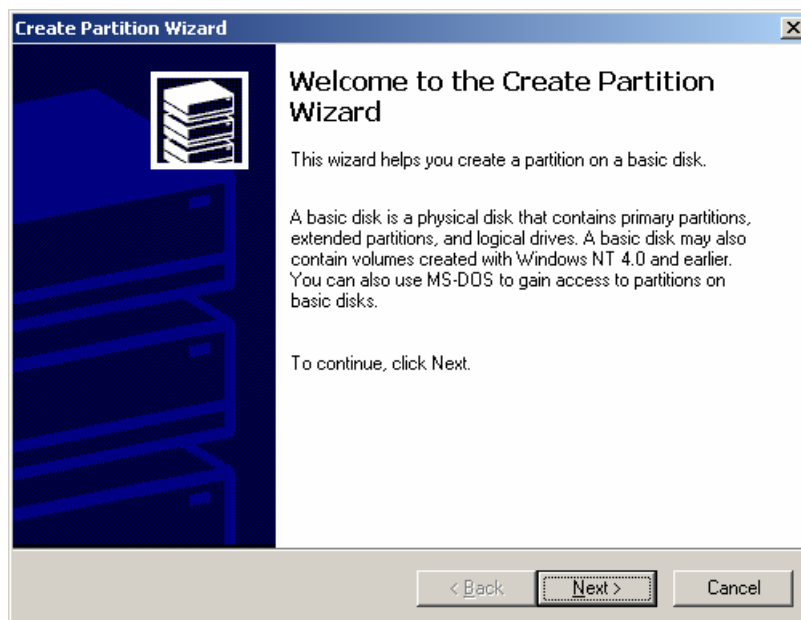


Figure 2-40 [Create Partition Wizard] dialog box

IV. Selecting the type of partition

In the [Select Partition Type] dialog box, select [Extended partition] to be the type of the partition. Click <Next> to continue. See Figure 2-41.

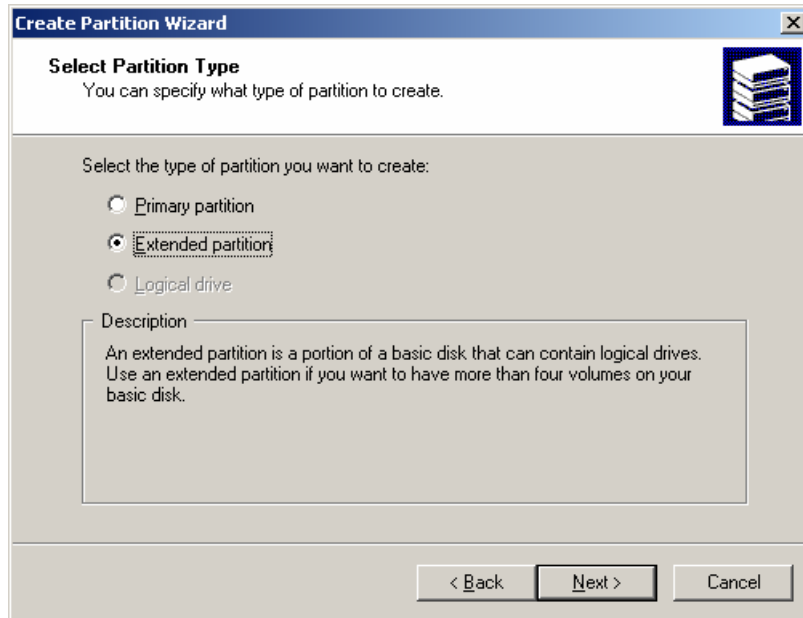


Figure 2-41 [Select Partition Type] dialog box

V. Specifying the partition size

In the [Specify Partition Size] dialog box, retain the default value, that is, the maximum disk space available. Click <Next> to continue. See Figure 2-42.

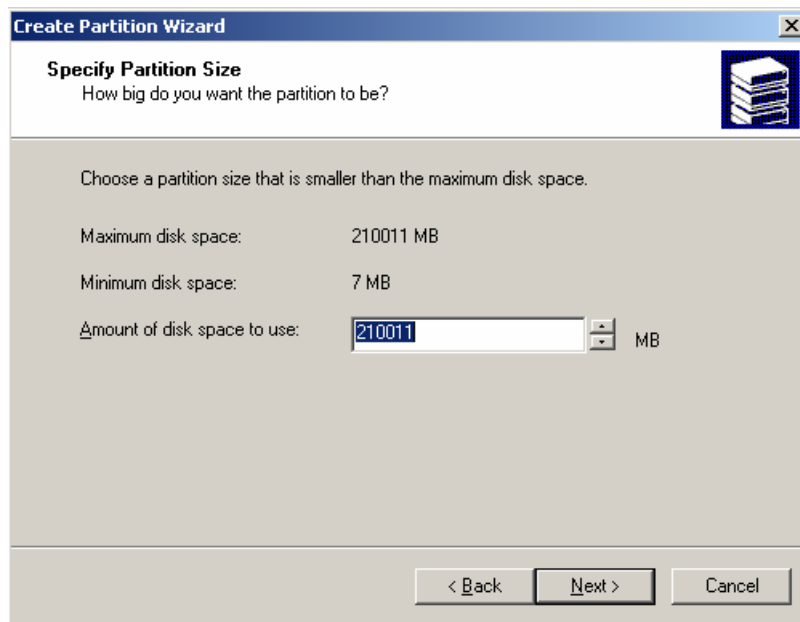


Figure 2-42 [Specify Partition Size] dialog box

VI. Completing the partition creation

- 1) The [Completing the Create Partition Wizard] dialog box is displayed, as shown in Figure 2-43.

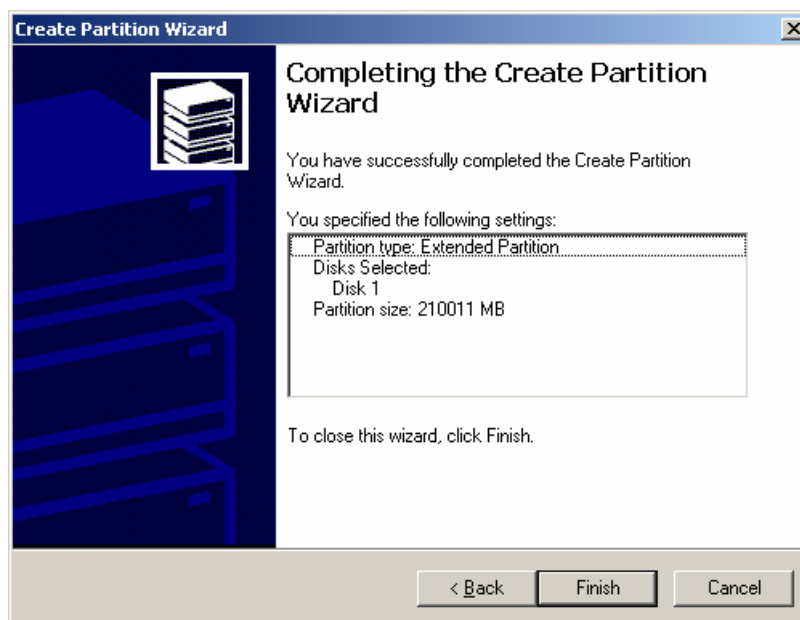


Figure 2-43 [Completing the Create Partition Wizard] dialog box

- 2) Confirm the displayed information. Click <Finish> to complete the partition creation. The [Unallocated] area status of [Disk 1] changes into "Free Space".

VII. Creating a logical drive

Right-click in the [Free Space] area of [Disk 1]. Select [Create Logical Drive] from the shortcut menu. The [Create Partition Wizard] is started. Click <Next> to continue. See Figure 2-44.

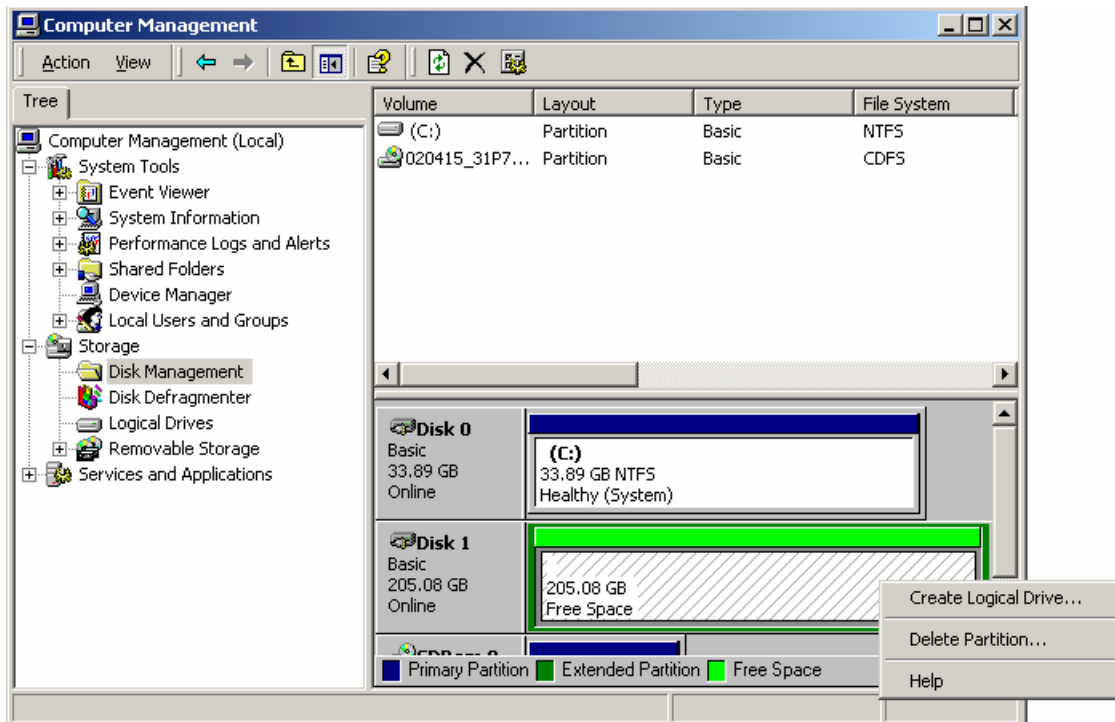


Figure 2-44 Creating logical drive

VIII. Selecting the type of partition

In the [Select Partition Type] dialog box, [Logical drive] is automatically selected to be the type of the partition. Click <Next> to continue. See Figure 2-45.

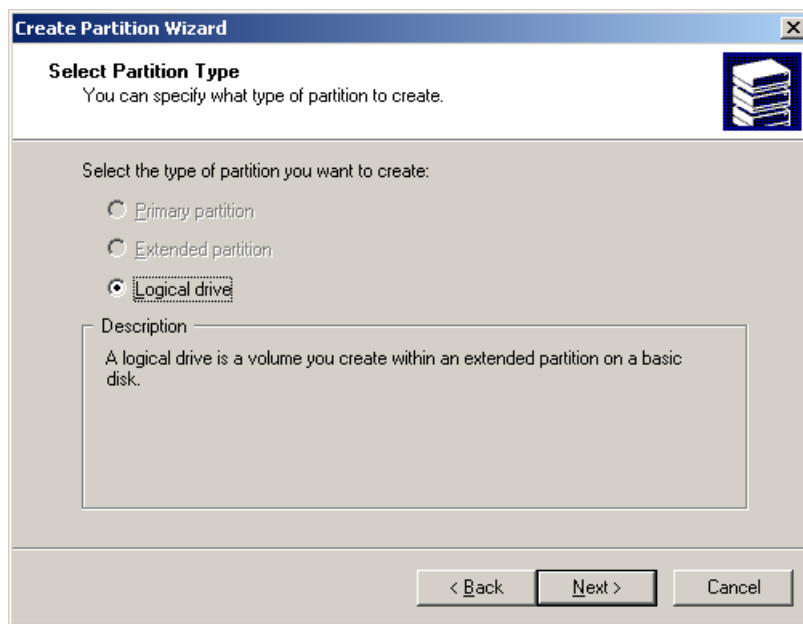


Figure 2-45 [Select Partition Type] dialog box

IX. Specifying the partition size

In the [Specify Partition Size] dialog box, enter "105001" in the [Amount of disk space to use] box. Click <Next> to continue. See Figure 2-46.

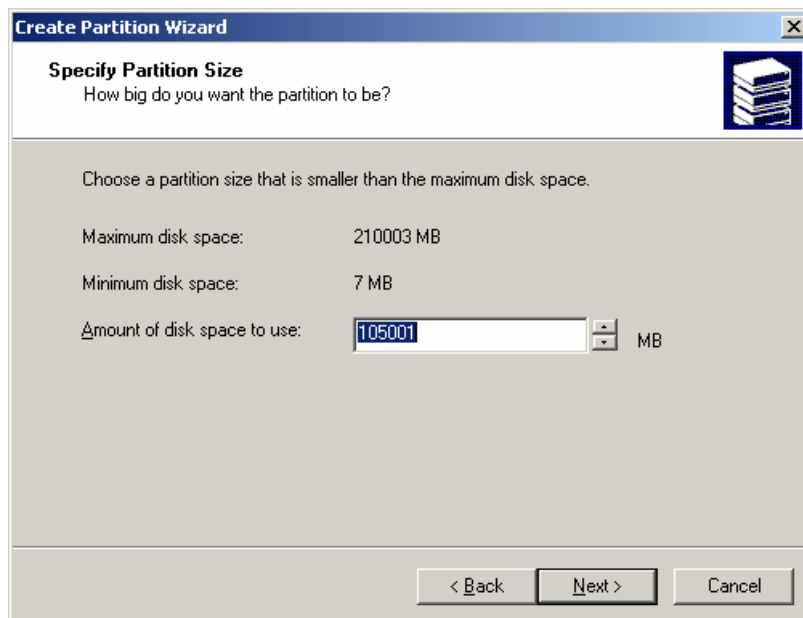


Figure 2-46 [Specify Partition Size] dialog box

X. Assigning a drive letter or path

In the [Assign Drive Letter or Path] dialog box, assign “D:” to the logical drive. Click <Next> to continue. See Figure 2-47.

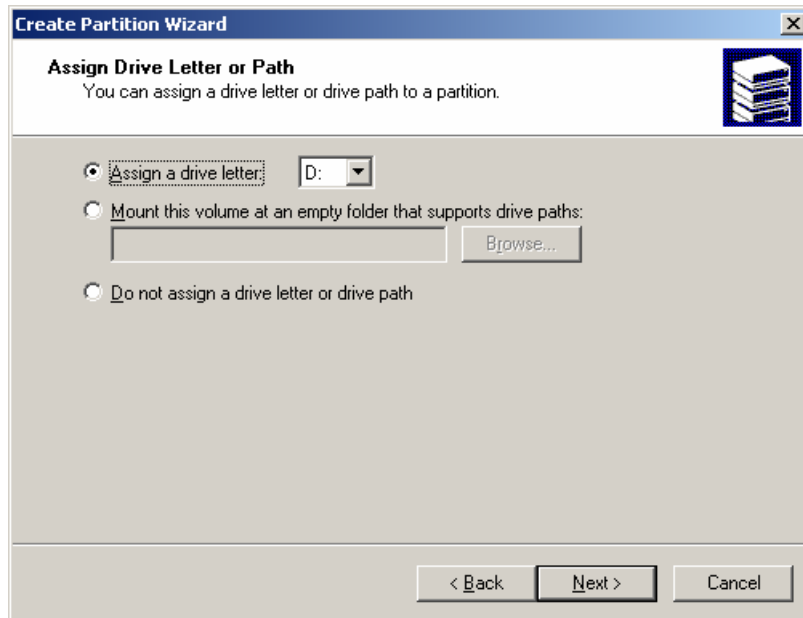


Figure 2-47 [Assign Drive Letter or Path] dialog box

XI. Formatting the partition

In the [Format Partition] dialog box, select [Format this partition with the following settings:] and [Perform a Quick Format]. Retain the default settings for the other parameters. Click <Next> to continue. See Figure 2-48.

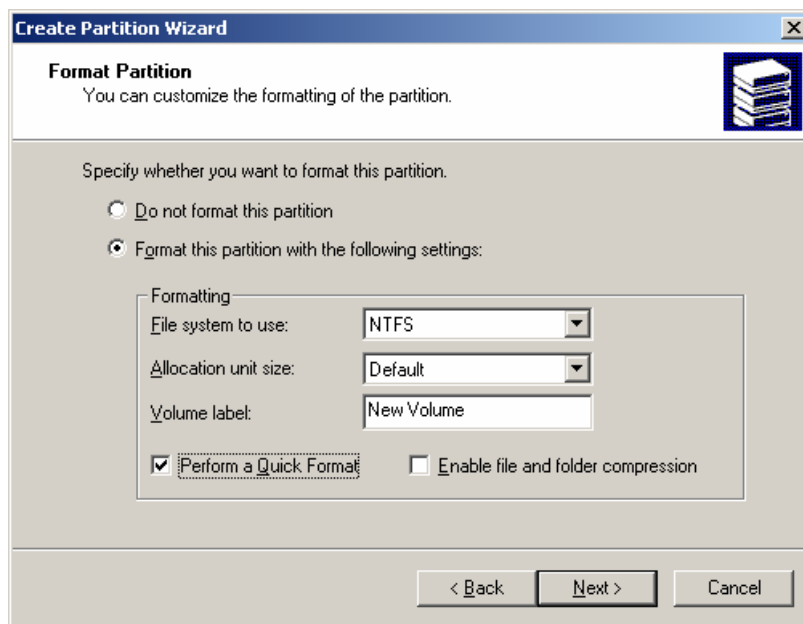


Figure 2-48 [Format Partition] dialog box

XII. Completing the creation of the logical drive

In the [Completing the Create Partition Wizard] dialog box, confirm the preceding settings and click <Finish> to complete the creation of the logical drive. See Figure 2-49.

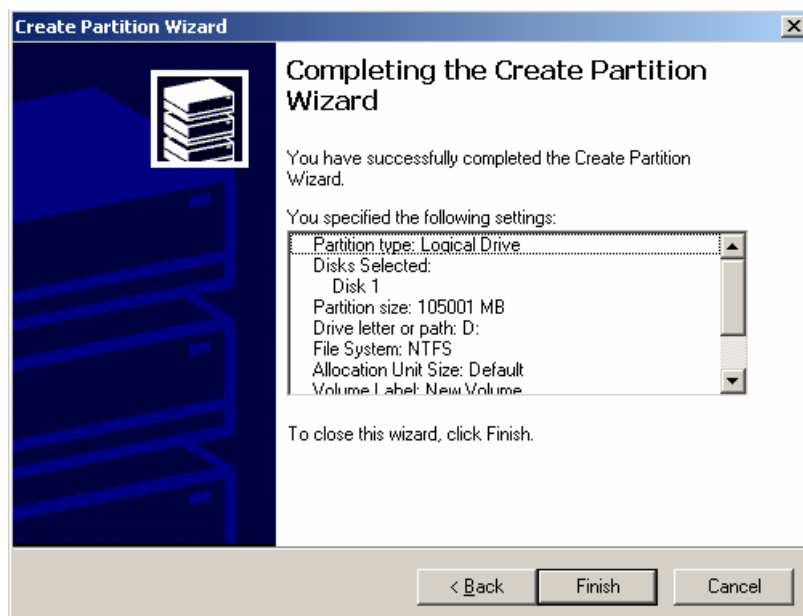


Figure 2-49 [Completing the Create Partition Wizard] dialog box

Drive D is automatically formatted. The creation of logical drive D is completed.

XIII. Creating another logical drive

Refer to the preceding steps to create logical drive E.

2.3.7 Setting IP Address for iGWB Network Adapter

The network ports are initially set to dynamically obtain IP addresses. You can assign an IP address for each network adapter according to the actual application. Setting of IP address depends on the actual situations at the site and the software installed. It is recommended to assign the following IP addresses for the network adapters as shown in Table 2-3.

Table 2-3 Assignment of IP addresses

Network adapter identifier	Connected device	IP address for active iGWB	IP address for standby iGWB	Virtual IP address
Netcard0 to 0#LAN Switch	Connected to the LAN Switch 0 for communication with the SoftX3000 on the active plane.	130.1.2.1	130.1.2.2	172.20.200.1
Netcard1 to 1#LAN Switch	Connected to the LAN Switch 1 for communication with the SoftX3000 on the standby plane.	130.1.3.1	130.1.3.2	172.30.200.1
Netcard2 to Office LAN	Connected to the bill console and NMS, also functioning as the first heartbeat path of the dual-system iGWB.	130.1.1.1	130.1.1.2	129.9.1.1
Netcard3 to Billing Center	Connected to the billing center, providing a billing interface.	130.1.4.1	130.1.4.2	/

The recommendations are the default values in the igwb.ini file. The IP addresses of the iGWB network adapters can also be differently planned with the following rules:

- The dual-system iGWB communicates with outside through the virtual IP address rather than the actual IP address of a network adapter.
- The IP address of the network adapter to the billing center must be negotiated with the billing center.
- The IP addresses must be consistent with those set in the igwb.ini file.

I. Confirming Working Status of All Network Adapters

Normally, the system automatically configures the driver for all network adapters after you install Windows 2003 Server successfully.

To verify the working status of the network adapters, proceed as follows.

- 1) At the Windows 2000 Server desktop, select [Start / Programs / Accessories / Communications / Network and Dial-up Connections]. The [Network and Dial-Up Connections] window appears, as shown in Figure 2-50.

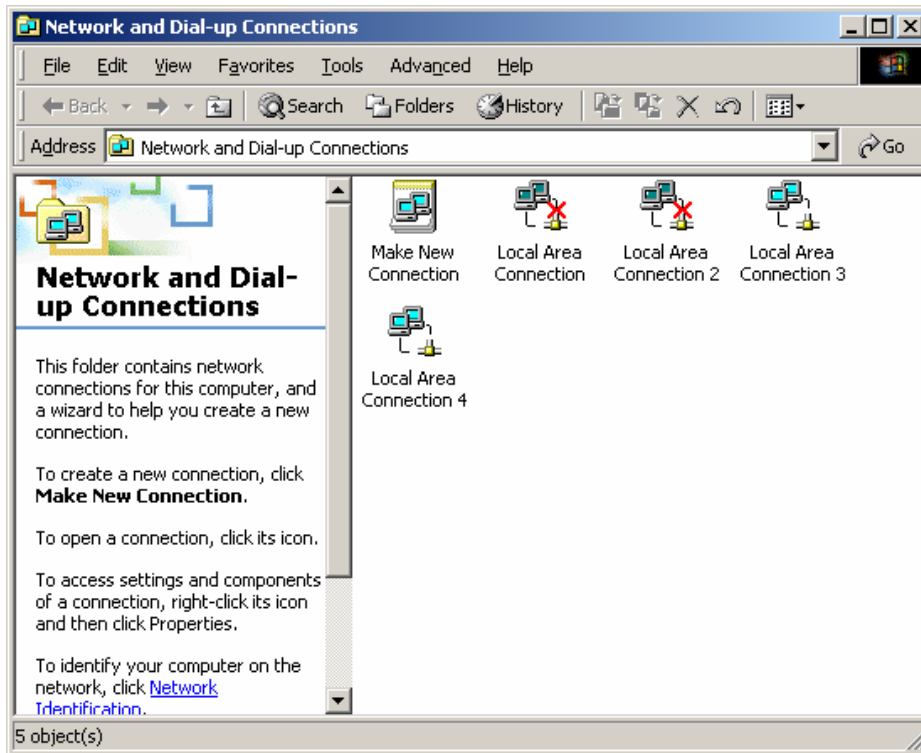

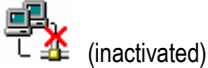


Figure 2-50 [Network and Dial-Up Connections] window

- 2) Check the network connections icons, as listed in Table 2-4

Table 2-4 Network connections icons

IF	THEN
The network connections icon is  (activated) or  (inactivated)	The network adapter is installed and can be used normally.
No corresponding icon is shown in the [Network and Dial-up Connections] window	The network adapter is not installed successfully. You need to reinstall the driver.


II. Checking and Reidentifying Network Adapters

The system also automatically searches for the network adapters and marks Local Area Connection, Local Area Connection 1, Local Area Connection 2, and Local Area Connection 3 orderly when installing the driver for iGWB network adapters.


The number sequence may be different from the actual physical numbering. Before configuring the IP addresses of iGWB network adapters. You must confirm the physical relationship between network adapters according to Figure 2-50, and identify network adapters again. In this way, you can identify network adapters correctly and prevent misoperations.

To achieve this purpose, proceed as follows:

Plug out all network cables connecting to iGWB network adapters. Then, the Local

Area Connection icons for all network adapter change into  (not activated).

Connect the corresponding network cable to the port of network adapter 3, and ensure that the Core LAN Switch 0 connecting with network adapter 3 is started. In this case, the “Local Area Connection” icon of one network adapter changes into

 (activated).

Right-click the activated icon, and select [Rename] from the shortcut menu to rename the network adapter to “Net Adapter 3 to Core LAN Switch 0”.

Identify the other three network adapters in the same way. It is recommended to name network adapter 1, 2 and 3 to Core LAN Switch 1, Office LAN and Billing System respectively.

III. Setting IP Address of Network Adapter 0

To assign an IP address, for example, 130.1.2.1 to the Network Adapter 0 to Core LAN Switch 0, proceed as follows.

At the Windows 2000 Server desktop, right-click the My Network Places icon. Select [Properties].

- 1) In the displayed windows, right-click [Local Area Connection]. Select [Properties].
- 2) Double-click [Internet Protocol (TCP/IP)]. Select [Use the following IP address]. Enter the following settings.
 - IP address 130.1.2.1
 - Subnet mask 255.255.255.0
 - Default gateway (Entered as required)
- 3) Click <OK> to complete the setting.

Repeat the preceding procedure to set the eight network adapters of the two servers.

2.3.8 Setting Automatic Logon to Windows 2000 Server

It is strongly recommended to set the automatic logon to Windows 2000 Server for security purposes. Proceed as follows:

- 1) Select [Start/Run]. In the displayed dialog box, enter "regedit" and press <Enter>. The [Registry Editor] window is displayed.
- 2) Select [HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows NT/CurrentVersion/Winlogon] in the navigation tree. Select [Edit/New/String Value] at the menu bar. Create a string of characters "AutoAdminLogon". Double-click the string. Assign "1" to it to enable the automatic logon.
- 3) Create a string of characters "DefaultUserName". Double-click the string. Enter the username for logon by default, for example, "Administrator".
- 4) Create a string of characters "DefaultPassWord". Double-click the string. Enter the password for logon by default. If those values exist, double-click and edit them.



Caution:

If no password is set, the automatic logon will fail.

After the setting, close the registry.

Now, the installation of the operating system of the server is completed.

2.4 Installing Billing Interface

The iGWB supports two types of online billing interfaces: FTP and FTAM. It is unnecessary to install both of them at the same time. In fact, only one set of interfaces is enough according to the design requirements.

Because the FTP server software is installed while Windows 2000 is installed, it is only required to configure the FTP server in this section. If the FTAM interface is used, the FTAM software must be installed and configured.

When the FTP interface is used, the iGWB serves as the FTP server, and the billing center as the FTP client. When the FTAM interface is used, the iGWB serves as the FTAM responder, and the billing center as the FTAM initiator.

2.4.1 Installing FTAM Protocol

UTS-FTAM 7.3 developed by Vertel is adopted as the FTAM protocol in the iGWB. It includes two sets of software: protocol stack software (UTS-NetLink 5.2) and application layer software (UTS-FTAM 7.2).

I. Applying for license

UTS-NetLink 5.2 and UTS-FTAM 7.2 use separate installation CDs and independent licenses. Each license is bound with the physical address (MAC address) of the corresponding network adapter. It might take 24 hours to apply for the licenses; therefore, application must be made in advance.

- 1) On each of the active and standby iGWB servers, run the command `C:\>ipconfig /all` to obtain the MAC address of the network adapter from the active/standby iGWB server to the billing center.
- 2) Send the MAC addresses (both of the servers must have their respective license) to `license@vertel.com`. The licenses will be obtained in one day.



Caution:

Do not send two or more MAC addresses of one server to the supplier, because it means two or more licenses are bought for the same server.

- 3) Receive the license e-mail from Vertel. The following is a license sample of Vertel:

```
SERVER snaylm 00065B24A878
VENDOR vertellm
INCREMENT UTSftam vertellm 1.9999 30-jul-2002 4 F3A2A3EB13BA ck=129 \
SN=200003150434

INCREMENT UTS-TCP vertellm 5.9999 30-jul-2002 uncounted C51951682126 \
HOSTID=00065B24A878 ck=129 SN=200003150434

INCREMENT UTS-LAN vertellm 5.9999 30-jul-2002 uncounted 807A7126DB50 \
HOSTID=00065B24A878 ck=129 SN=200003150434
```

The first four lines are the contents of the UTS_FTAM license. The latter four lines are the contents of the UTS_NetLink license. For the UTS_FTAM license, `snaylm` should be replaced with the host name in actual installation. The usage of the license file will be described in the subsequent installation steps in detail.

II. Installing UTS-NetLink 5.2

- 1) Insert the UTS-NetLink 5.2 CD into the CD-ROM drive. Double-click Setup.exe. A setup message is displayed, as shown in Figure 2-51.

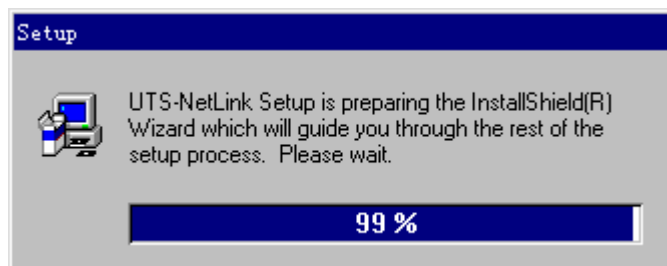


Figure 2-51 Setup message

- 2) After the InstallShield Wizard is prepared, the [Welcome] dialog box is displayed. Click <Next>. The [Software License Agreement] dialog box is displayed, as shown in Figure 2-52.

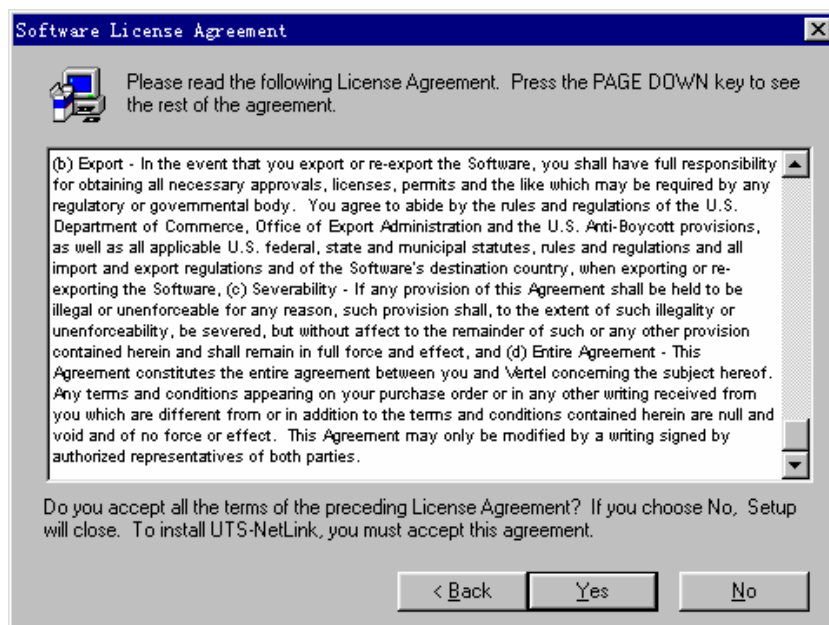


Figure 2-52 [Software License Agreement] dialog box

- 3) Click <Yes> to accept the agreement. The [Choose Destination Location] dialog box is displayed, as shown in Figure 2-53.

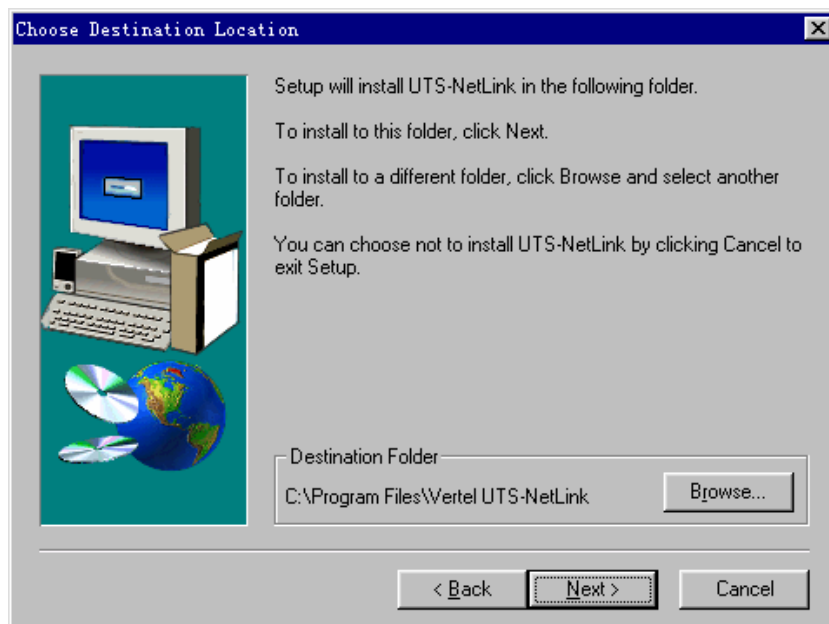


Figure 2-53 [Choose Destination Location] dialog box

- 4) Click <Browse> to select a destination folder. The default destination folder is recommended. Click <Next>. The [Select Program Folder] dialog box is displayed, as shown in Figure 2-54.

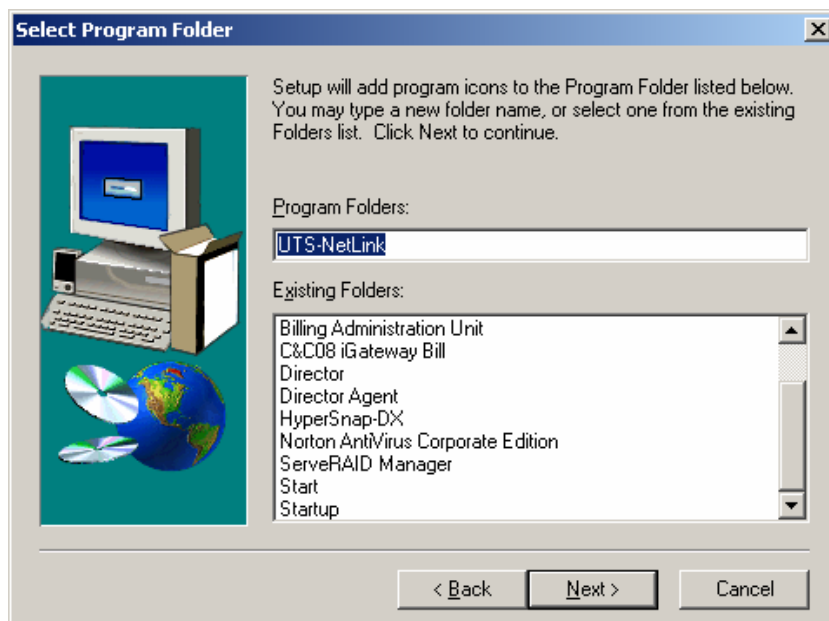


Figure 2-54 [Select Program Folder] dialog box

- 5) Click <Next>. The [Start Coping Files] dialog box is displayed. Click <Next>. The InstallShield Wizard starts copying files.

- 6) After the files are copied, the [UTS-NetLink Configuration] dialog box is displayed. Click <Next>. The [Configuration Applet] dialog box is displayed, as shown in Figure 2-55.

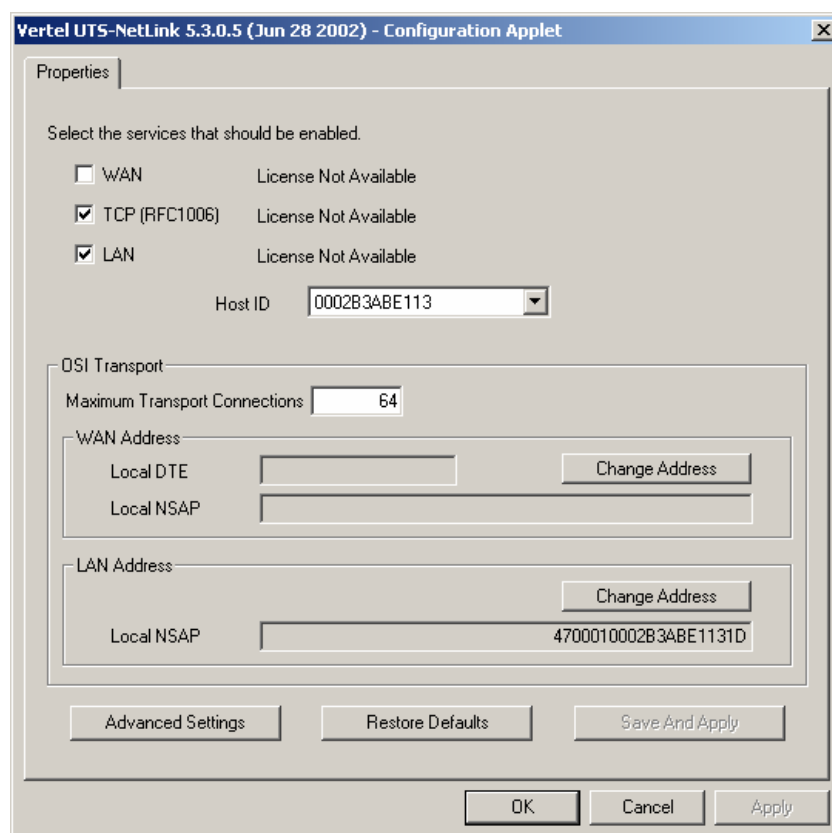


Figure 2-55 [UTS-NetLink Configuration] dialog box

- 7) Set the required parameters of the network adapter such as local NSAP. The default settings are recommended.
- 8) (After the installation, you can select [Start/Setting/Control Panel] and double-click Vertel UTS-NetLink in the control panel to open this configuration dialog box to change or view the settings.) Click <OK>. The [Network Configuration] dialog box is displayed. Click <Next>. The InstallShield Wizard automatically configures the network components. After the configuration, the [Setup Complete] dialog box is displayed, as shown in Figure 2-56.

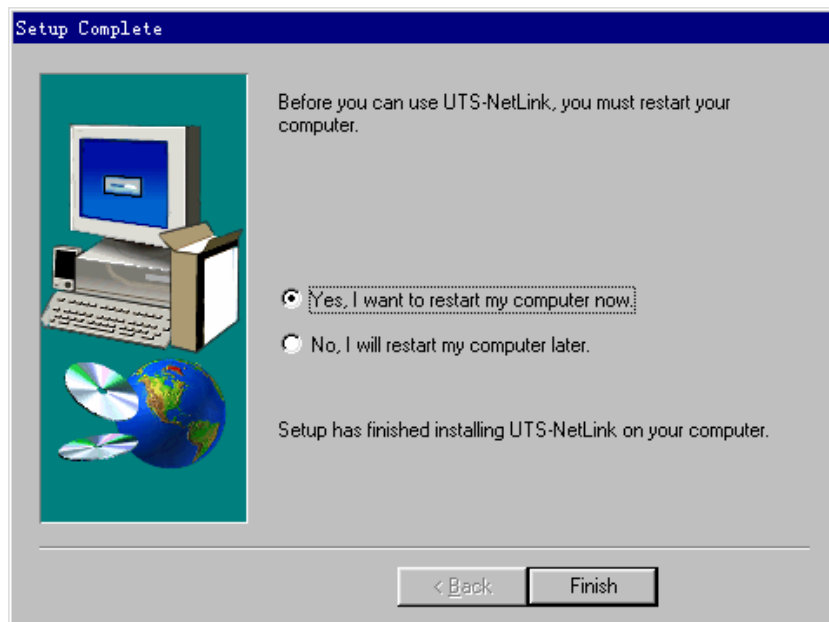


Figure 2-56 [Setup Complete] dialog box

- 9) Select [No, I will restart my computer later]. Click <Finish>.
- 10) The UTS-NetLink license is copied to C:\Program Files\Vertel UTS-NetLink\etc\license.dat. Save the file. Close the file. The installation of the UTS-NetLink 5.2 is completed.

III. Installing UTS-FTAM 7.2

- 1) Insert the UTS-FTAM 7.2 CD into the CD-ROM drive. Double-click Setup.exe. A setup message is displayed, as shown in Figure 2-57.

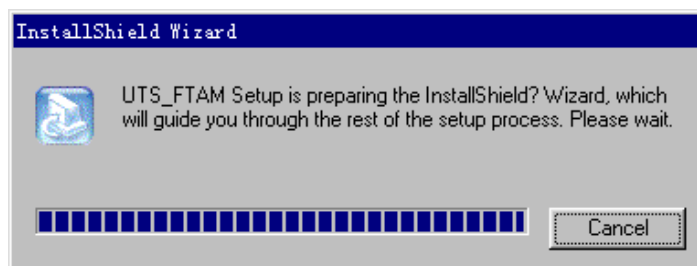


Figure 2-57 InstallShield Wizard message

- 2) After the InstallShield Wizard is prepared, the [InstallShield Wizard] dialog box is displayed, and you are asked whether to install the UTS_FTAM 7.2. Click <Next>. You are prompted to select a destination folder, as shown in Figure 2-58.

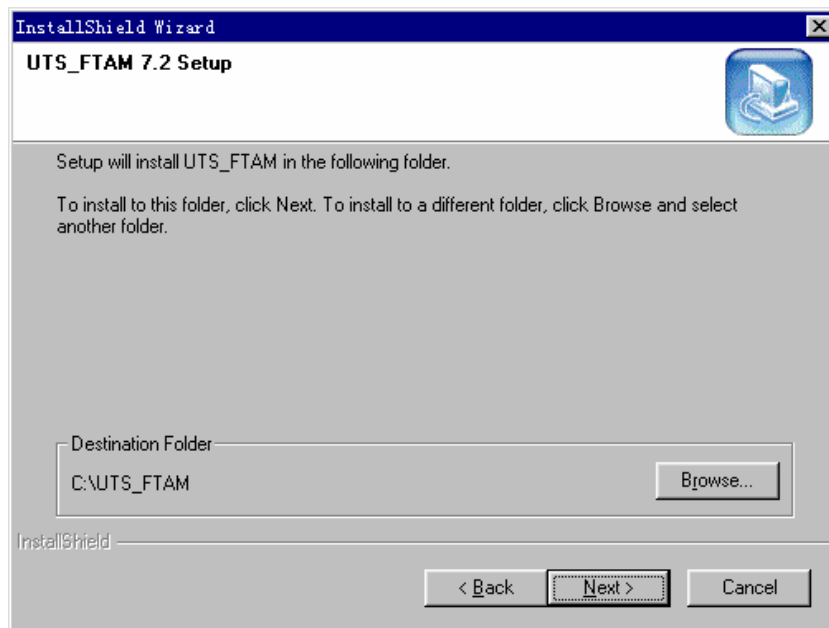


Figure 2-58 Selecting destination folder

- 3) Retain the default destination folder. Click <Next>. You are prompted to select the type of setup, as shown in Figure 2-59.

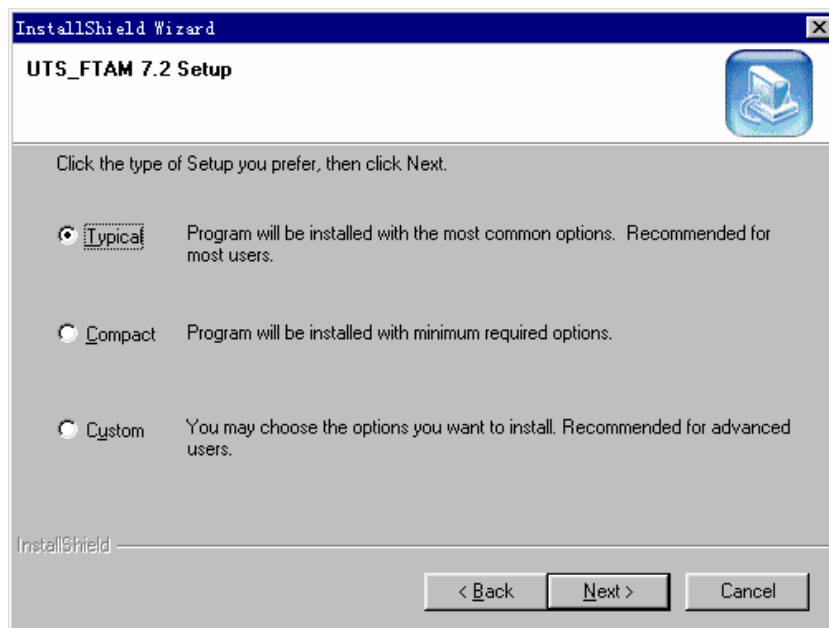


Figure 2-59 Selecting setup type

- 4) Select [Typical]. Click <Next>. You are prompted to select the installation folder, as shown in Figure 2-60.

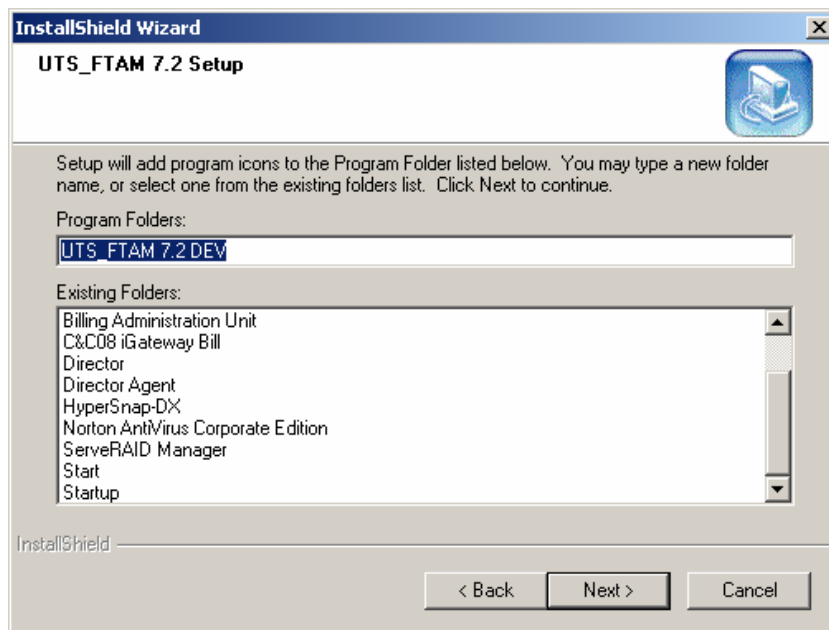


Figure 2-60 Selecting installation folder

- 5) Click <Next>. The current setting status is displayed. Click <Next>. The InstallShield Wizard automatically copies the files.
- 6) After the files are copied, the [install services] dialog box is displayed, as shown in Figure 2-61.

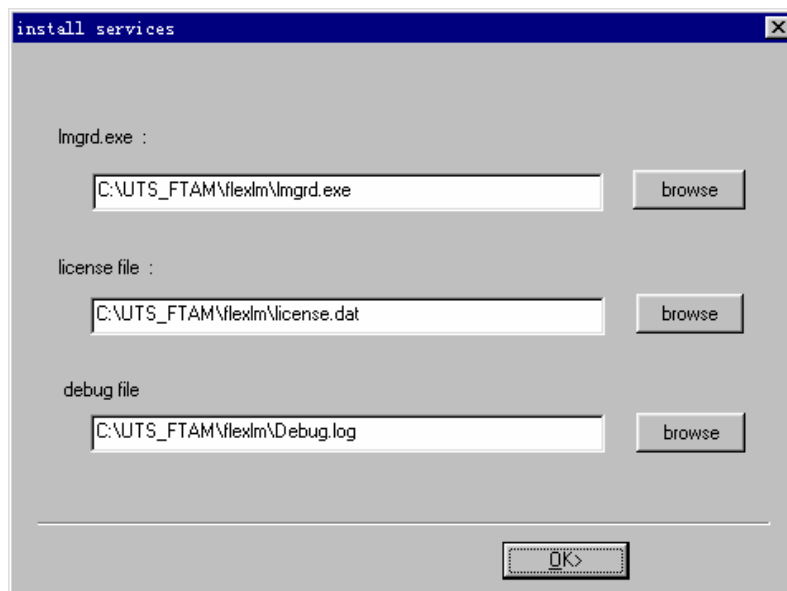


Figure 2-61 Selecting installation path

- 7) Retain the default settings. Click <OK>. The [InstallShield Wizard Complete] dialog box is displayed, as shown in Figure 2-62.

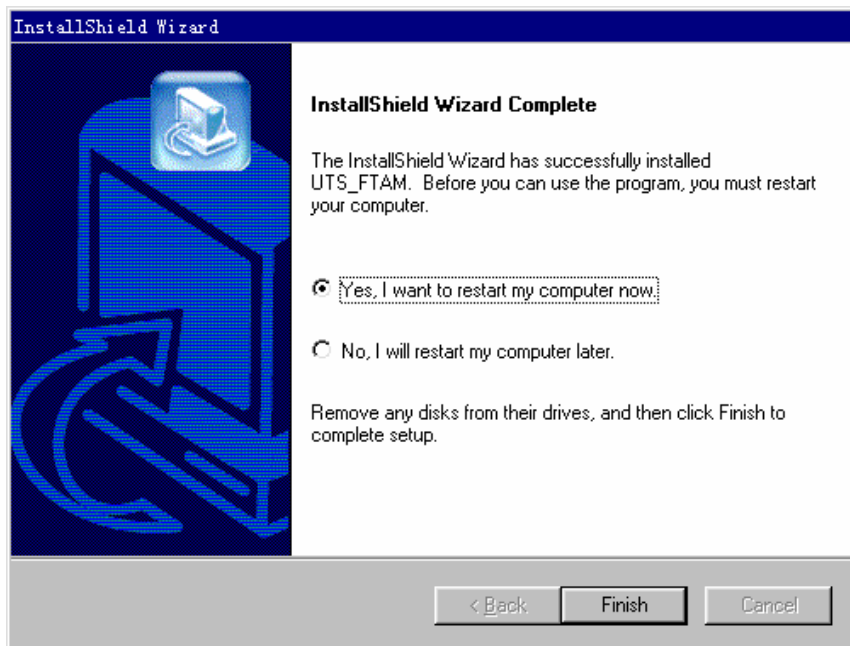


Figure 2-62 [InstallShield Wizard Complete] dialog box

- 8) Select [No, I will restart my computer later]. Click <Finish>.
- 9) Create a license.dat under C:\UTS_FTAM\FlexIm\. Copy the UTS_FTAM7.2 license to the license.dat. Save the file. Close the file.
- 10) Right-click the My Computer icon. Select [Properties] from the shortcut menu. The [System Properties] dialog box is displayed. Click the [Advanced] tab. Click <Environment Variables>. Check whether there is a variable "LM_LICENSE_FILE" in the system variables. If there is not, create an environment variable. Assign the installation paths to the UTS_NetLink and UTS_FTAM licenses for the variable. If you retain the default installation paths during the installation process, the value is "C:\Program Files\Vertel UTS-NetLink\etc\license.dat; C:\UTS_FTAM\flexIm\ license.dat". (The paths are separated by a semi-colon ";".)
- 11) Restart the computer to complete the installation.

IV. Configuring FTAM parameters

The iGWB is the FTAM responder, and the configuration is not required. The FTAM initiator (bill collector of the billing center), however, must be configured.

The local end should let the initiator know the NASP for configuration use.

2.4.2 Installing FTP Protocol

If the iGWB is required to provide an FTP interface to the billing center, the FTP server software must be installed and configured in the iGWB. Usually, the FTP

server software is installed during the installation of the operating system. If the FTP server software is not installed, install it as follows:

I. Installing FTP server

To install the FTP server, proceed as follows:

- 1) Insert the Windows 2000 Server CD.
- 2) Select [Start/Setting/Control Panel]. Double-click the Add and Remove Programs icon, and install the Windows 2000 component.

II. Setting FTP parameters

The FTP parameters to be set include the FTP user and the directory open to the billing center. Proceed as follows:

- 1) Select [Start/Programs/Administrative Tools/Internet Service Manager]. See Figure 2-63.

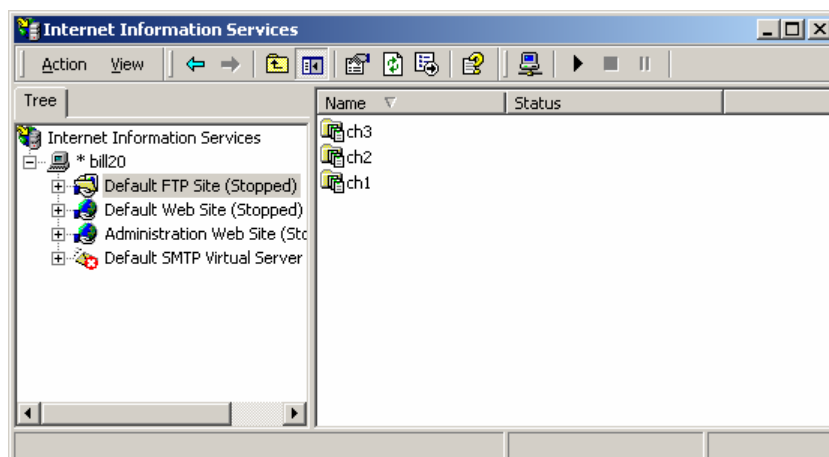


Figure 2-63 Starting FTP configuration window

- 2) Right-click [Default FTP Site]. Select [Properties] from the shortcut menu. See Figure 2-64.

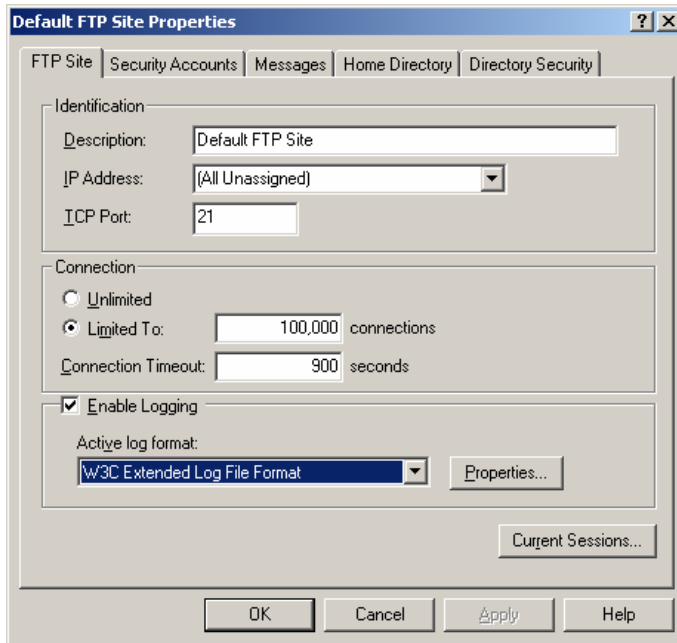


Figure 2-64 [Default FTP Site Properties] dialog box

3) Click the [Security Accounts] tab. See Figure 2-65.

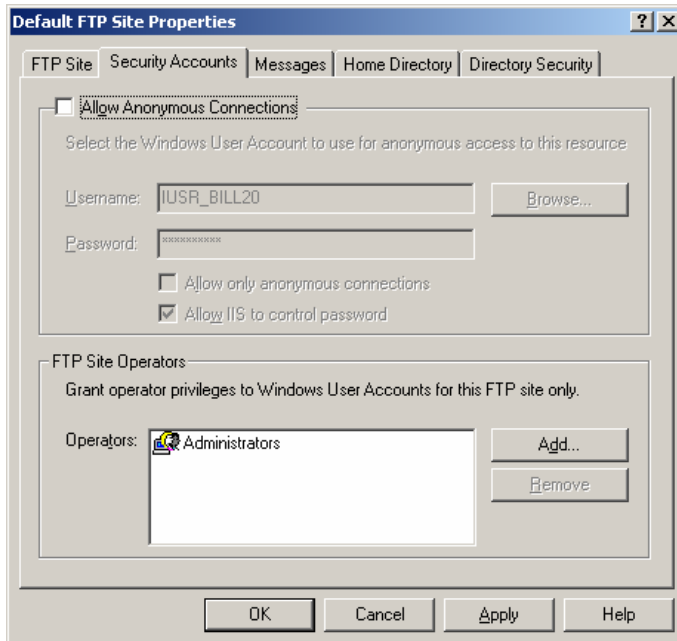


Figure 2-65 [Security Accounts] tab

Do not select [Allow only anonymous connections]. Retain the settings of the other parameters. Click the [Home Directory] tab.

4) At the [Home Directory] tab, click <Browse>. Set the local path to "E:\backsave\second", that is, the directory for the iGWB to store the final bill

files. Select the read and write attributes. Set the directory list style to "UNIX".
Click <OK> to complete the setting.

2.4.3 Setting User Authority

In view of security, the correct username and password must be entered when the billing center attempts to fetch bills from the iGWB through FTP or FTAM. This section presents how to set username, password, and access authority for the billing center to get access to the iGWB.

- 1) Select [Start/Programs/Administrative Tools/Computer Management/Local Users and Groups] to start the user management program. See Figure 2-66

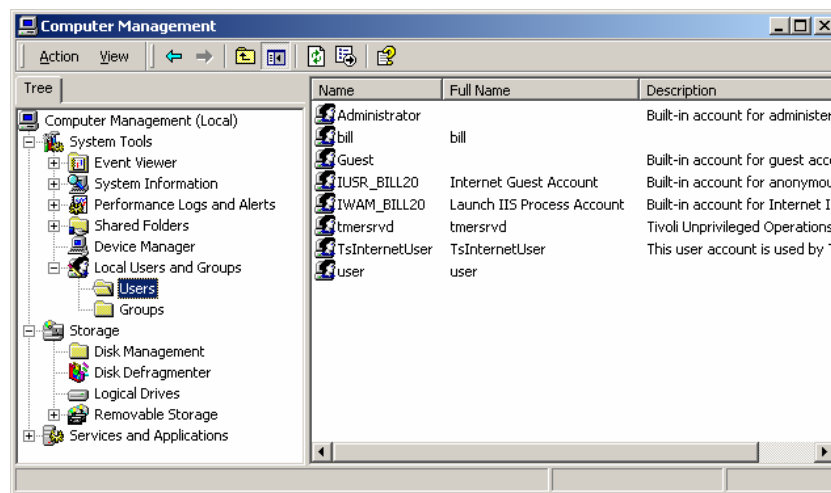


Figure 2-66 Domain user management window

- 2) Select [Users]. Select [Action/New User] to create a username and password for the billing center to log on to the iGWB. A dialog box is displayed, as shown in Figure 2-67.

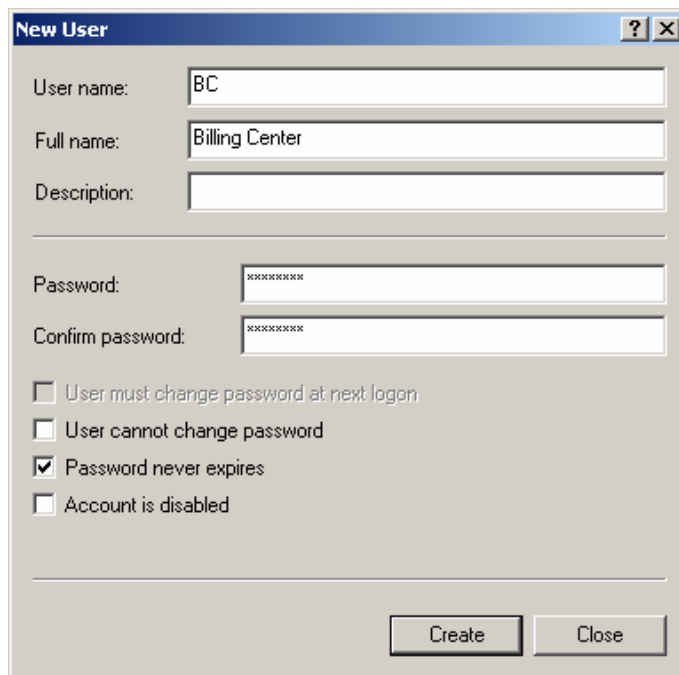


Figure 2-67 [New User] dialog box

- 3) Enter the username, password, and confirm password. Select [Password never expires]. Do not select [User must change password at next logon] or [Account is disabled]. Select [User cannot change password] as required. Click <Create>.
- 4) Quit the program.

2.5 Installing iGWB Server Software

2.5.1 Installing Server Software

Both the active and standby servers must be installed with the iGWB server software by the following procedure:

I. Starting the server

Power on the server. After Windows 2000 Server is started, insert the iGWB installation CD into the CD-ROM drive of the active server.

II. Choosing the setup language

- 1) Double-click Setup.EXE. The [Choose Setup Language] dialog box is displayed. The iGWB supports two languages: simplified Chinese and U.S. English. Select [U.S. English]. See Figure 2-68.

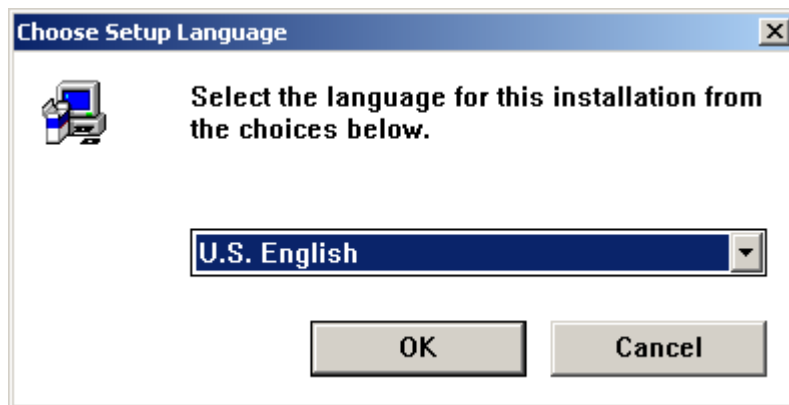


Figure 2-68 [Choose Setup Language] dialog box

Click <OK> to continue.

2) The [Welcome] dialog box is displayed, as shown in Figure 2-69.



Figure 2-69 [Welcome] dialog box

Click <Next> to continue.

III. Confirming the license agreement

The [Software License Agreement] dialog box is displayed, as shown in Figure 2-70. Read the license agreement carefully.

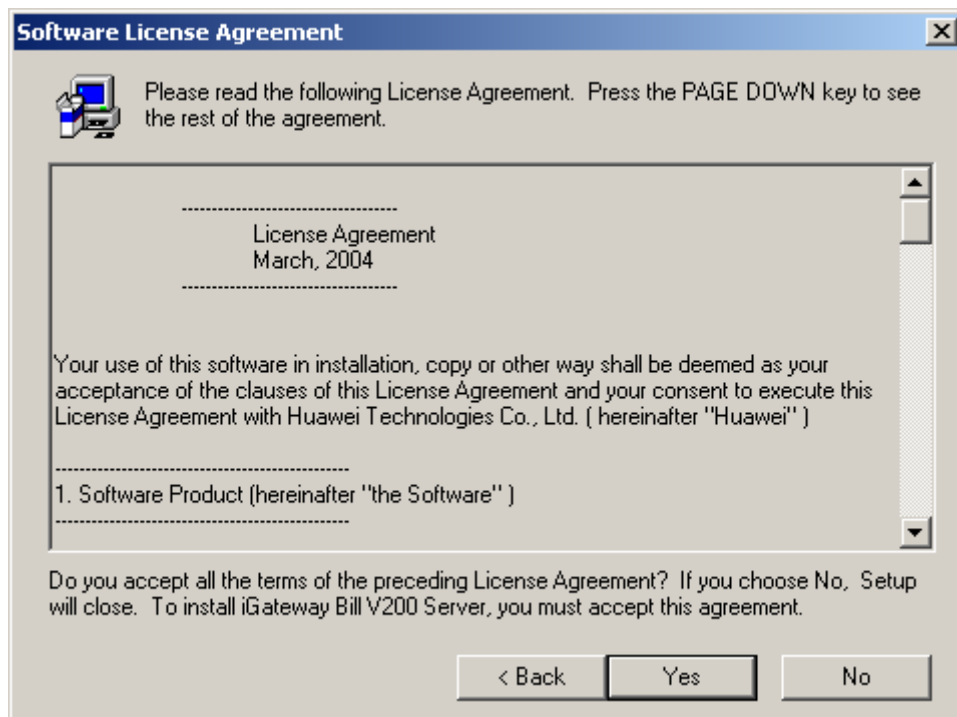


Figure 2-70 [Software License Agreement] dialog box

Click <Yes> to accept the agreement.

IV. Entering user information

In the [User Information] dialog box, enter your name and company. See Figure 2-71.

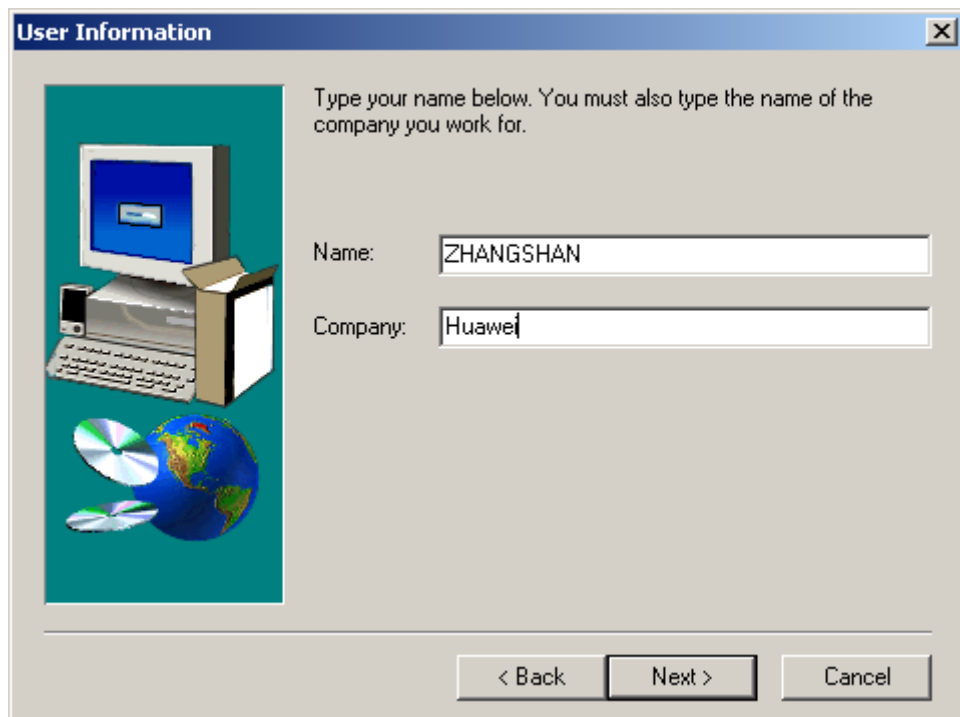


Figure 2-71 [User Information] dialog box

After the correct user information is entered, click <Next> to continue.

V. Selecting the program folder

In the [Select Program Folder] dialog box, enter a program folder. The default setting is recommended. See Figure 2-72.

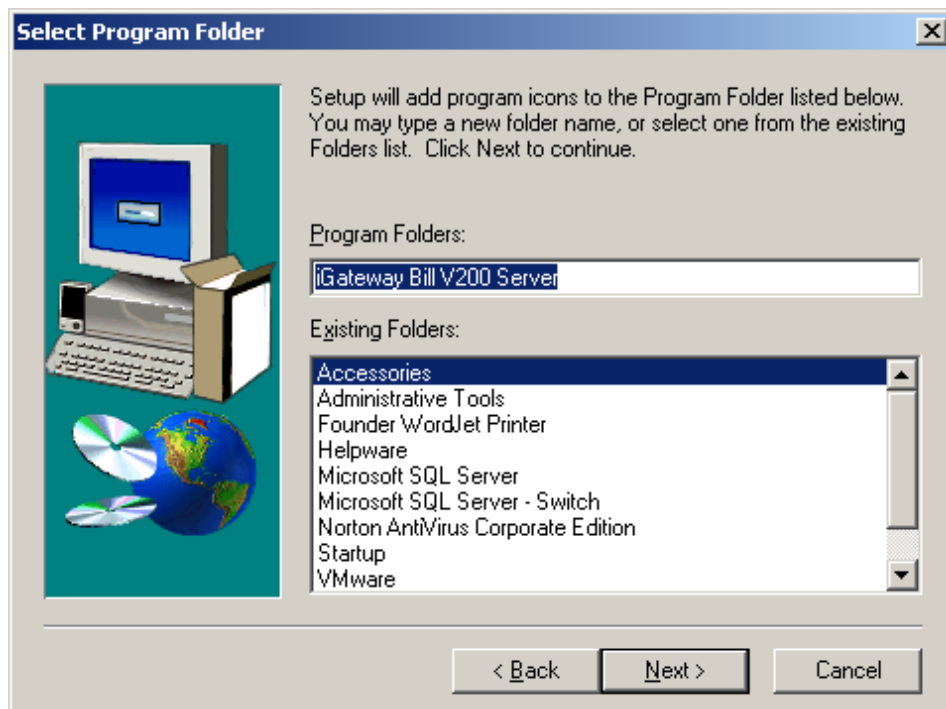


Figure 2-72 [Select Program Folder] dialog box

Click <Next> to continue.

VI. Selecting the destination location

In the [Choose Destination Location] dialog box, you can click <Browse> to change a destination folder. The default settings are recommended. See Figure 2-73.

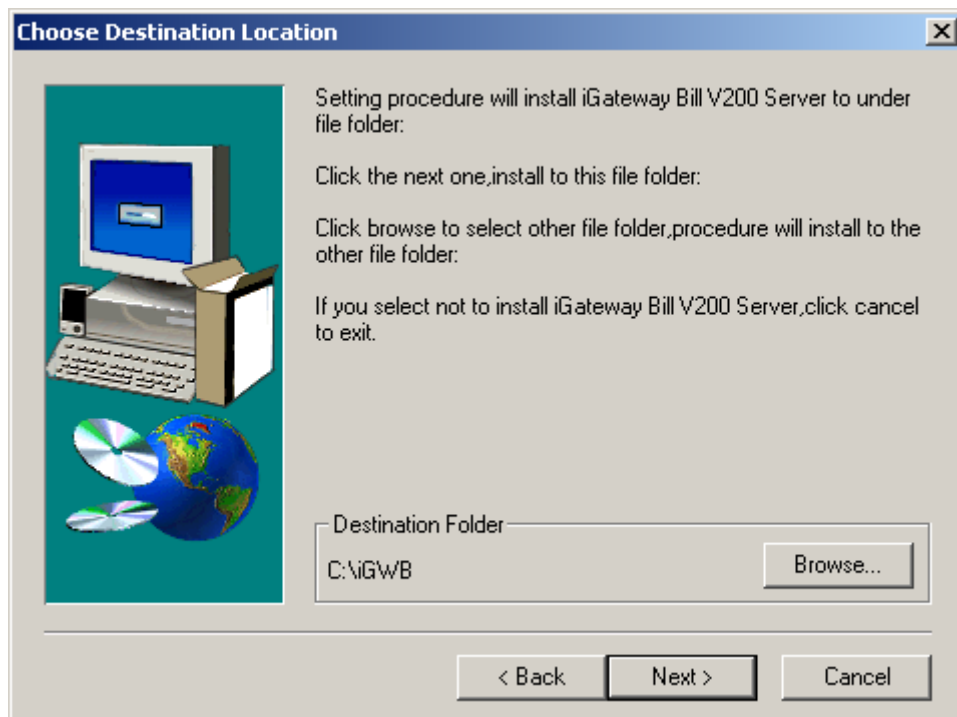


Figure 2-73 [Choose Destination Location] dialog box

After the installation path is set, click <Next> to continue.

VII. Starting copying files

The current settings are displayed in the [Start Copying Files] dialog box. You are prompted that file copying is to start. If the settings are not correct, click <Back> to modify them. See Figure 2-74.

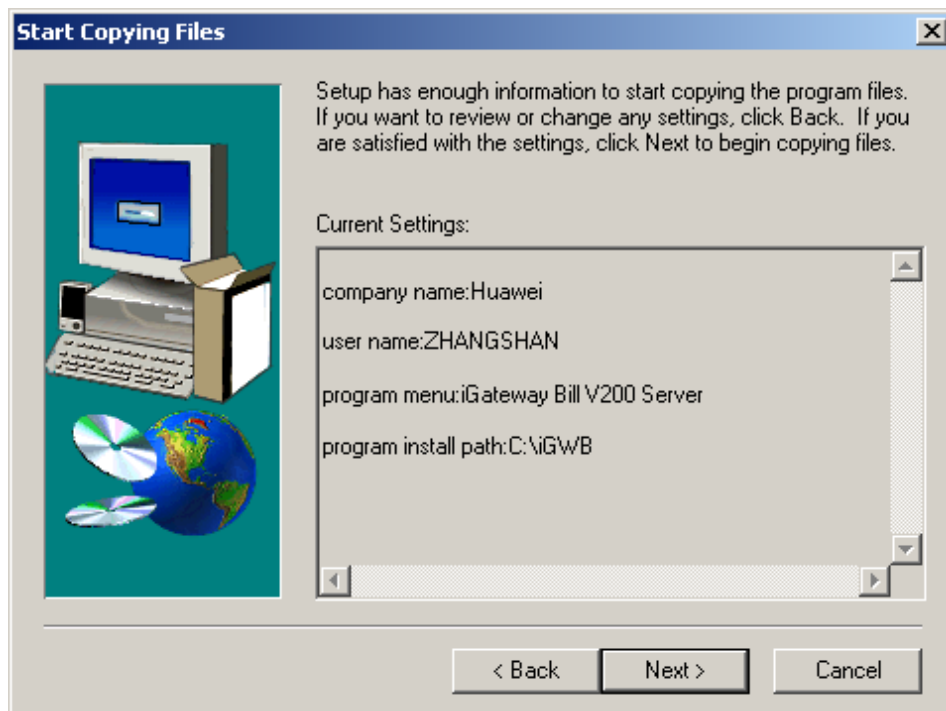


Figure 2-74 [Start Copying Files] dialog box

After the current settings are confirmed, click <Next> to start copying files.

VIII. Completing the installation

After the files are copied, the [Setup Complete] dialog box is displayed, as shown in Figure 2-75.

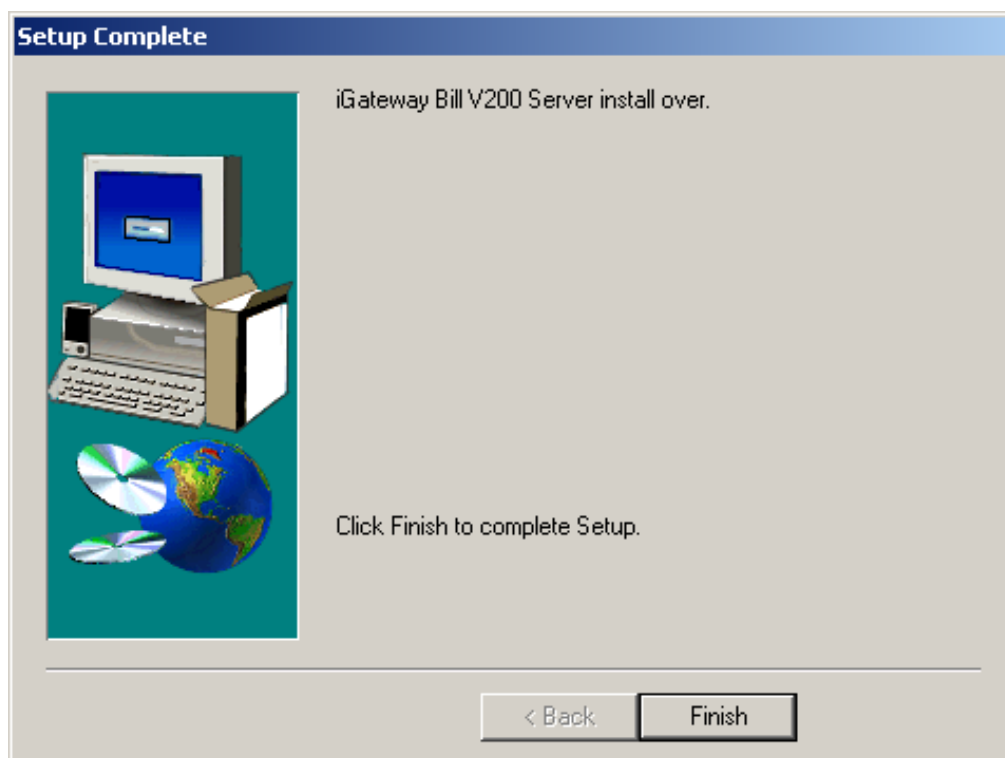


Figure 2-75 [Setup Complete] dialog box

Click <Finish> to complete the installation of the iGWB software on the active server.

Switch the input and output to the standby iGWB server by using the integrated converter. Insert the iGWB installation CD into the CD-ROM drive. Repeat the preceding steps to install the software on the standby server.

2.5.2 Modifying Server Software Settings

After the software is installed on the active and standby iGWB servers, it is necessary to set the parameters. The parameter configuration file of the server is `igwb.ini` in, by default, `C:\iGWB\config\ini`. The file can be opened by text editor, for example, Notepad.

Note:

- After editing the file, select [File/Save]. Do not select [Save as...] because it will change the extension of the file into, for example, ".txt" and cause the iGWB unbootable.
 - When installing the second server, you can refer to the parameter configuration file for the first server. The parameter values must be modified according to the fact, for example, ServerNo in the common parameter, LocallIP and PeerIP in the heartbeat link parameter, and OrginallIP in the shared resource parameter.
-

In the following description, the “non-mandatory” configuration items should use the defaulting settings if it is not for a particular purpose, and the “mandatory” configuration items can be modified according to the actual requirements.

I. Common parameters

The [Common] field defines the common parameters for the various processes at the iGWB V200 server. Table 2-5 shows the parameter configuration.

Table 2-5 Configuration of common parameters

Configuration item	Configuration description	Recommended value
APCount	Non-mandatory , used to set the number of access points. If the iGWB server is installed in the SoftX3000, the value is 1.	1
ServerNo	Mandatory , used to set the active (0) or standby (1) state for the iGWB server. According to the installation requirement, the server installed in the lower position of the rack is the active one, while the one in the upper position is the standby one.	0
NoCluster	Mandatory , used to set whether the current system is a dual-system. The default value is 0, indicating that the current system is a dual-system. The value 1 indicates that it is a single system.	0

II. Access point parameters

The [AccessPoint1] field defines the access point features. Table 2-6 shows the parameter configuration.

Table 2-6 Configuration of access point parameters

Configuration item	Configuration description	Recommended value
APType	Mandatory , used to set the type of the access point. The parameter value 0 indicates C&C08 product; 1 indicates MSC product; 2 indicates STP product; 3 indicates GPRS product; 4 indicates WCDMA product; 5 indicates SoftSwitch product. For SoftX3000, it is 5.	5
APName	Mandatory , used to set the name of the access point. For SoftX3000, it is "X3KM". This value must not be modified.	X3KF
LocalIpToEx	Mandatory , used to set the IP address of the local active network port connected to the SoftSwitch. Its value is the same as that of VirtualIP of Resource2.	172.20.200.1
LocalIpToExBak	Mandatory , used to set the IP address of the local standby network port connected to the SoftSwitch. Its value is the same as that of VirtualIP of Resource3.	172.30.200.1
LocalPortToEx	Mandatory , used to set the port number of the local active network port connected to the SoftSwitch.	9900
LocalPortToExBak	Mandatory , used to set the port number of the local standby network port connected to the SoftSwitch.	9900
BillRecSize	Mandatory , used to set the size of an original bill record. Use the default value.	156
BinAlarmSend	Non-mandatory , used to set whether to send the binary alarm. 0 indicates "not send", and 1 means "send". Use the default value.	1
SaveSecond	Non-mandatory , used to set whether the back disk file is saved in two copies. 0 indicates "not saved", and 1 means "saved". Use the default value.	1

III. MML server parameters

The [MML] field defines the network parameters for the communication between iGWB server and client. Table 2-7 shows the parameter configuration.

Table 2-7 Configuration of MML parameters

Configuration item	Configuration description	Recommended value
LocalIpToMMLClient	Mandatory , used to set the IP address of iGWB server for connecting with iGWB client. The IP address is also the virtual IP address of the iGWB for connecting with the network management system (the same as VirtualIP of Resource1 to be mentioned below).	Be set according to the actual situations.

IV. Dual-system parameters

The [Cluster] field defines the parameters for the running of the iGWB servers in dual-system mode. Table 2-8 shows the parameter configuration.

Table 2-8 Configuration of dual-system parameters

Configuration item	Configuration description	Recommended value
InstallShareDiskArray	Mandatory , used to set whether the hard disk array is shared between the dual systems. The value 0 indicates the non-shared mode; the other values mean the shared mode. Use the default value.	0
HeartBeatBroken	Non-mandatory , used to set the heartbeat timeout duration, in seconds, of the dual systems. Use the default value.	300
HeartBeatCount	Non-mandatory , used to set the number of heartbeat links. In normal cases, the iGWB has two heartbeat links. One uses the network, and the other uses serial port. Use the default value.	2
ResourceCount	Mandatory , used to set the number of resources (virtual IP addresses) shared by the dual systems. The iGWB requires a minimum of three virtual IP addresses. One is used for connecting to OMC or the bill console, another is for the active plane network port of the SoftSwitch, and the other is for the standby plane network port. In special cases, the fourth virtual IP address might be required.	3

V. Heartbeat link parameters

The [Link1] and [Link2] fields define the features of the two heartbeat links between the dual systems of the iGWB. [Link1] is used to set the parameters of the first heartbeat link (private network). [Link2] is used to set the parameters of the second heartbeat link (serial port). The parameters of the links are not exactly the same.

Generally, the default values are used for the link parameters. Table 2-9 shows the parameter configuration.

Table 2-9 Configuration of heartbeat link parameters

Configuration item	Configuration description	Recommended value
Type	Mandatory , used to set the type of the heartbeat link. UDP indicates the adoption of UDP/IP (private network). COM indicates the serial port.	Link1: UDP Link2: COM
Name	Non-mandatory , used to set the name of the heartbeat link. UDP_LINK is recommended for the private network heartbeat link. COM_LINK is recommended for the serial port heartbeat link.	Link1: UDP_LINK Link2: COM_LINK
Port	Non-mandatory , used to set the serial port number used when the heartbeat link adopts serial port. The available values include 1 (COM1) and 2 (COM2). Because the IBM343 server is configured only with COM2, the value here must be "2".	2
LocalIP	Mandatory , used to set the local IP address for communication use when the heartbeat link adopts UDP.	Actual IP address of network adapter 1
PeerIP	Mandatory , used to set the peer IP address for communication use when the heartbeat link adopts UDP.	Actual IP address of the peer network adapter 1

VI. Shared resource parameters

The [Resource1], [Resource2], and [Resource3] fields define the shared resources of the dual systems, usually the virtual IP addresses shared by the dual systems. Supposing the ResourceCount in [Cluster] is set to N, the [Resource1], [Resource2] to [ResourceN] come into being.

The iGWB requires three virtual IP addresses, which has parameters with the same meanings. Table 2-10 shows the parameter configuration.

Table 2-10 Configuration of shared resource parameters

Configuration item	Configuration description	Recommended value
ResType	Mandatory , used to set the resource type. The resources are all assigned with IP.	IP
ResName	Non-mandatory , used to set the resource name.	Resource1: OMC_IP Resource2: IP_PLANE1 Resource3: IP_PLANE2

Configuration item	Configuration description	Recommended value
OriginalIP	Mandatory , used to set the local original IP address.	Resource1: Be set according to the actual situations. Resource2: Be set according to the actual situations. Resource3: Be set according to the actual situations.
VirtualIP	Mandatory , used to set the virtual IP address.	Resource1: Be set according to the actual situations. Resource2: 172.20.200.1 Resource3: 172.30.200.1
VirtualMask	Mandatory , used to set the mask of VirtualIP.	255.255.0.0
SwitchGroup	Non-mandatory , used to set the switching group. The default value is 0.	Resource1 is independent and set to "0", that is, the setting is not changed. Resource2 and Resource3 are grouped together and set to "1".

VII. Network backup parameters

The [NetBackup], [BackupTask1], and [BackupTask2] fields define the parameters related to network backup. These fields are optional and configured only in the case of network backup. Table 2-11 shows the parameter configuration.

Table 2-11 Configuration of network backup parameters

Configuration item	Configuration description	Recommended value
UserName	Conditionally mandatory , used to specify the logon username when network backup is adopted.	/
DestHostIP	Mandatory , used to specify the IP address of the remote host when network backup is adopted. If it is set to "local", it indicates local backup.	/
LocalIP	Mandatory , used to set the IP address (virtual IP address) of the local network adapter connected to the OMC.	Be set according to the actual situations.
Password	Conditionally mandatory , used to define the password for logging on to the network backup server. It is used together with UserName.	/

Configuration item	Configuration description	Recommended value
BackupTaskCount	Mandatory , used to set the number of backup tasks. An access point can have several backup tasks to back up the original bills and the final bills by channel. Each channel requires independent backup tasks.	Be set according to the actual backup situations.
SourceDir	Mandatory , used to specify the path to the source file to be backed up. An access point can have several backup tasks to back up the original bills and the final bills by channel. Each channel requires independent backup tasks. The SourceDir values vary with different backup tasks.	Be set according to the actual backup situations.
DestDir	Conditionally mandatory , used to specify the destination backup path. It can be an FTP virtual directory when network backup mode is adopted. An access point can have several backup tasks to back up the original bills and the final bills by channel. Each channel requires independent backup tasks. The DestDir values vary with different backup tasks.	Be set according to the actual backup situations.

 **Note:**

- A parameter configuration is subject to [BackupTaskN] (N represents the backup task number) if it has been configured in [BackupTaskN]. Otherwise, its configuration is subject to [NetBackup].
 - When network backup mode is adopted, password is presented in plain text when configured for the first time. After the program runs, it will be set to be ciphered text automatically.
 - For the parameters not listed here, use the default values.
 - In the case of network backup, SourceDir must be a directory with a date folder or a directory directly with bill files. Backup cannot be implemented if it is set to other directories.
-

After the active and standby servers are configured with the preceding parameters, save the files and close them.

2.5.3 Modifying Software Watchdog Settings

After the iGWB server software is configured, you need to modify the software watchdog settings and start the related service.

- 1) Switch the input and output to the active server. Select [Start/Programs/Administrative Tools/Services]. The [Services] window is displayed, as shown in Figure 2-76.

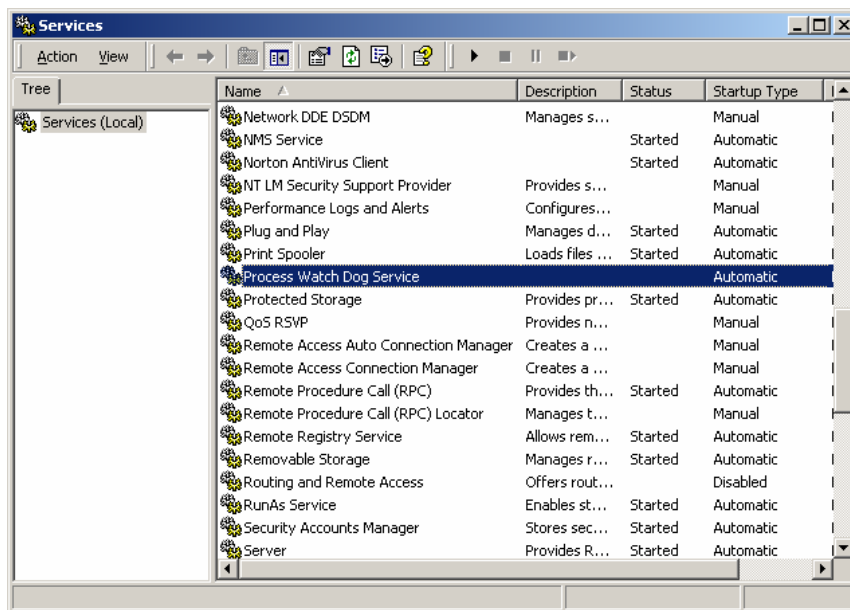


Figure 2-76 [Services] window

- 2) Right-click the Process Watch Dog Service icon. From the shortcut menu, select [Properties]. The [Process Watch Dog Service Properties] dialog box is displayed.
- 3) Confirm that “Automatic” is set in the [Startup type] box. Click [Start] to start the service. Figure 2-77 shows the properties after the modification. Click <OK> to complete the setting.

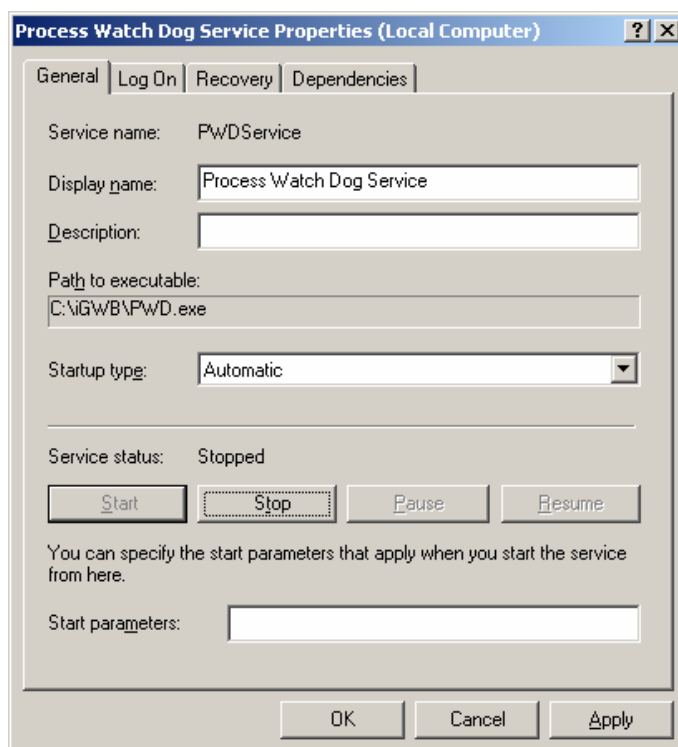


Figure 2-77 [Process Watch Dog Service Properties] dialog box after modification

- 4) Switch the input and output to the standby server. Perform the same setting operations.

Now, the installation and configuration of the iGWB server software are completed. Restart the server.

2.6 Installing iGWB Client Software

The iGWB client can run on multiple operating systems, such as Windows 98 and Windows 2000. A computer is employed as the hardware. The software package to be installed on the iGWB client includes the operating system and the iGWB client software. In addition, it is necessary to set the client software.

2.6.1 Installing Operating System

Refer to the related installation guide of the used operating system.

2.6.2 Installing Client Software

I. Choosing the setup language

- 1) Copy the contents of the client software installation CD (Client directory) to any directory of the client. Double-click \Client\SETUP.EXE under this directory (or

directly run it in the installation CD). The [Choose Setup Language] dialog box is displayed. The iGWB supports two languages: simplified Chinese and U.S. English. Select [U.S. English]. See Figure 2-78.

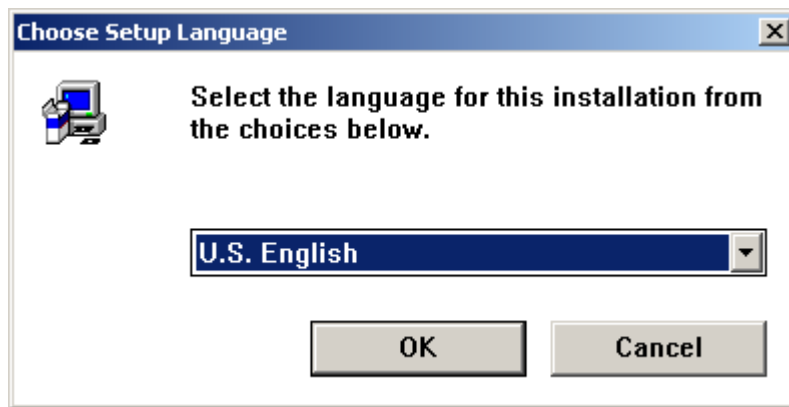


Figure 2-78 [Choose Setup Language] dialog box

Click <OK> to continue.

2) The [Welcome] dialog box is displayed, as shown in Figure 2-79.



Figure 2-79 [Welcome] dialog box

Click <Next> to continue.

II. Confirming the license agreement

The [Software License Agreement] dialog box is displayed, as shown in Figure 2-80. Read the license agreement carefully.

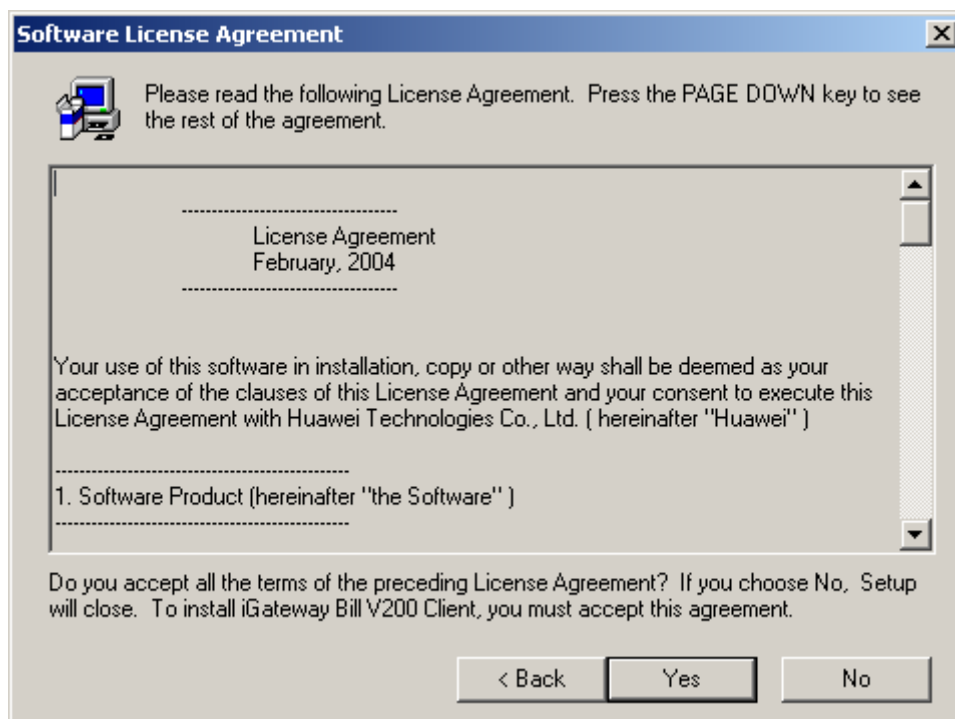


Figure 2-80 [Software License Agreement] dialog box

Click <Yes> to accept the agreement.

III. Entering user information

In the [User Information] dialog box, enter your name and company. See Figure 2-81.

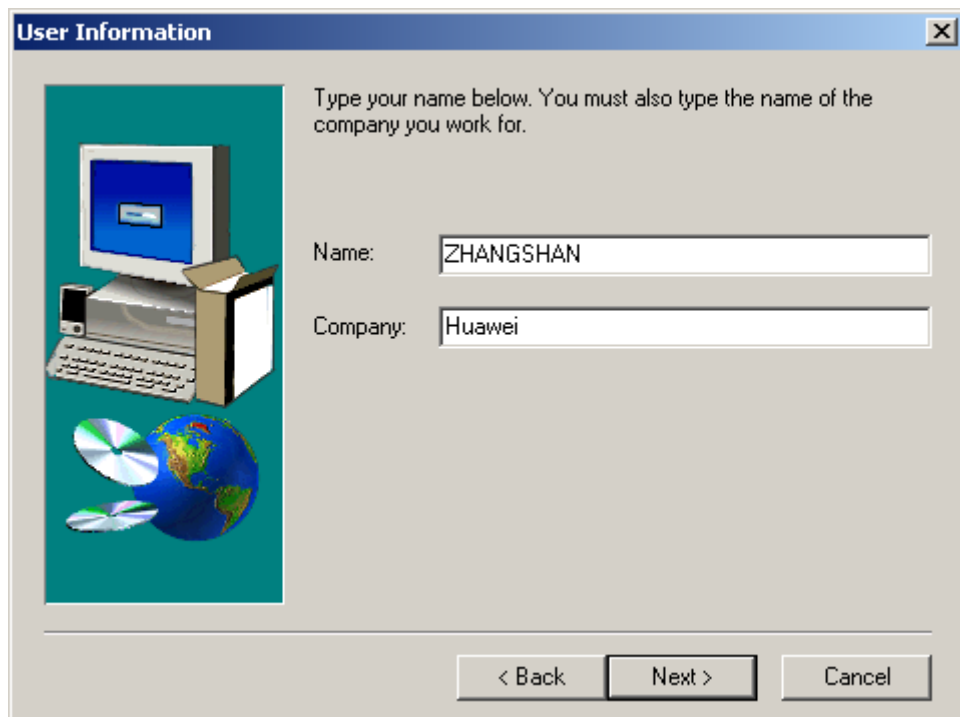


Figure 2-81 [User Information] dialog box

After the correct user information is entered, click <Next> to continue.

IV. Selecting the program folder

In the [Select Program Folder] dialog box, enter a program folder. The default setting is recommended. See Figure 2-82.

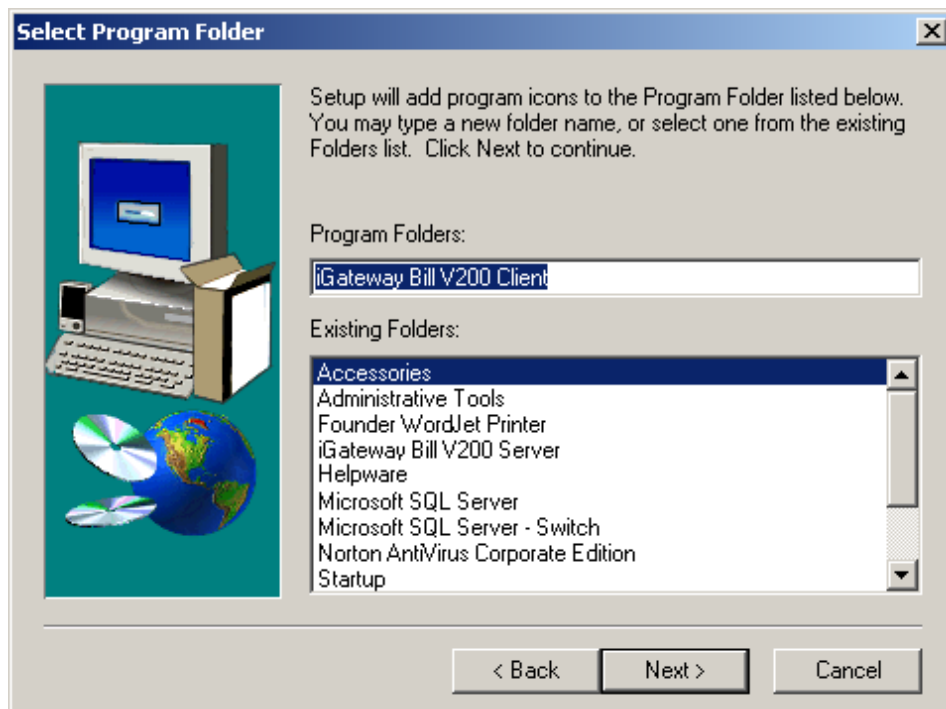


Figure 2-82 [Select Program Folder] dialog box

Click <Next> to continue.

V. Selecting the destination location

In the [Choose Destination Location] dialog box, you can click <Browse> to change a destination folder. The default settings are recommended. See Figure 2-83.

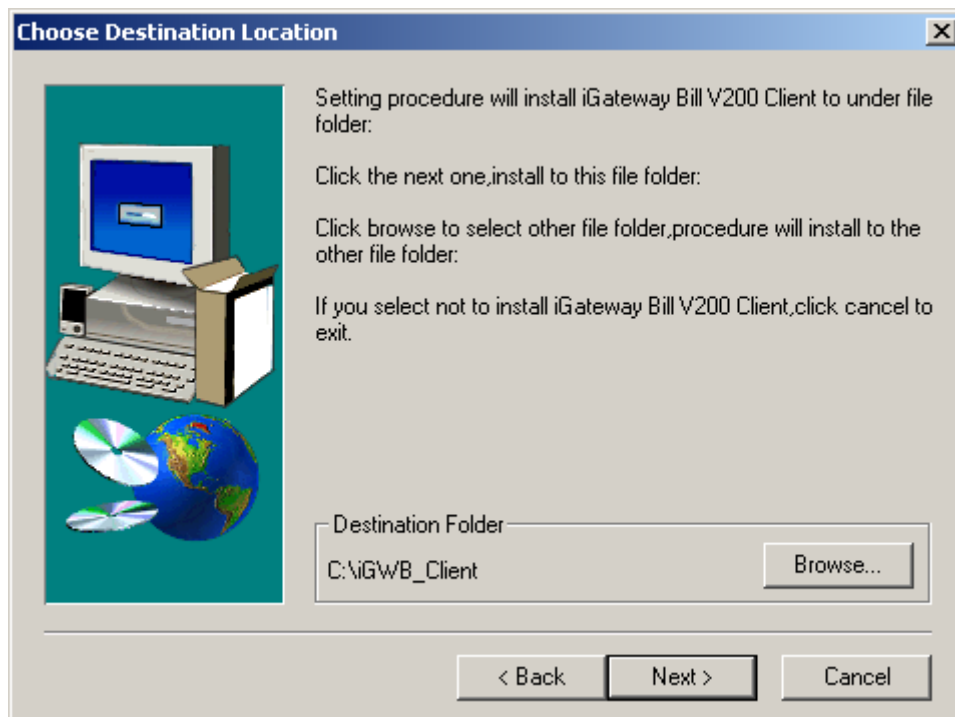


Figure 2-83 [Choose Destination Location] dialog box

After the installation path is set, click <Next> to continue.

VI. Starting copying files

The current settings are displayed in the [Start Copying Files] dialog box. You are prompted that file copying is to start. If the settings are not correct, click <Back> to modify them. See Figure 2-84.

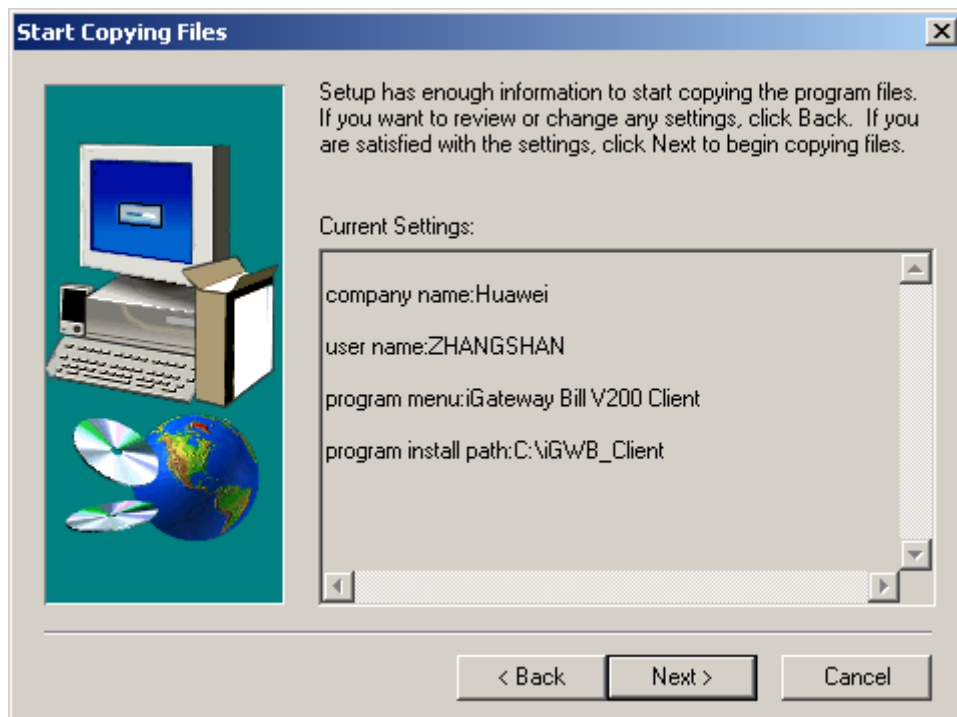


Figure 2-84 [Start Copying Files] dialog box

After the current settings are confirmed, click <Next> to start copying files.

VII. Completing the installation

After the files are copied, the [Setup Complete] dialog box is displayed, as shown in Figure 2-85.

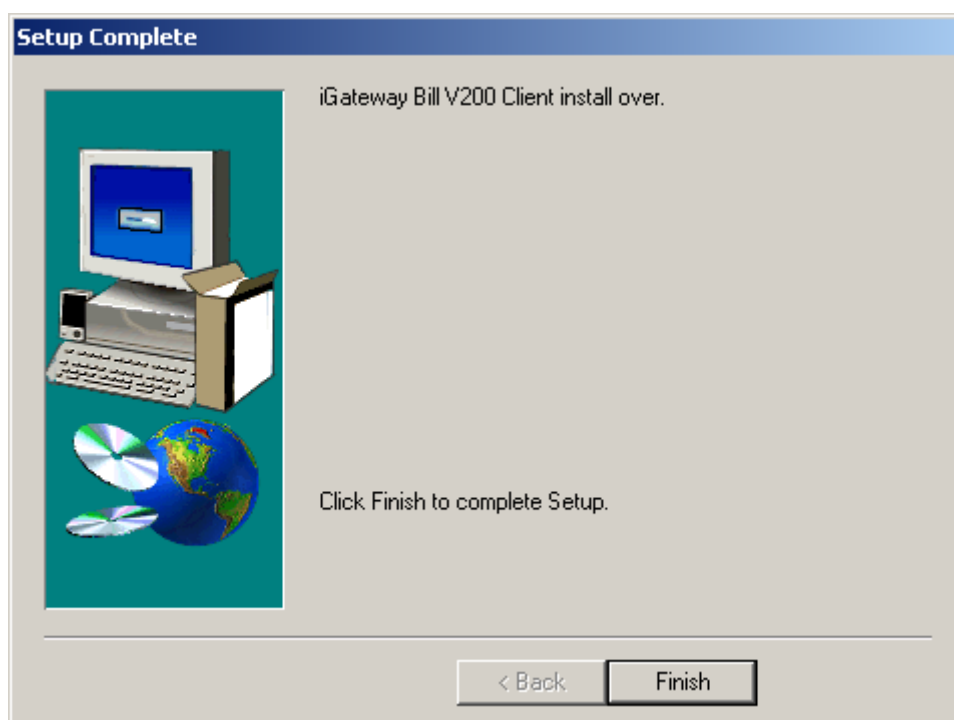


Figure 2-85 [Setup Complete] dialog box

Click <Finish> to complete the installation of the iGWB client software.

2.6.3 Modifying Client Settings

I. Configuring the ports

The client uses two ports: a maintenance port and a debugging port. By default, the maintenance port number is 6000, and the debugging port number is 6007. Use the default values.

The client software supports the port configurations. You can open the configuration file `uiconfig.ini` on the system directory (`C:\Winnt\uiconfig.ini`) to modify the configuration items under `[PORT]` as follows:

`[PORT]`

`MAINTAINPORT=6000`

`DEBUGPORT=6007`

Note:

The setting of MAINTAINPORT should be consistent with that of the corresponding port of the server.

II. Configuring the network adapter

Set the IP address of the network adapter of the client according to the related IP address plan.

Now, the installation of the iGWB client software is completed. You can start the client to connect to the server.

2.7 Modifying iGWB Factory Settings

2.7.1 Checklist of iGWB Factory Settings

Before the delivery, all other software except the iGWB server software has been installed, and some key parameters required during the installation have been preset. The preset information constitutes the factory settings of the iGWB, as shown in Table 2-12.

Table 2-12 iGWB factory settings

Preset item	Preset value	Modified or not
Computer name	iGWB0 for the active server iGWB1 for the standby server	Whether to be modified depends on the actual situations.
Workgroup name	WORKGROUP	Whether to be modified depends on the actual situations.
IP address of network adapter 0	130.1.2.1 for the active server 130.1.2.2 for the standby server 172.20.200.1 as the virtual IP address	Whether to be modified depends on the actual situations.
IP address of network adapter 1	130.1.3.1 for the active server 130.1.3.2 for the standby server 172.30.200.1 as the virtual IP address	Whether to be modified depends on the actual situations.
IP address of network adapter 2	130.1.1.1 for the active server 130.1.1.2 for the standby server 129.9.1.1 as the virtual IP address	Whether to be modified depends on the actual situations.

Preset item	Preset value	Modified or not
IP address of network adapter 3	130.1.4.1 for the active server 130.1.4.2 for the standby server	Whether to be modified depends on the actual situations.
Password of Windows 2000 Server administrator	igwb	It must be modified.

If you select the on-site installation process of the iGWB server software (as shown in Figure 2-2), the factory settings of the iGWB should be modified before the installation.

2.7.2 Modifying Computer Name and Workgroup

I. Opening the [System Properties] dialog box

At the Windows 2000 Server desktop, right-click the My Computer icon. Select [Properties] from the shortcut menu. The [System Properties] dialog box is displayed. Click the [Network Identification] tab. See Figure 2-86.

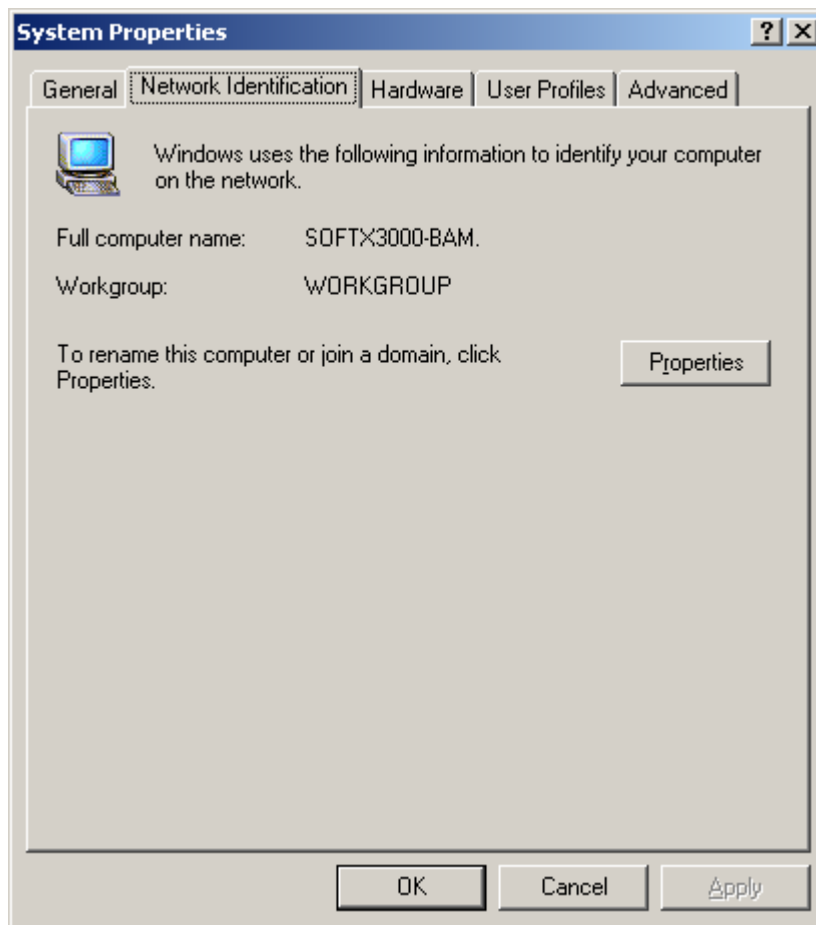


Figure 2-86 [Network Identification] dialog box

II. Modifying the computer name and workgroup name of the iGWB

Click <Properties> in Figure 2-86. The [Identification Changes] dialog box is displayed. Enter the computer name of the iGWB, for example, SHENZHEN, in the [Computer Name] box. Enter the workgroup name, for example, SWITCH, in the [Workgroup] box. Click <OK>. See Figure 2-87.

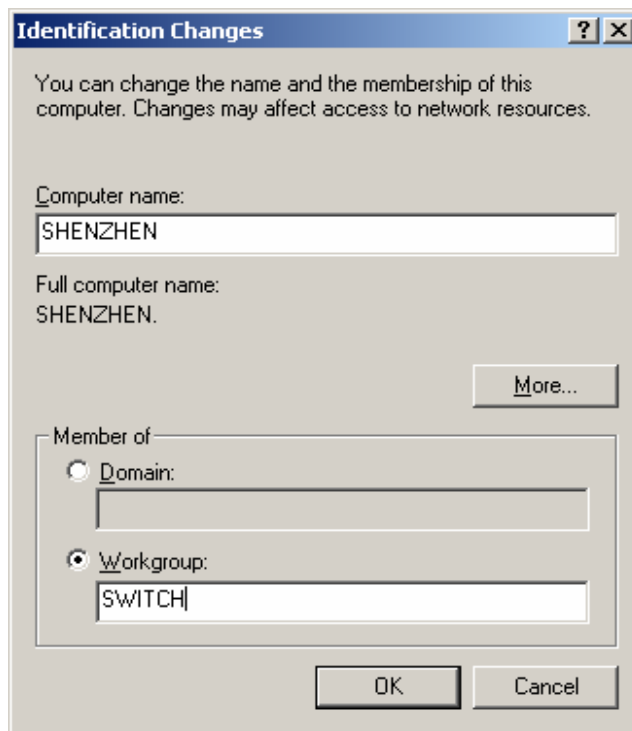


Figure 2-87 [Identification Changes] dialog box

III. Confirming the changes and restarting the iGWB

- 1) The [Network Identification] dialog box is displayed, as shown in Figure 2-88. Click <OK>.



Figure 2-88 [Network Identification] dialog box (1)

- 2) Another [Network Identification] dialog box is displayed to prompt you to restart the computer for the changes to take effect. Click <OK>. See Figure 2-89.

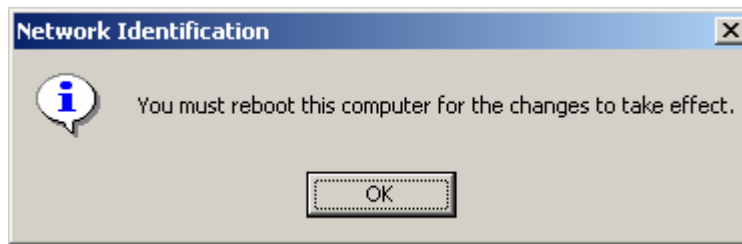


Figure 2-89 [Network Identification] dialog box (2)

2.7.3 Modifying IP Address of Network Adapter

The IP address of network adapter can be modified according to the actual situations. For the operations, refer to section 2.3.7 Setting IP Address for iGWB Network Adapter.

2.7.4 Modifying Administrator Password

I. Opening the [Computer Management] window

At the Windows 2000 Server desktop, right-click the My Computer icon. Select [Manage] from the shortcut menu. The [Computer Management] window is displayed, as shown in Figure 2-90.

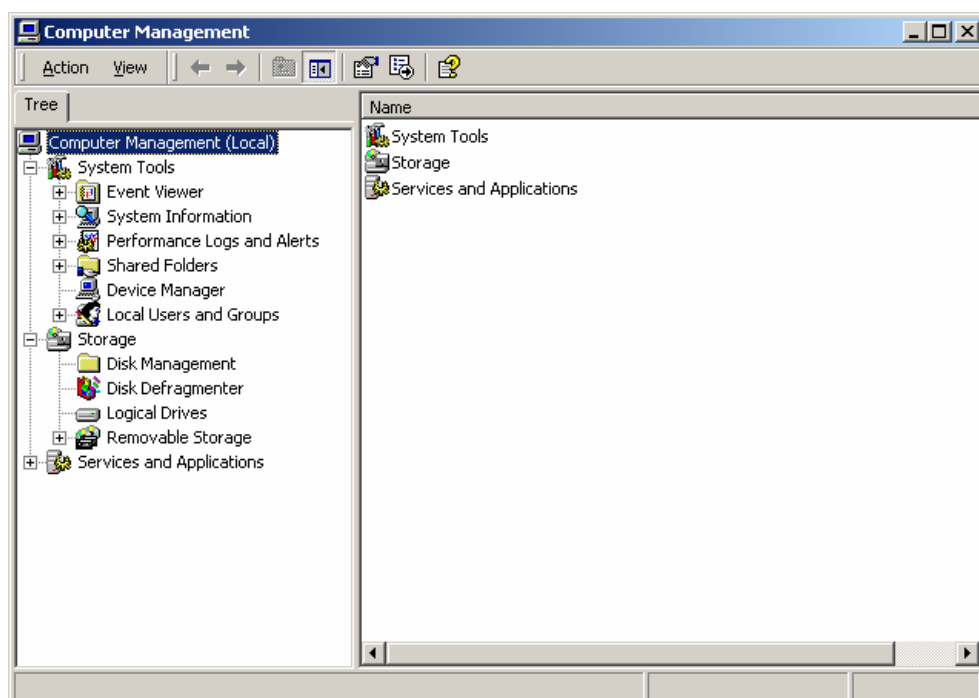


Figure 2-90 [Computer Management] window (1)

II. Displaying local users and groups

In the [Computer Management] window, select [System Tools/Local Users and Groups] at the navigation tree. All defined users are listed in the right pane, as shown in Figure 2-91.

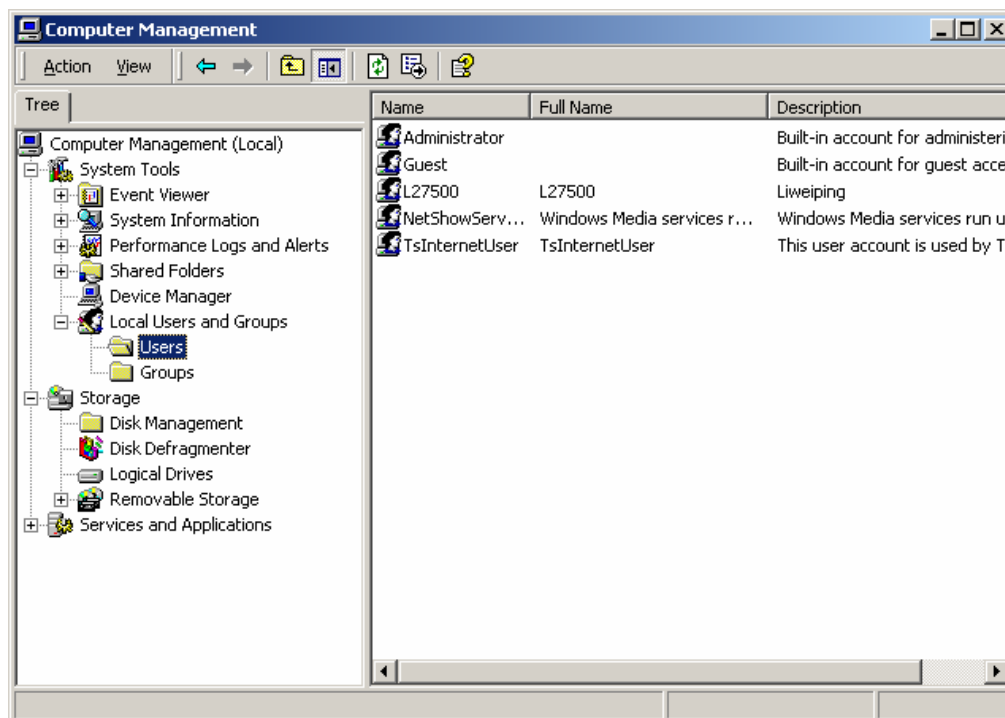


Figure 2-91 [Computer Management] window (2)

III. Modifying the password of Windows 2000 Server administrator

- 1) Right-click Administrator in the right pane of the [Computer Management] window. Select [Set Password] from the shortcut menu. See Figure 2-92.

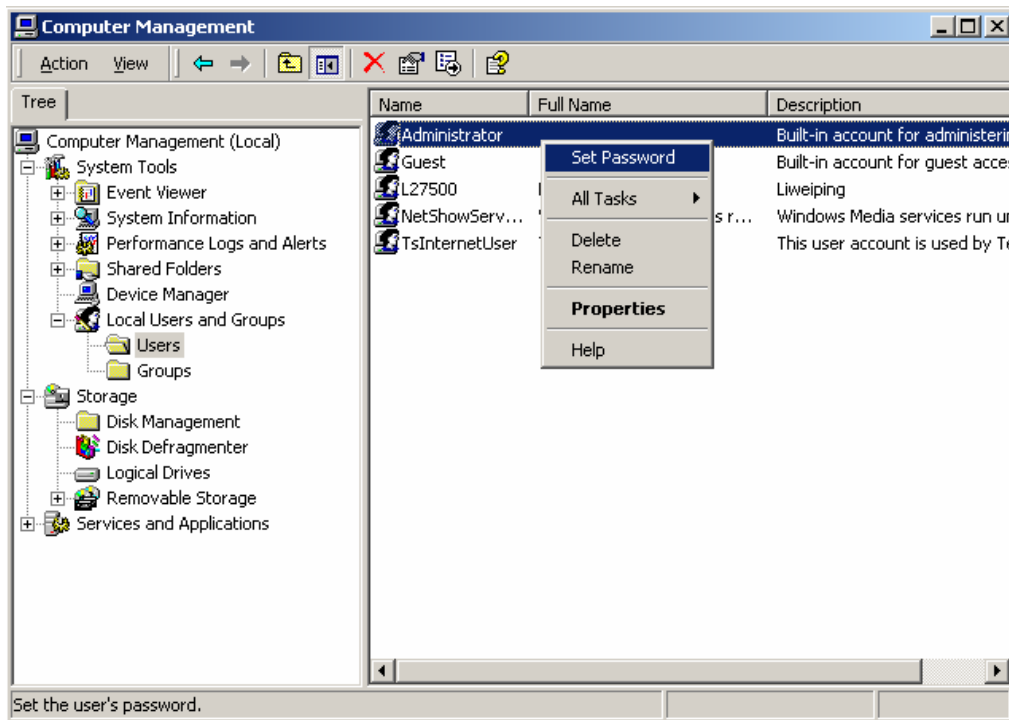


Figure 2-92 [Computer Management] window (3)

- 2) In the [Set Password] dialog box, enter the new password and confirm the password. Click <OK>. See Figure 2-93.

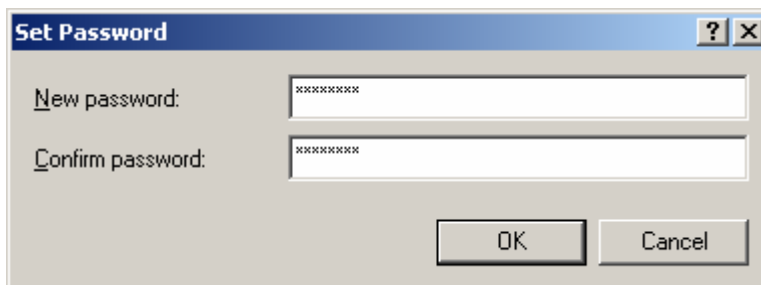


Figure 2-93 [Set Password] dialog box

- 3) The [Local Users and Groups] dialog box is displayed. You are prompted that the password has been changed. Click <OK>. See Figure 2-94.

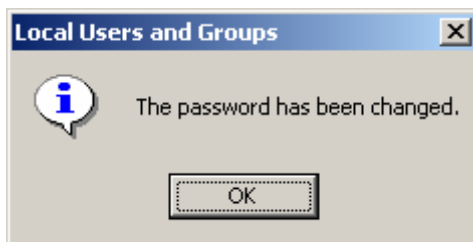


Figure 2-94 [Local Users and Groups] dialog box

2.7.5 Installing iGWB Server Software

Refer to section 2.5.1 Installing Server Software for the installation of the iGWB server software.

Refer to section 2.5.2 Modifying Server Software Settings for the configuration of the iGWB server software.

2.7.6 Modifying Software Watchdog Settings

Refer to section 2.5.3 Modifying Software Watchdog Settings for the modification of the software watchdog settings.

2.7.7 Setting Automatic Logon to Windows 2000 Server

Refer to section 2.3.8 Setting Automatic Logon to Windows 2000 Server for the setting of the automatic logon to Windows 2000 Server.

2.8 Checking Installed Hardware and Software

The software and hardware must be checked after they are installed. For the iGWB, hardware installation checks should be performed on the cables, and software installation checks should be on the operating system, the server software, and the client software.

2.8.1 Checking Installed Hardware

Because the iGWB server is installed with the BAM server of the SoftX3000, the iGWB server and the BAM server are checked together. For details, refer to *U-SYS SoftX3000 SoftSwitch System Hardware Installation Manual*.

2.8.2 Checking Windows 2000 Server

I. Patch version

It is required to patch Windows 2000 Server so that the operating system can run normally.

After Windows 2000 Server is installed, check the patch version as follows:

- 1) At the Windows 2000 Server desktop, right-click the My Computer icon. Select [Properties] from the shortcut menu. The [System Properties] dialog box is displayed, as shown in Figure 2-95.

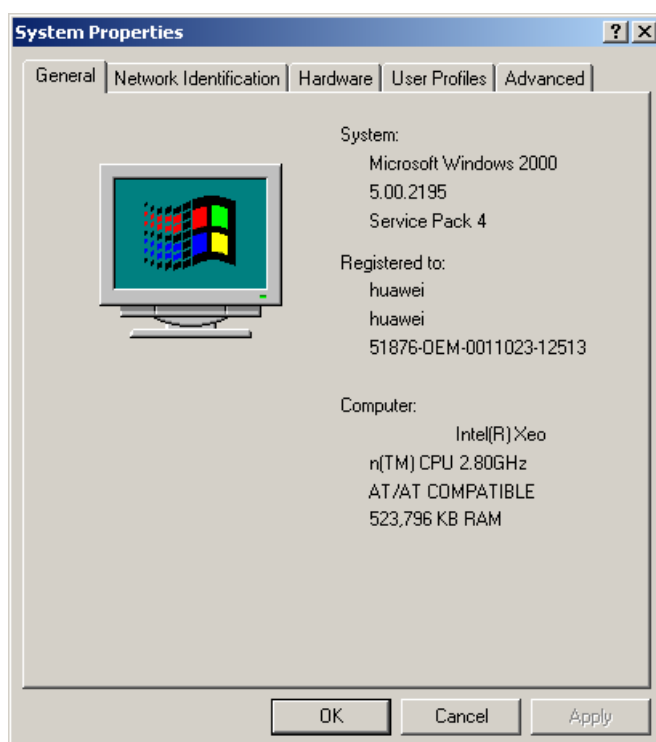


Figure 2-95 [System Properties] dialog box

- 2) The system information is displayed at the [General] tab. The correct version is Service Pack 4.
- 3) If the patch version is not correct, for example, earlier than Service Pack 3, check whether the installation process is carried out correctly. For example, check whether the used installation CD is correct.

II. Internet Explorer version

It is required to use Internet Explorer 5.5 or later versions so that the terminal OAM software can run normally. If the Internet Explorer version is not correct, some system functions will be influenced, such as online help functions.



Caution:

IE uses the default version during the installation of the Windows 2000 server.

After Windows 2000 Server is installed, check the Internet Explorer version as follows:

- 1) Start Internet Explorer.

- 2) On the menu bar of Internet Explorer, select [Help/About Internet Explorer]. The [About Internet Explorer] dialog box is displayed, as shown in Figure 2-96.



Figure 2-96 [About Internet Explorer] dialog box

- 3) The first line of words is the version of Internet Explorer, for example, Version: 5.50 4807.2300 (in Figure 2-96) in which “Version: 5.50” means that the version of Internet Explorer is 5.5.
- 4) If the Internet Explorer version is not correct, for example, earlier than 5.5, check whether the installation process is carried out correctly. For example, check whether the used installation CD is correct.

III. Automatic logon function

It is strongly recommended to set Windows 2000 Server to be in the automatic logon mode when Windows 2000 Server is installed. The purpose is to ensure the secure running of the system. In other words, the iGWB can automatically log on to Windows 2000 Server after being reset as a result of instantaneous power outage, operation mistake, or CPU overload.

After the automatic logon function of Windows 2000 Server is set, check the function as follows:

- 1) At the Windows 2000 Server desktop, select [Start/Shut Down...]. The [Shut Down Windows] dialog box is displayed. Select [Restart] from the drop-down list. Click <OK>. See Figure 2-97.



Figure 2-97 [Shut Down Windows] dialog box

- 2) The iGWB is restarted. After the restart, the system automatically logs on to Windows 2000 Server in the capacity of administrator, where you can perform operations at the Windows desktop without entering the logon password.
- 3) If you are prompted to press <Ctrl+Alt+Del> after the iGWB restarts, the automatic logon function of Windows 2000 Server is set unsuccessfully. Re-setting is needed.

2.8.3 Checking Server Software

I. Working state

- 1) Switch the input and output to the active server. Check the bulb in the status area. If the bulb is lit, it indicates that the active server is configured correctly and operating well.
- 2) Manually switch over the iGWB servers. Switch the input and output to the standby server. Check the bulb in the status area. If the bulb is lit in five minutes, it indicates that the standby server is configured correctly. Switch the input and output to the active server. Check the bulb of the active server. If the bulb is not lit, it indicates that the parameters of the active and standby servers are all set correctly and both servers are operating well.
- 3) If a running status exception happens during the start process, check the trace files in C:\iGWB\trace, and correct the configuration file accordingly. If the system is still abnormal after configuration correction, it is recommended to re-install the iGWB server software. For the analysis and modification of the trace files, refer to Chapter 4 "System Maintenance".

II. Program components

After installing the iGWB server software, check whether all program components are installed as follows:

- 1) At the Windows 2000 Server desktop, select [Start/Programs/iGateway Bill V200 Server]. The program components of the iGWB server software are displayed in a menu.
- 2) A complete set of iGWB server software includes the following program components:
 - Start iGateway Bill
 - Stop iGateway Bill
 - Uninstall System

III. Software version

- 1) Log on to the bill console from the client.
- 2) Select [Help/About iGWB]. The [About iGWB Client] dialog box is displayed, as shown in Figure 2-98. "V200R002" is the version of the iGWB software.

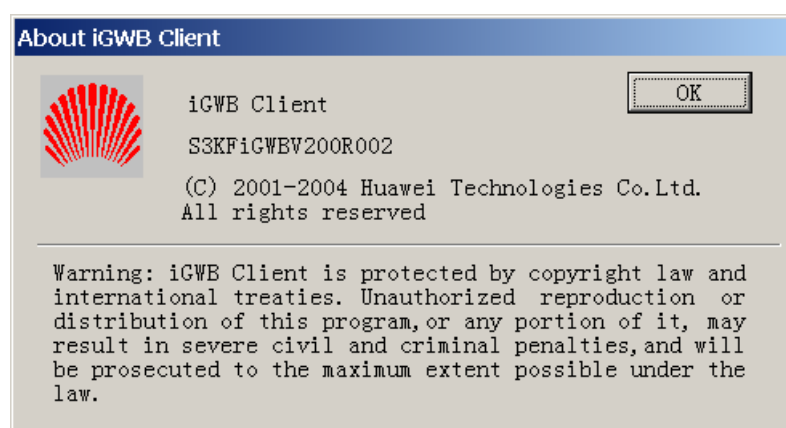


Figure 2-98 [About iGWB Client] dialog box

Note:

The version of the iGWB software can be queried only when the client successfully logs on.

2.8.4 Checking Client Software

After the iGWB client software is installed, check the program components as follows:

At the Windows 2000 Server desktop, select [Start/Programs/iGateway Bill V200 Client]. The program components of the iGWB client software are displayed in a menu.

A complete set of iGWB client software includes the following program components:

- Help
- iGWB Client
- Uninstall System

Chapter 3 Basic Operations

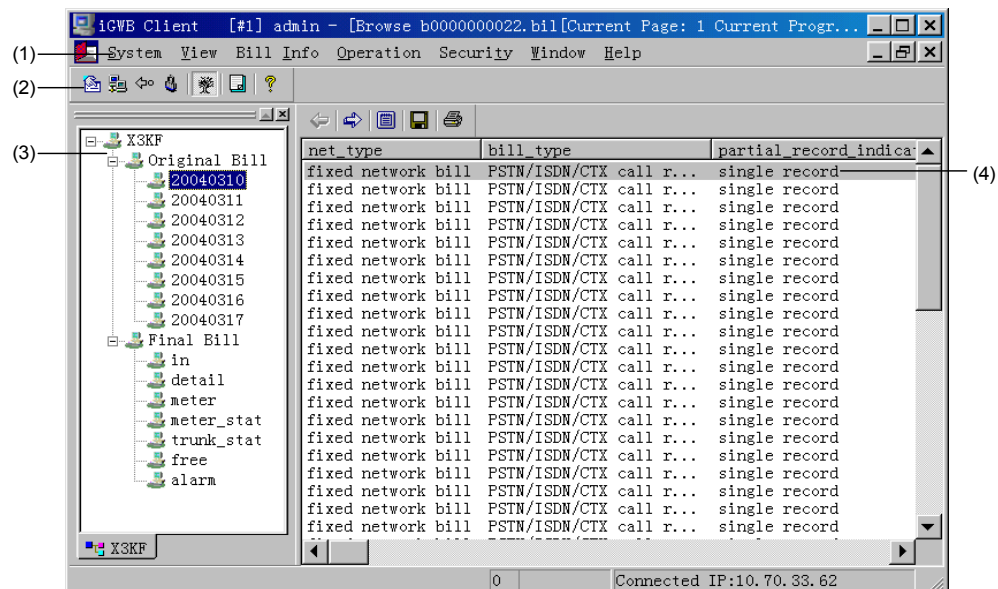
3.1 Introduction to CDR Console

CDR console, the client system of the iGWB, adopts graphical user interfaces (GUI). In terms of functional structure, the CDR console is composed of a system management part, a service function part, and a debugging function part. The major functions of each part are as follows:

- The system management part provides login, logout, office management, and system customization functions.
- The service function part provides CDR browse, CDR query, log browse, state query, and user management functions.
- The debugging function part provides functions to graphically display debugging information, protocol trace information, and service workflow information as well as saving the information, which facilitates debugging and troubleshooting tasks.

3.1.1 Graphical User Interfaces

The iGWB client is designed in the GUI manner and composed of a navigation tree, an operation window, a menu bar, and a toolbar, as shown in Figure 3-1.



- (1) Menu bar (2) Toolbar
(3) Navigation tree (4) Operation window

Figure 3-1 Main interface of CDR console

3.1.2 Menu Bar

On the CDR console, the menus dynamically vary with the current state. As shown in Figure 3-1, the [Bill Info] menu is available when you are browsing CDRs. Table 3-1 lists the menus on the main interface.








Table 3-1 Menus on the main interface of CDR console

Menu	Sub-menu	Function
System	Relogin	To log out and log in as another user.
	Logout	To log out from the current user account and end the current operation.
	Lock System	To lock the CDR console when it is not used. The corresponding shortcut key is F12.
	Office Management	To set the offices managed by the CDR console.
	System Customize	To set the automatic locking period and the response timeout of the system.
	Exit	To quit the CDR console.
View	Navigator Tree	To show or hide the navigation tree. The corresponding shortcut key is F2.
	Toolbar	To show or hide the toolbar.
	Status Bar	To show or hide the status bar.
	Refresh	To refresh the interface display. The corresponding shortcut key is F5.
Operation	Debug	To enter the system debugging mode.
	State Query	To enter the state query mode.
	Switch	To manually switch over the active and standby iGWB servers.
	Upgrade	To execute an auxiliary upgrade of the system.
Security	Log Browse	To view the operation records.
	Operator Management	To enter the operator management mode.
Window	Cascade	To cascade all windows.
	Tile	To tile all windows.
	Arrange Icons	To arrange all window icons.
	Close All	To close all windows.
Help	Help Topics	To open the help.
	About iGWB	To display the product version information.

3.1.3 Toolbar

The toolbar provides shortcuts to the frequently performed operations. On the toolbar, the shortcut icons also dynamically vary with the current state. Table 3-2 lists the shortcuts on the toolbar.

Table 3-2 Toolbar on the main interface

Shortcut	Matched menu option	Function
	Relogin	To log out and log in as another user.
	Office Management	To set the offices managed by the CDR console.
	Logout	To log out from the current user account and end the current operation.
	Lock System	To lock the CDR console when it is not used.
	Navigator Tree	To show or hide the navigation tree.
	Debug	To enter the system debugging mode.
	Help Topics	To open the help.

3.2 System Management

3.2.1 CDR Console Management

To use CDR console functions, log in to the client. After the use, be sure to log out for the sake of security.

I. Starting CDR console

- 1) Select [Start/Programs/iGateway Bill V200 Client/iGWB Client] to start the CDR console. The [Login] dialog box is displayed, as shown in Figure 3-2.

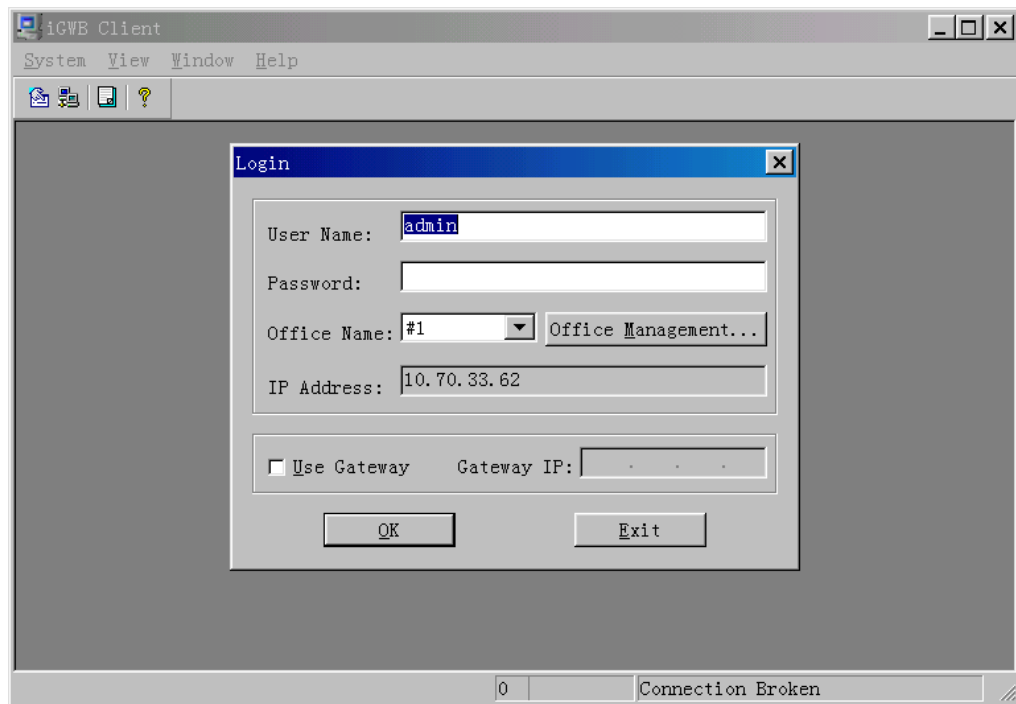


Figure 3-2 [login] dialog box

- 2) Enter a user name and the correct password. Select the office to be managed. Click <OK>. The window as shown in Figure 3-3 is displayed. The navigation tree of CDR files is displayed in the left pane of the window.

Note:

For a newly installed iGWB client, the user name is admin and the password is null by default.

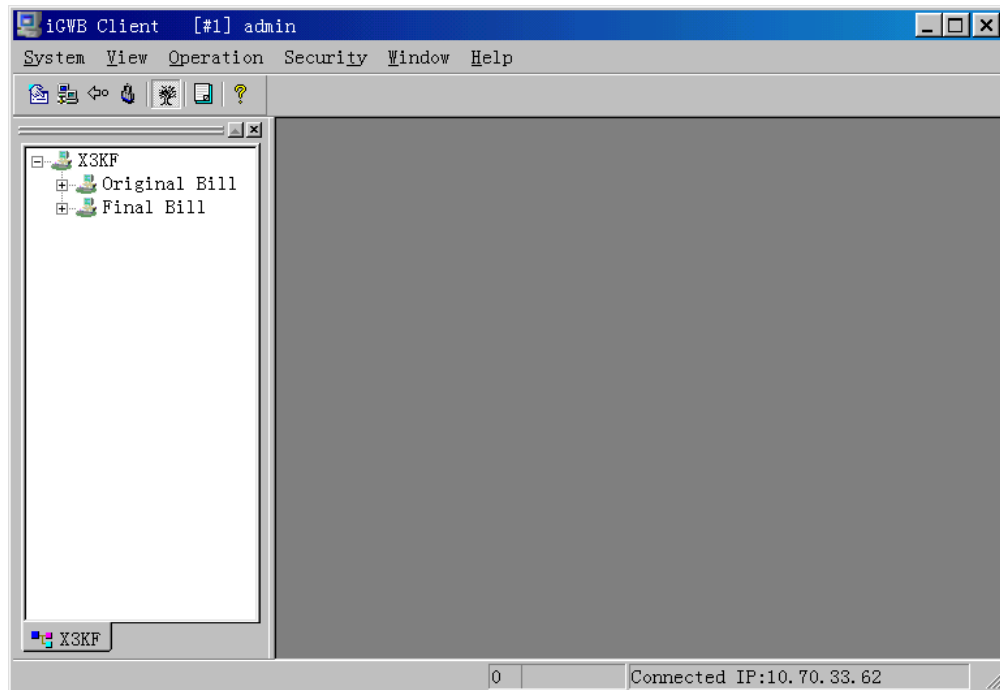


Figure 3-3 Main interface of CDR console after login

II. Exiting CDR console

On the main interface of the CDR console, select [System/Exit]. A confirmation dialog box is displayed. Confirm it to exit the CDR console.

III. logging out

On the main interface of the CDR console, select [System/Logout], or click the icon



on the toolbar. A confirmation dialog box is displayed.

Confirm it, and the system will clear the contents of the navigation tree, and closes all windows of the CDR console.

IV. Re-logging in

1) On the main interface of the CDR console, select [System/Relogin], or click the



icon on the toolbar. If the user has logged in, the system prompts whether to log out the current user. Click <OK>, and the [Login] dialog box is displayed. If the user has not logged in, the [Login] dialog box is displayed directly, as shown in Figure 3-4.

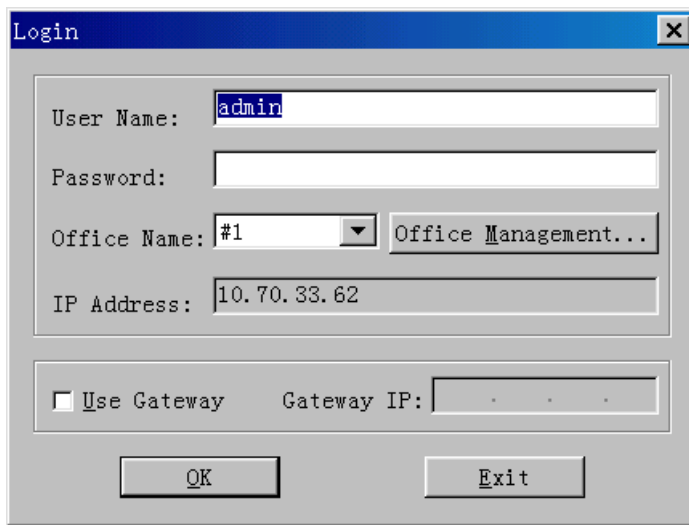


Figure 3-4 [Login] dialog box

- 2) In the [Login] dialog box, enter the user name and password. Select the name of the office to be managed. Click <OK>.

The navigation tree is displayed after the successful login.

V. Locking system

When you are not operating the CDR console terminal, lock it to avoid unauthorized operations.

- 1) On the main interface of the CDR console, select [System/Lock System], or click



the icon on the toolbar (or press <F12>). The [Lock System] dialog box is displayed, as shown in Figure 3-5.



Figure 3-5 [Lock System] dialog box

- 2) To unlock the system, enter the correct password, and click <OK>. If you click <Relogin>, the system will clear the navigation tree, close all the windows, and display the [Login] dialog box as shown in Figure 3-4.


3.2.2 Office Management

Office refers to an iGWB server site maintained by the CDR console.

The purpose of office management is to set the IP address of the office. The system supports simultaneously setting the IP addresses of several offices. The client can select an office to maintain.


I. Switching managed offices

When a CDR console manages more than one iGWB office, this operation is used to switch between the managed offices. This operation is the same as "Relogin".

- 1) On the main interface of the CDR console, select [System/Relogin], or click the  icon on the toolbar. If the user has logged in, the system prompts whether to log out the current user. Click <OK>, and the [Login] dialog box is displayed. If the user has not logged in, the [Login] dialog box is displayed directly.
- 2) In the [Login] dialog box, enter the user name and password. Select the name of the office to be managed. Click <OK>.

The navigation tree is displayed after the successful login.

II. Adding office

- 1) Obtain the IP address of the iGWB office to be added (the IP address for the server to connect the network management system). Determine the name of the office.
- 2) On the CDR console, select [System/Office Management], or click the  icon on the toolbar. The [Office Management] dialog box is displayed, as shown in Figure 3-6.

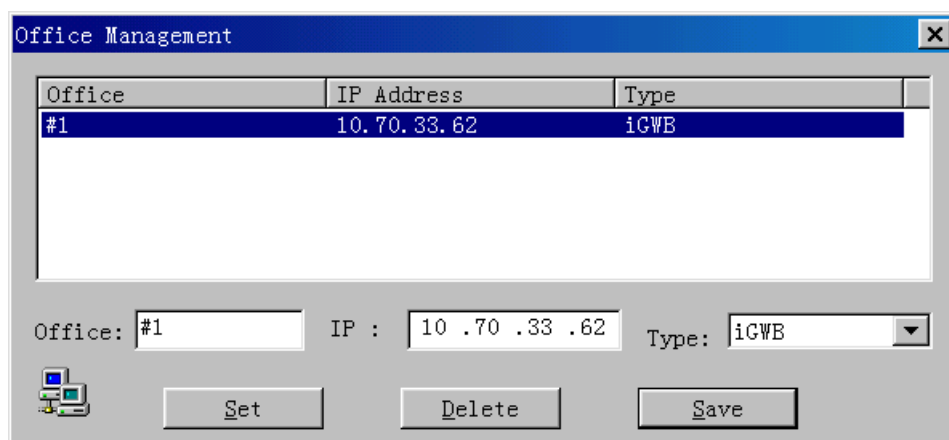




Figure 3-6 [Office Management] dialog box

- 3) In the dialog box, set the parameters of the office, including the office name, IP address, and type (only iGWB is available). Click <Set>. The information of the office is added in the list box. Confirm it, and click <Save> to complete the addition of the office.

III. Deleting office

- 1) Obtain the IP address of the iGWB office to be deleted (the IP address for the server to connect the network management system) and the name of the office.
- 2) On the CDR console, select [System/Office Management], or click the  icon on the toolbar. The [Office Management] dialog box is displayed, as shown in Figure 3-6.
- 3) In the list box, select the office to be deleted. Click <Delete>. The information of the office is removed from the list box. Confirm it, and click <Save> to complete the deletion of the office.

IV. Modifying office

- 1) Obtain the IP address of the iGWB office to be modified (the IP address for the server to connect the network management system) and the name of the office.
- 2) On the CDR console, select [System/Office Management], or click the  icon on the toolbar. The [Office Management] dialog box is displayed, as shown in Figure 3-6.
- 3) In the list box, select the office to be modified. Enter the new IP address of the office. Click <Set>. The information of the office is updated in the list box. Confirm it, and click <Save> to complete the modification of the office.



Caution:

When starting the client for the first time, be sure to configure the IP address of the server at the client. Otherwise, the client does not know which office it is connected to. Therefore, when you select [Start/Programs/iGateway Bill V200 Client/iGWB Client] to start the main interface of the CDR console and the [Login] dialog box is displayed as shown in Figure 3-2, you should click <Office Management> in the [Login] dialog box and add an office in the [Office Management] dialog box before login.

3.2.3 System Customization

I. Customizing timeout setting

This operation is used to customize the maximum interval (that is, timeout setting) before the system responds after a command is submitted. If the duration exceeds this interval, the terminal system determines that the command is time out and provides a prompt.

- 1) On the CDR console, select [System/System Customize]. The [System Customize] dialog box is displayed, as shown in Figure 3-7.

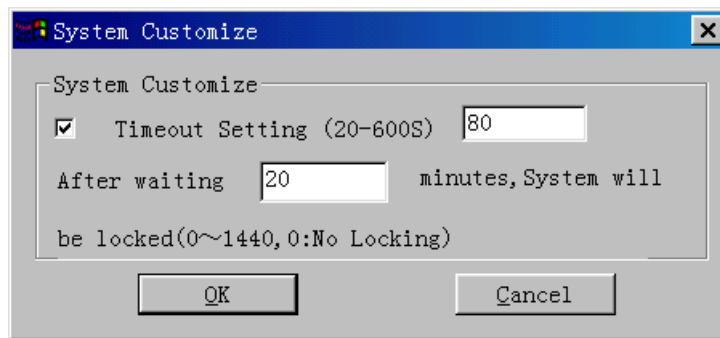


Figure 3-7 [System Customize] dialog box

- 2) Select the [Timeout Setting] check box. Enter the customized time value. (That value is in the range of 20 to 600 seconds.)

II. Customizing automatic locking time

This operation is used to set whether to lock the CDR console when necessary and, if lock, how long to wait. If no operations are performed on the CDR console for the defined time, the CDR console will be locked automatically. To unlock the system, enter the correct password.

Select [System/System Customize]. The [System Customize] dialog box is displayed, as shown in Figure 3-7.

Enter the duration (in minutes) before the system is automatically locked. The time value ranges from 0 to 1440 minutes. If it is set to "0", the system will not be locked.

3.2.4 View Functions

I. Showing or hiding navigation tree

Select [View/Navigator Tree]. If there is a check mark “√” before the [Navigator Tree] option, the navigation tree is shown. Otherwise, it is hidden. Click that menu option or press <F2>, and the navigation tree is shown or hidden.

II. Showing or hiding toolbar

Select [View/ToolBar]. If there is a check mark “√” before the [ToolBar] option, the toolbar is shown. Otherwise, it is hidden. Click that menu option, and the toolbar is shown or hidden.

III. Showing or hiding status bar

Select [View/StatusBar]. If there is a check mark “√” before the [StatusBar] option, the status bar is shown. Otherwise, it is hidden. Click that menu option, and the status bar is shown or hidden.

3.3 Service Operations

3.3.1 CDR Management

The CDR console provides the CDR management functions to browse, query, or print CDRs.

I. Browsing CDR

To browse the CDRs based on the generation time and CDR type, proceed as follows:

- 1) After you log in to the CDR console, the main interface as shown in Figure 3-8 is displayed.

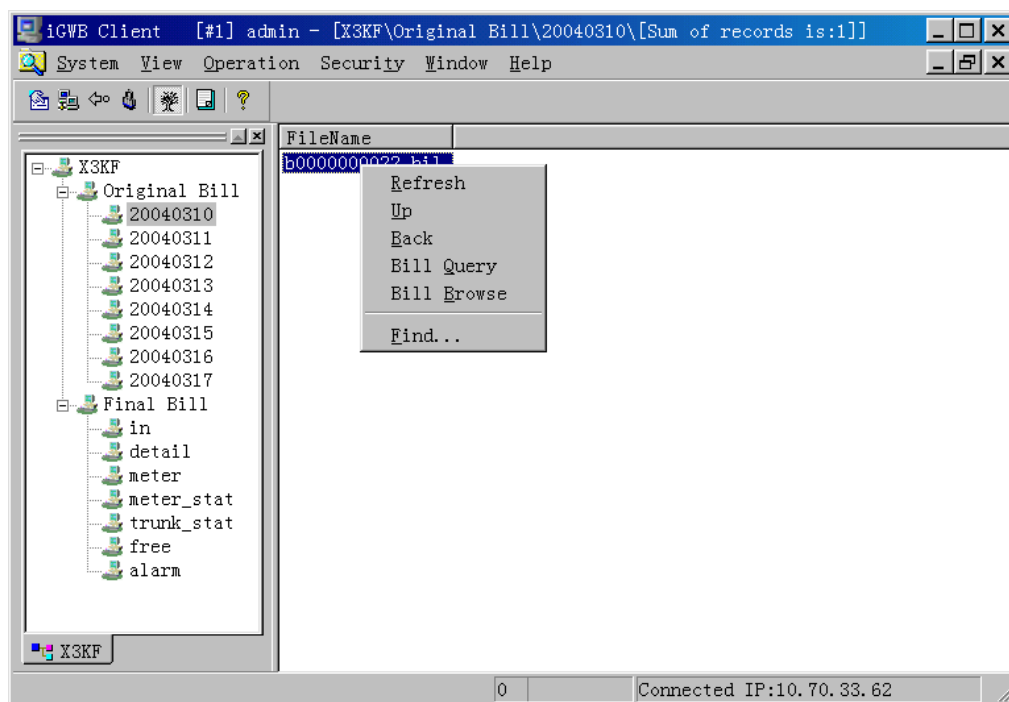


Figure 3-8 Main interface of CDR console

The left pane shows the navigation tree of the CDR console. The navigation tree visually displays the CDR storage mode in the server. Under [Original Bill], the original CDRs are displayed according to date, and the corresponding CDR file is *.bil. Under [Final Bill], several types of final CDRs supported by the system are displayed, which are also called “channel”, and the corresponding CDR file is *.dat. See Figure 3-8. The options on the right-click menu are described as follows:

- Clicking [Refresh] re-obtains data from the server or from the navigation tree to update the file list.
 - Clicking [Up] opens the upper-level directory list.
 - Clicking [Back] opens the directory opened last time.
 - Clicking [Bill Query] queries the CDRs according to the specified conditions.
 - Clicking [Bill Browse] displays the contents of the selected CDR.
 - Clicking [Find] invokes the search dialog box.
- 2) Double-click a CDR file. The [Choose Bill Format for File Browsing] dialog box is displayed, as shown in Figure 3-9.

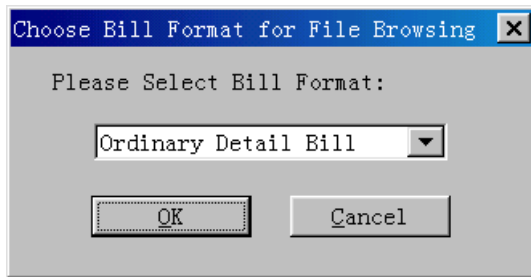


Figure 3-9 [Choose CDR Format for File Browsing] dialog box

The CDR formats available in the window include the following:

- Ordinary detail CDR
 - Free statistics CDR
 - Intelligent network CDR
 - Meter table statistics CDR
 - Meter table CDR
 - Alarm CDR
- 3) Select a desired CDR format. All the CDRs in the selected format in the original CDR files are displayed, as shown in Figure 3-10. If the CDRs are displayed in more than one page, right-click and select [Next Page] to view other pages.

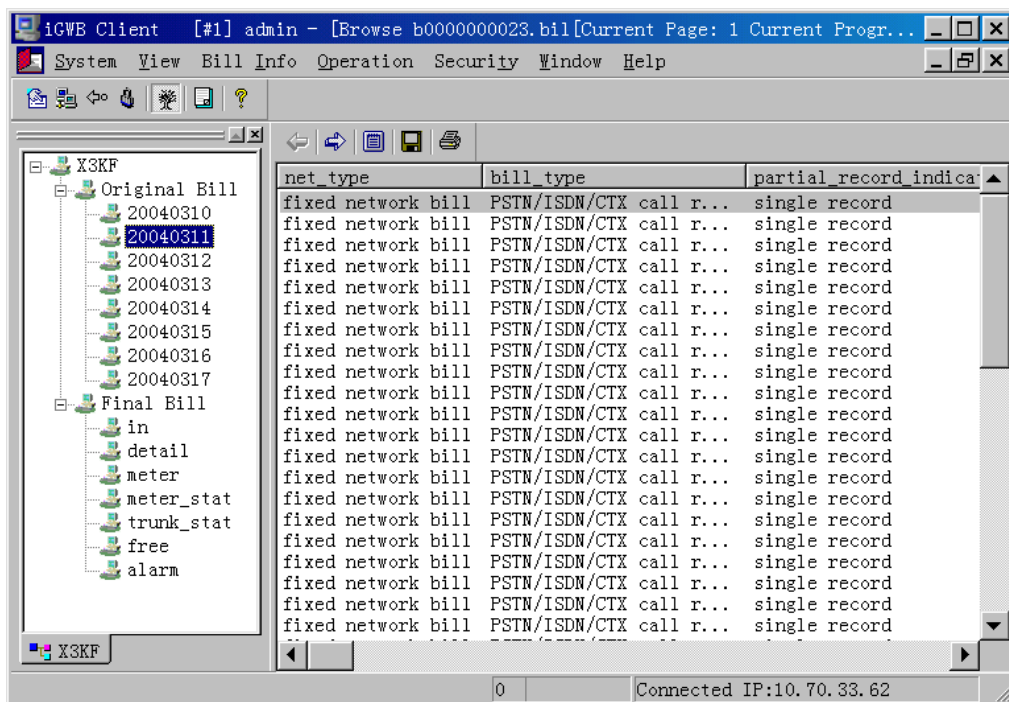


Figure 3-10 CDR list window

- 4) Double-click a particular CDR. The CDR details are displayed in a list box, as shown in Figure 3-11.

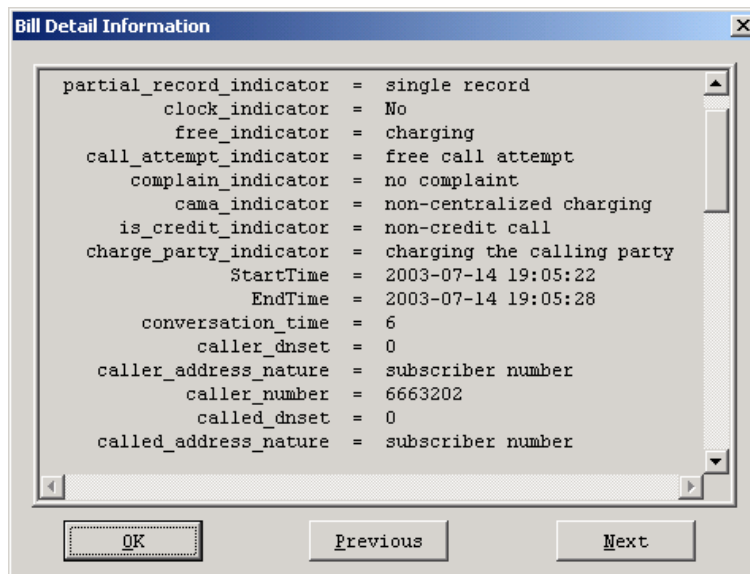



Figure 3-11 CDR details

The CDR details vary with the CDR type. For more, refer to *U-SYS SoftX3000 SoftSwitch System Technical Manual-Structure & Principle*.

After viewing the CDR, click <OK> to close the window.

II. Saving CDR information

To save all or selected CDR records to the client in the text format for future reference, proceed as follows:

- 1) In the CDR browse state, select [Bill Info/Save], or click the  icon on the toolbar, or select [Save] from the right-click menu. The [Save Bill Information] dialog box is displayed, as shown in Figure 3-12.

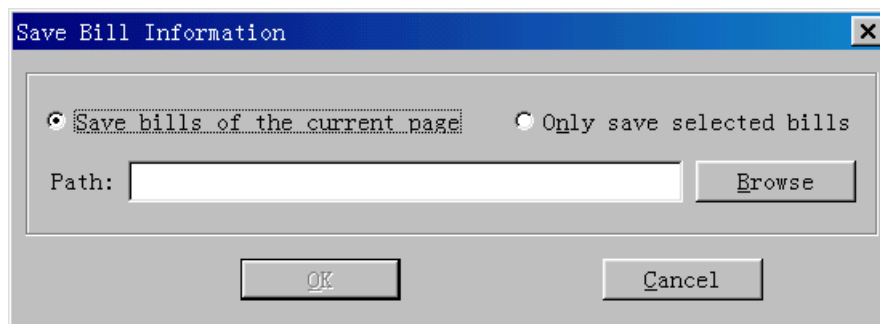


Figure 3-12 [Save Bill Information] dialog box

- 2) According to your requirement, select [Save bills of the current page] or [Only save selected bills]. Enter the name and the path of the destination file to save in, or select an existing path by clicking <Browse>. Click <OK> to save the CDRs.

III. Querying CDR

- 1) In the CDR file list window, right-click and select [Bill Query]. A dialog box as shown in Figure 3-13 is displayed.

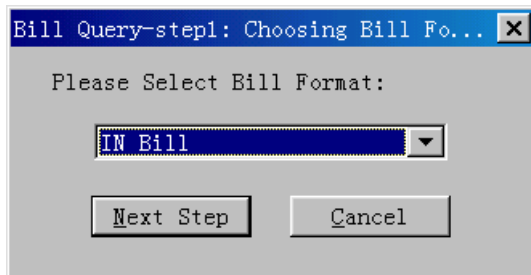


Figure 3-13 [Bill Query-step1: Choosing Bill Format] dialog box

- 2) Select a desired CDR format. Click <Next Step>. The dialog box as shown in Figure 3-14 is displayed.

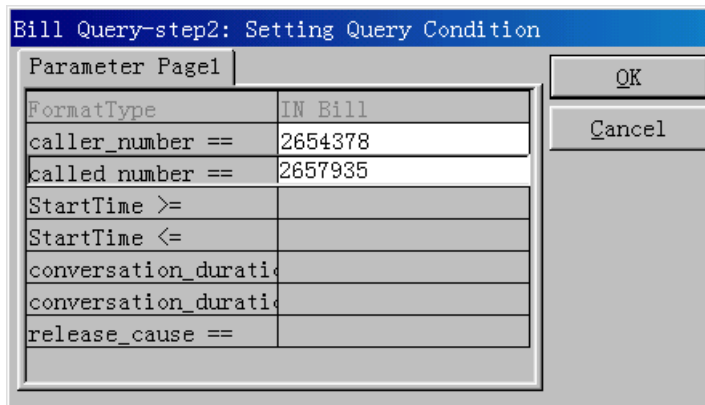


Figure 3-14 [Bill Query-step2: Setting Query Condition] dialog box


Note:

CDR query conditions vary with CDR formats.

- 3) Set the query conditions in the fields. Click <OK>. If the records matching the conditions are found, the CDR query result window will be displayed.

If the CDRs are displayed in more than one page, right-click and select [Next Page] to view other pages.

IV. Printing CDR

In the CDR list window as shown in Figure 3-10, select the CDR to be printed. Select [Bill Info/Print], or click the  icon in the toolbar of the CDR browse window to print the selected CDR.

3.3.2 State Query

I. Querying state

To query the running state of the iGWB such as CPU usage, heartbeat state, and disk usage, proceed as follows:

- 1) In the main window of the CDR console, select [Operation/State Query]. The [State Query] window is displayed with the current state information of the server, as shown in Figure 3-15.

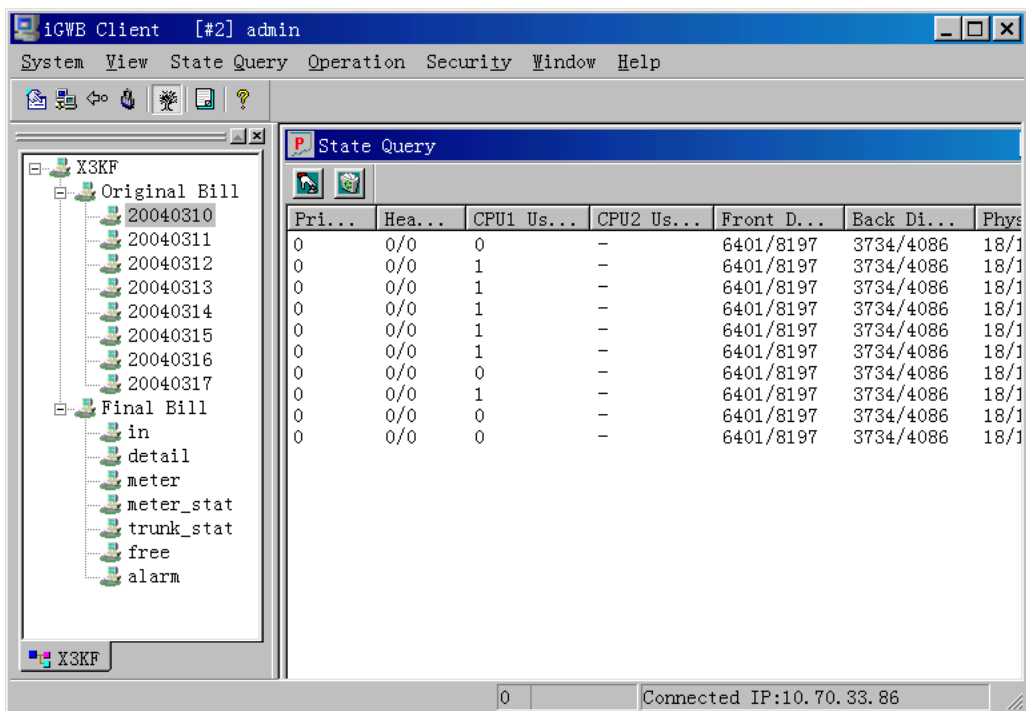


Figure 3-15 [State Query] window

- 2) Double-click any entry. The system opens a window, dynamically displaying the information of all the items. See Figure 3-16.

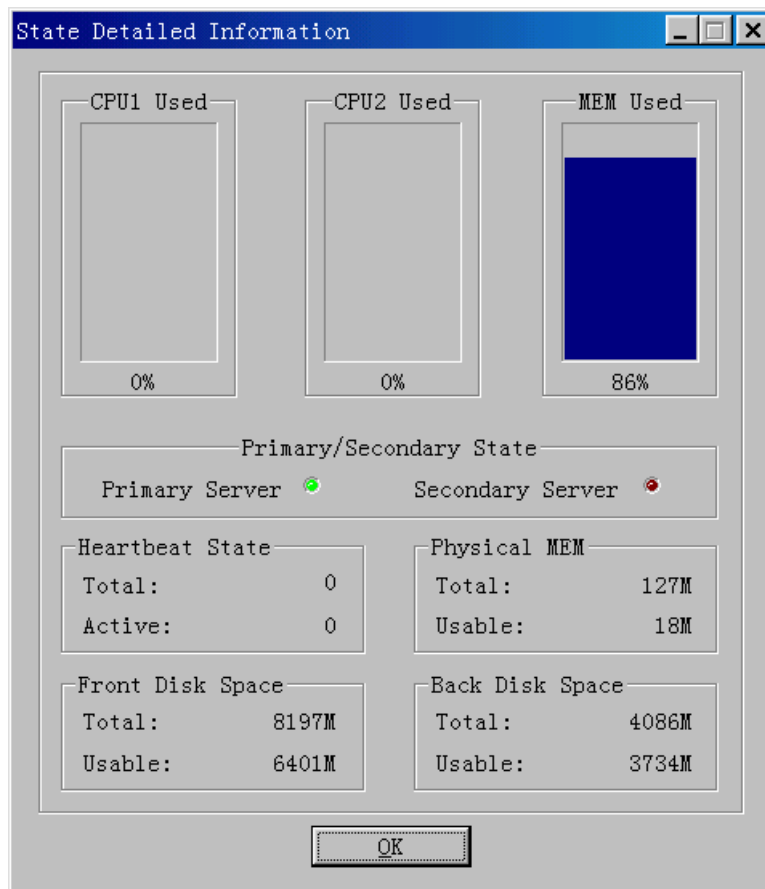


Figure 3-16 [State Detailed Information] window

The items in the [State Detailed Information] window are interpreted as follows:

- [CPU1 Used] and [CPU2 Used] indicate the CUP usage of the dual systems.
- [MEM Used] indicates the memory usage.
- [Primary/Secondary State] indicates the state of the active/standby server. If the server is operating well, the corresponding green indicator is lit.
- [Heartbeat State] indicates the working state of the heartbeat links.

[Total] indicates the total number of heartbeat links. [Active] indicates the number of active heartbeat links.

- [Physical MEM] indicates the usage of the physical memory.

[Total] indicates the total capacity. [Usable] indicates the available size of the physical memory.

- [Front Disk Space] indicates the space for storing the original CDRs.


[Total] indicates the total capacity. [Usable] indicates the available size.

- [Back Disk Space] indicates the space for storing the backup CDRs.

[Total] indicates the total capacity. [Usable] indicates the available size.

II. Setting properties of state query

This operation is used to set the properties of state query, including whether to automatically save the query results and the state refreshing period during the query.

When the state query window is opened, select [State Query/Setting Properties] on the main window of the CDR console, or click the  icon on the toolbar. The [Setting Properties] dialog box is displayed, as shown in Figure 3-17.

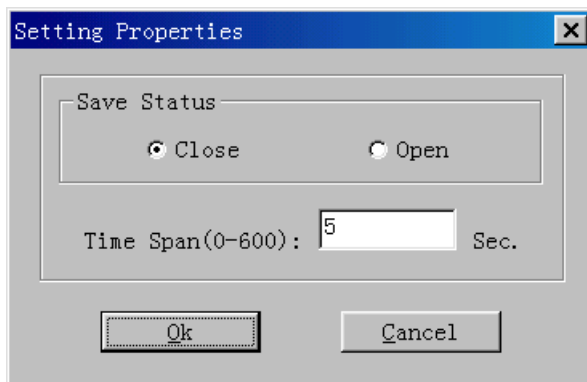


Figure 3-17 [Setting Properties] dialog box

Modify [Save Status] and [Time Span] as required.

- [Save Status] means whether to save the state information in the state query window to the StatsInfo.txt file on the client installation directory. If the status is [Close], the information will not be saved; if the state is [Open], the state information will be saved.
- [Time Span] refers to the refreshing time interval in the range of 0 to 600 seconds, which is used for refreshing the state information at the server.

3.3.3 Log Management

I. Browsing log

The system and operation logs are helpful in system maintenance. To browse a log, proceed as follows:

- 1) In the main window of the CDR console, select [Security/Log Browse]. The [LogView] window is displayed. See Figure 3-18.

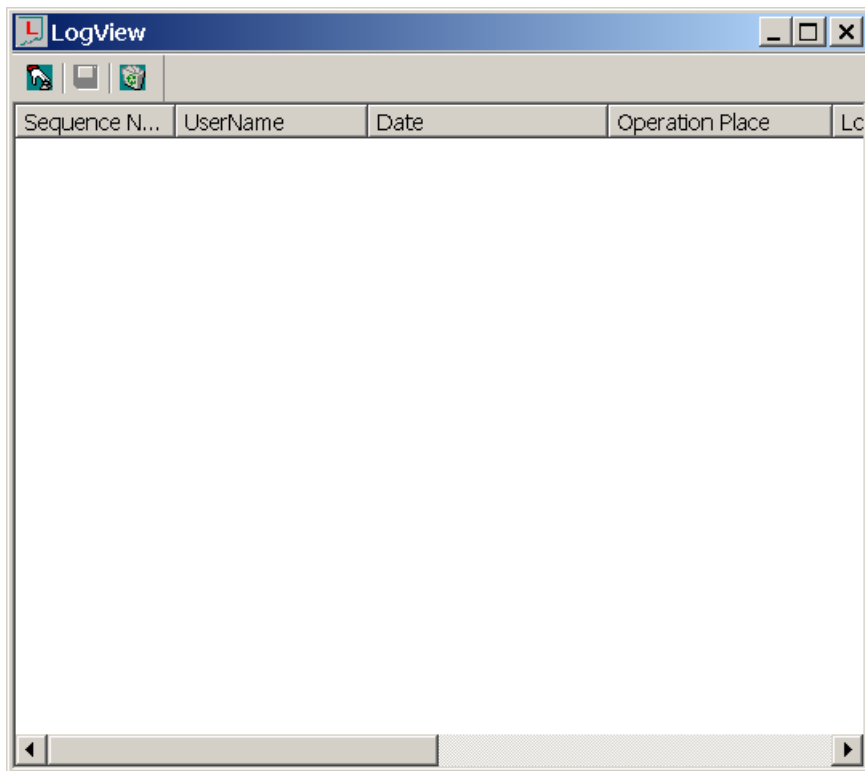



Figure 3-18 [LogView] window

- 2) In the main window of the CDR console, select [Log/Browse Log], or in the [LogView] window, click the  icon on the toolbar. The [Set Log Browse Property] dialog box is displayed, as shown in Figure 3-19.

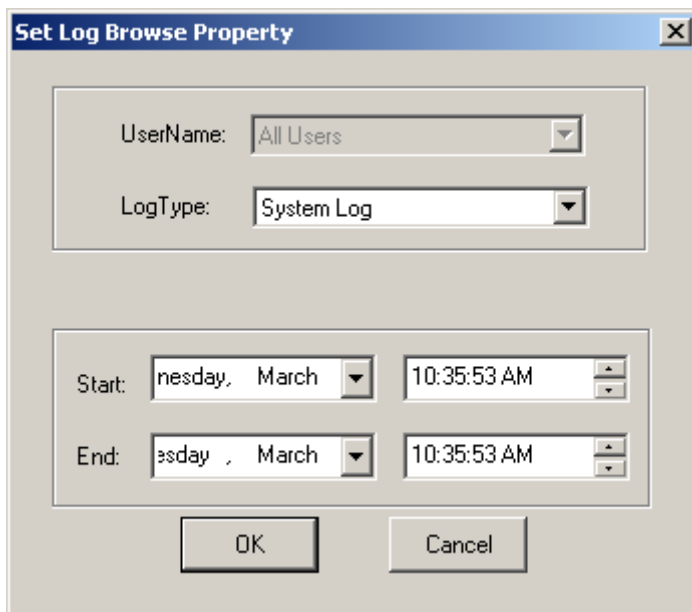
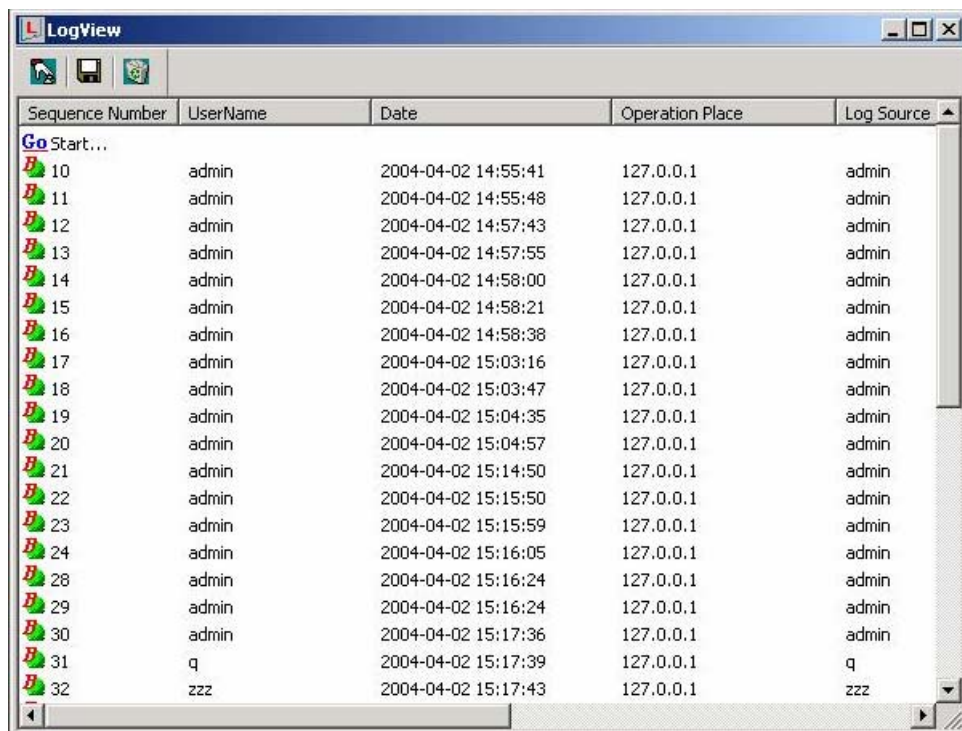


Figure 3-19 [Set Log Browse Property] dialog box

- 3) Enter the log browse conditions.
 - The [UserName] field indicates the object for which a log is generated. The drop-down options include [All Users] and created users. [All Users] indicates all the users that have been created.
 - In the [LogType] list, [System Log] and [Operation Log] are available. The system log records the operations of the software modules of the system. The operation log records the operations of users.
 - The [Start] and [End] fields indicate the time range during which the log is generated.

There are two types of operator authorities at the client: administrator authority and normal user authority. If logging in as an administrator, you can browse the system log and the operation logs of all users. If logging in as a normal user, you can browse only your own operation log.

- 4) Select the user name and the type of the log to be browsed. Set the start time and the end time. Click <OK>. The found log list is displayed in the [LogView] window, as shown in Figure 3-20.



Sequence Number	UserName	Date	Operation Place	Log Source
Go Start...				
10	admin	2004-04-02 14:55:41	127.0.0.1	admin
11	admin	2004-04-02 14:55:48	127.0.0.1	admin
12	admin	2004-04-02 14:57:43	127.0.0.1	admin
13	admin	2004-04-02 14:57:55	127.0.0.1	admin
14	admin	2004-04-02 14:58:00	127.0.0.1	admin
15	admin	2004-04-02 14:58:21	127.0.0.1	admin
16	admin	2004-04-02 14:58:38	127.0.0.1	admin
17	admin	2004-04-02 15:03:16	127.0.0.1	admin
18	admin	2004-04-02 15:03:47	127.0.0.1	admin
19	admin	2004-04-02 15:04:35	127.0.0.1	admin
20	admin	2004-04-02 15:04:57	127.0.0.1	admin
21	admin	2004-04-02 15:14:50	127.0.0.1	admin
22	admin	2004-04-02 15:15:50	127.0.0.1	admin
23	admin	2004-04-02 15:15:59	127.0.0.1	admin
24	admin	2004-04-02 15:16:05	127.0.0.1	admin
28	admin	2004-04-02 15:16:24	127.0.0.1	admin
29	admin	2004-04-02 15:16:24	127.0.0.1	admin
30	admin	2004-04-02 15:17:36	127.0.0.1	admin
31	q	2004-04-02 15:17:39	127.0.0.1	q
32	zzz	2004-04-02 15:17:43	127.0.0.1	zzz

Figure 3-20 List of found logs

- 5) Double-click a log entry, or select it and press <Enter>. The [Detail Information of Log] window is displayed. See Figure 3-21.

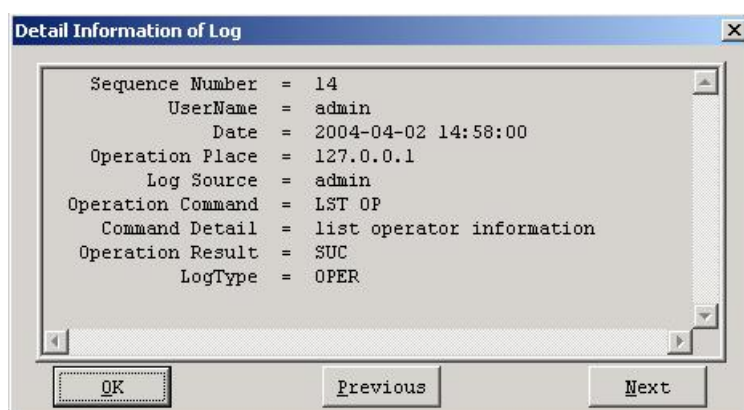


Figure 3-21 [Detail Information of Log] window


The log entry contains the following information:

- Sequence Number: The sequence number of the log entry.
- UserName: It is usually the same as Log Source, expressed in the manner of access point name (for example, x3k) plus log storage position (for example, frontsave).
- Date: The time when the operation is performed.
- Operation Place: The IP address of the workstation that sends the operation command.
- Log Source: The source of the log file. For example, "(x3k) mt_frontsave" refers to the original CDR directory of the office x3k.
- Operation Command: The executed operation command.
- Command Detail: The details of the command, including the position (office) on which the command is executed, and the character string of the command.
- Operation Result: The execution result of the command. "SUC" indicates that the command is executed successfully. "FAIL" indicates that the command is unsuccessfully.
- LogType: The type of the log. "SYS" represents the system log. "OPER" represents the operation log.

To view the contents of the next log entry, click <Next>. To view the details of the previous log entry, click <Previous>.

II. Saving log information

To save all or selected log entries to the client in the text format for future reference, proceed as follows:

- 1) In the main window of the CDR console, select [Log/Save to File], or in the [LogView] window, click the  icon on the toolbar. The [Save Log Information] dialog box is displayed, as shown in Figure 3-22.

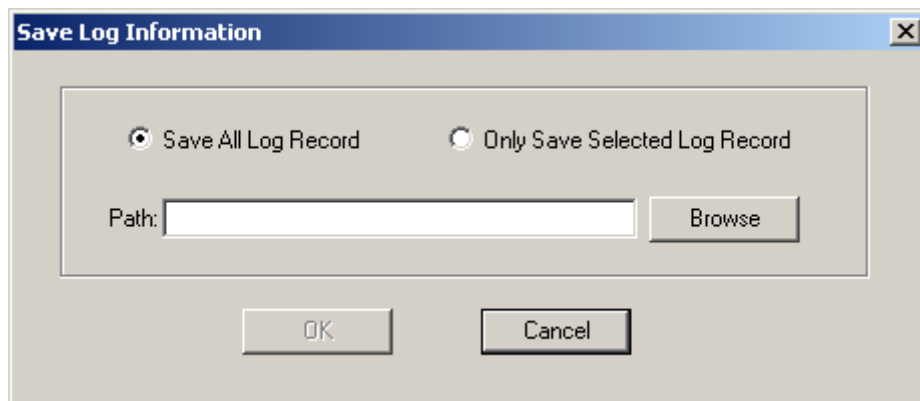


Figure 3-22 [Save Log Information] dialog box

- 2) According to your requirement, select [Save All Log Record] or [Only Save Selected Log Record]. Enter the name and the path of the destination file to save in, or select an existing path by clicking <Browse>. Click <OK> to save them.

3.3.4 User Management

In the main window of the CDR console, select [Security/User Management]. The [Operator Management] window is displayed. See Figure 3-23.

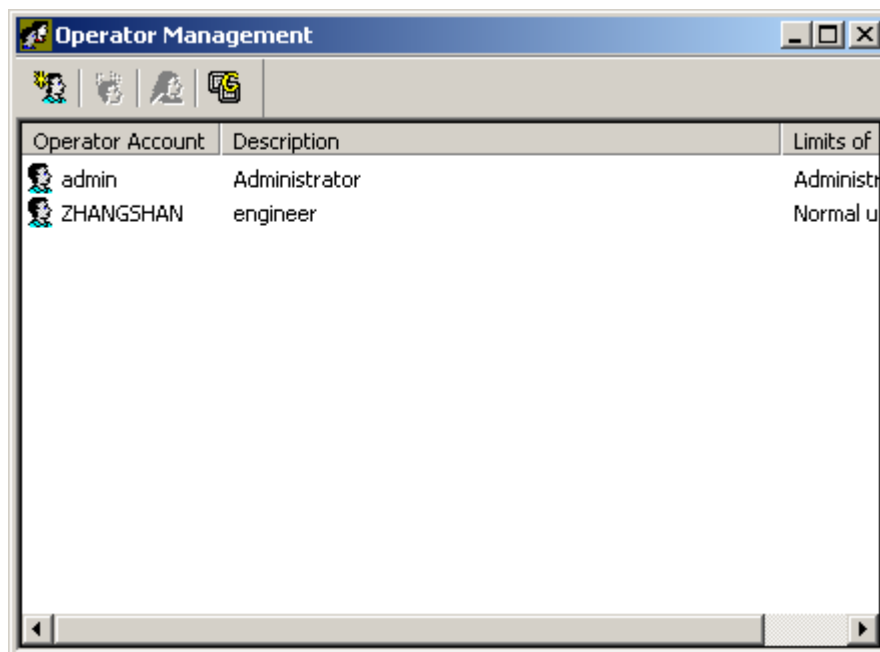



Figure 3-23 [Operator Management] window

I. Adding operator

To add an operator with "Normal User" authorities, proceed as follows:

Log in as an administrator. In the main window of the CDR console, select [User/Add], or in the [Operator Management] window, click the  icon on the toolbar. The [Add Operator] dialog box is displayed, as shown in Figure 3-24.

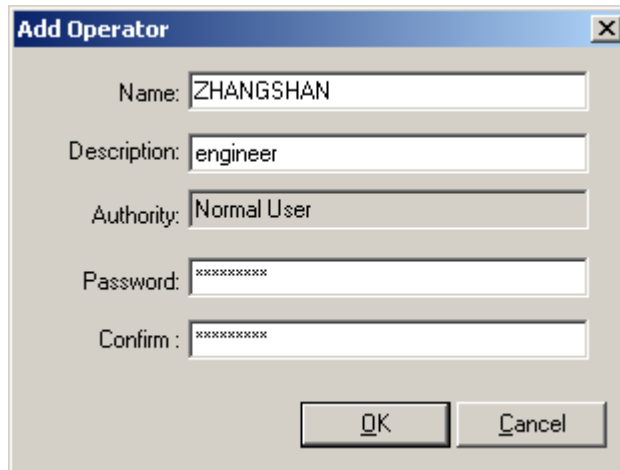


Figure 3-24 [Add Operator] dialog box

Set the parameters. Click <OK>.


View the [Operator Management] window, and you can find that the newly added operator is displayed.

Note:

After the client software is installed, the system will automatically create an administrator account, which is the only one in the system and cannot be deleted. An administrator can add or delete normal users, but a normal user has no authority to add or delete other users.

II. Deleting operator

To delete an unused operator with “Normal User” authorities, proceed as follows:

Log in as an administrator. In the [Operator Management] window as shown in Figure 3-23, select the operator to be deleted. In the main window of the CDR console, select [User/Delete], or in the [Operator Management] window, click the  icon on the toolbar. A confirmation dialog box is displayed, as shown in Figure 3-25.

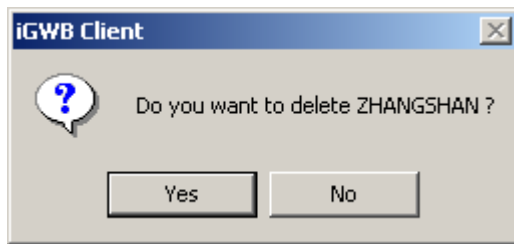



Figure 3-25 Deletion confirmation dialog box

Click <Yes> to delete the selected operator. Meanwhile, the user information list is refreshed and the operator is deleted.

III. Modifying operator properties

To modify the properties of an operator with “Normal User” authorities, including operator description and password, proceed as follows:

In the [Operator Management] window, select the operator account to be modified. In the main window of the CDR console, select [User/Modify], or in the [Operator

Management] window, click the  icon on the toolbar. The [Modify Operator Property] dialog box is displayed, as shown in Figure 3-26.

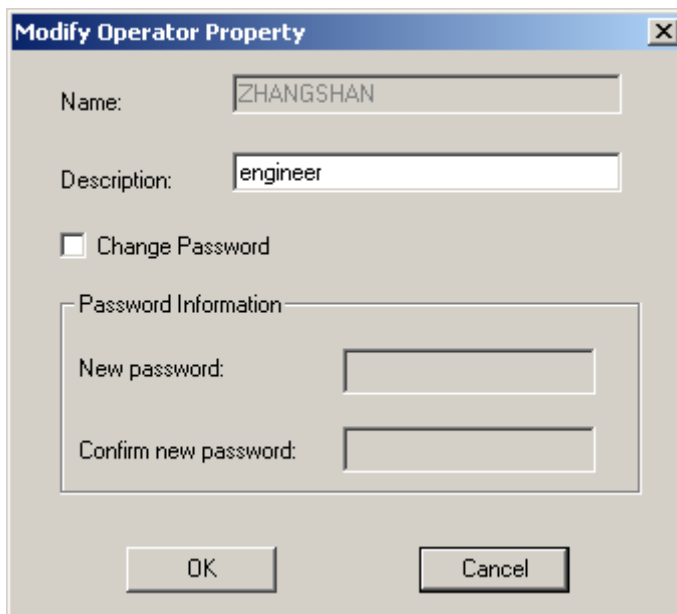


Figure 3-26 [Modify Operator Property] dialog box

Modify the operator description and the password. (The operator name cannot be modified.) Click <OK>.

 **Caution:**

An administrator can modify the operator description and password of itself and normal users.
A normal user can only modify the own description and password.

3.3.5 Other Functions

 **Caution:**

Only administrator has the authority to perform the following service functions.

I. Manual switchover

To forcedly switch over the active and standby iGWB servers, proceed as follows:

 **Caution:**

This is a dangerous operation, because a successful switchover will disconnect the server from the CDR console.

Log in as an administrator. In the main window of the CDR console, select [Operation/Switch]. A warning dialog box is displayed, as shown in Figure 3-27.

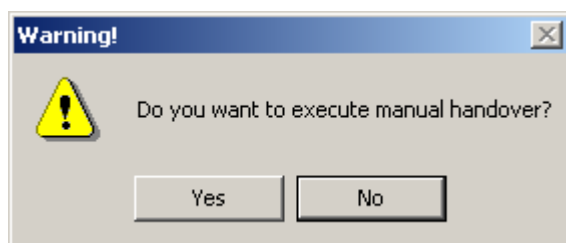


Figure 3-27 Configuration of manual switchover

Click <Yes> to start the switchover between the active and standby iGWB servers.

II. Auxiliary upgrade

The purpose of “auxiliary upgrade” is to make preparations for server software upgrade, such as combining all CDRs and stopping CDR receipt. Auxiliary upgrade is only applicable to a special upgrade. (For details about special upgrade, refer to Chapter 4 “System Maintenance”.)

Caution:

This is a dangerous operation, because CDRs might be lost. If this operation is mistakenly performed, restart the iGWB program.

Log in as an administrator. In the main window of the CDR console, select [Operation/Upgrade]. A warning dialog box is displayed, as shown in Figure 3-28.

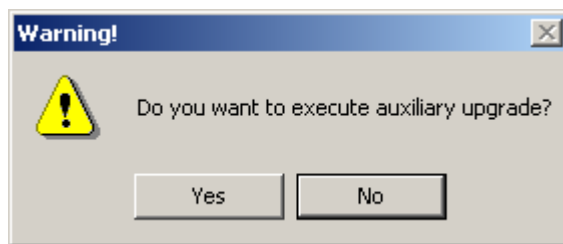



Figure 3-28 Confirmation of auxiliary upgrade

Click <Yes> to start the auxiliary upgrade of the iGWB server.

3.4 System Debugging

The iGWB debugger provides functions to display the debugging information, protocol trace information, and service workflow information in real time, and save the information as well.

- Debug information refers to the running state information of each module of the server, and it is displayed according to different levels.
- Protocol trace information is the message information between the SoftX3000 and the iGWB.
- Workflow information refers to the service message information among modules and processes at the server.

In the main window of the CDR console, select [Operation/Debug], or click the  icon on the toolbar. The debugging information browse window is displayed, as shown in Figure 3-29.

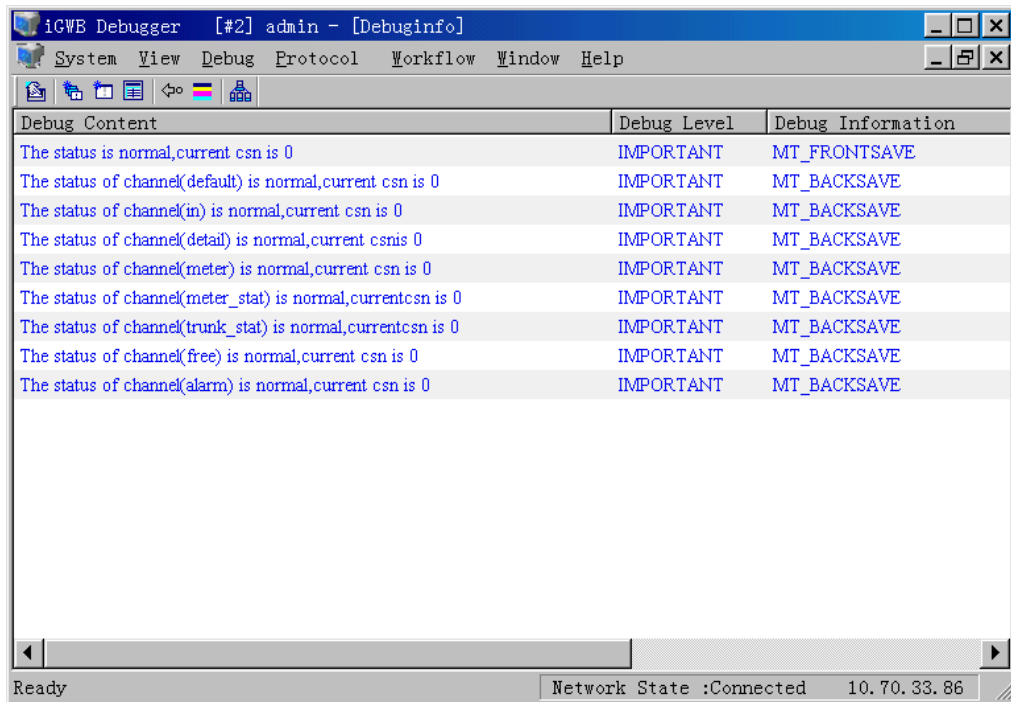



Figure 3-29 Debugging information browse window

3.4.1 Debugging Information

I. Browsing debugging information

This operation is used to browse the running state information of each module of the iGWB system in real time. It can be used as an auxiliary means for troubleshooting purposes.

When the debugger is started, the CDR console automatically opens the debug information window as shown in Figure 3-29. You can also select [Debug/Browse

Debug Message] in the debugger window as shown in Figure 3-29, or click the  icon on the toolbar to open the debugging information window.

Right-click in the debugging information window. A shortcut menu is displayed, as shown in Figure 3-30.

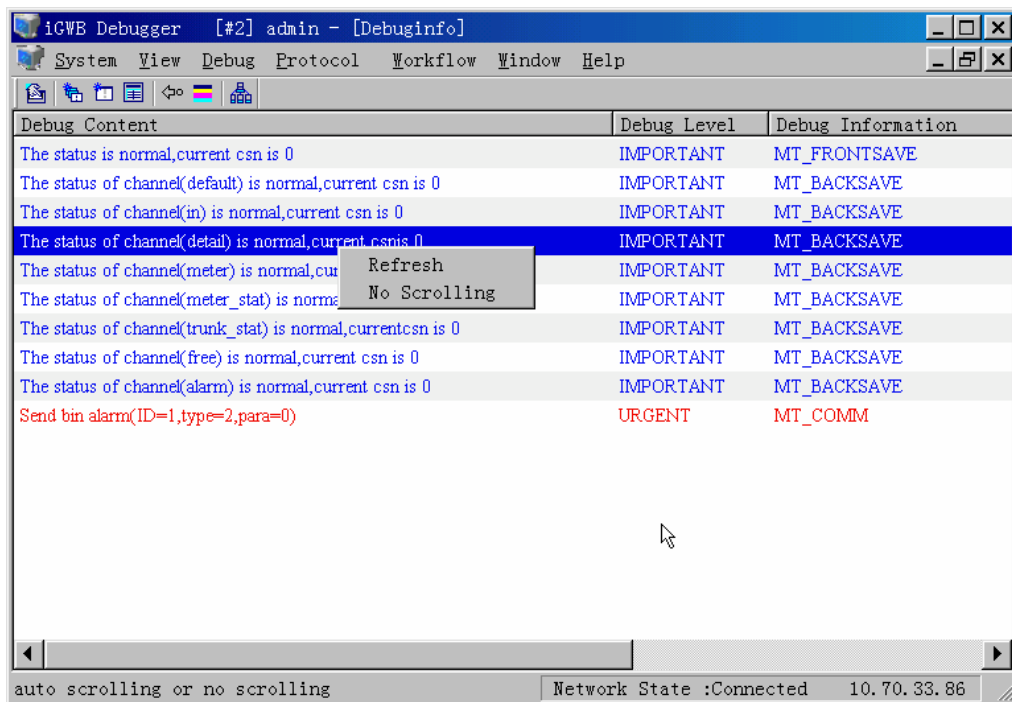


Figure 3-30 Right-click menu in browse window

With the right-click menu, the displayed information can be refreshed, and scrolling of the information can be disabled.

Note:

The right-click menu functions are also provided in the protocol trace information windows and workflow information window described later.

II. Saving debugging information in real time

This operation is used to save the debugging information in real time to the client for future reference.

This operation enables or disables the real-time saving switch.

In the debugger window, select [Debug/Save Debug Message] to enable the switch for saving the debugging information. (After the switch is enabled, a check mark “√” is displayed before the option.) The reported debugging information can be saved to the client in real time.

III. Listing, setting, and deleting mask level

By setting the mask level of the debugging information, the debugging information of specific levels can be masked and not be displayed in the browse window. The masked information is not deleted, but its display is controlled.



Caution:

Only administrator has the authority to perform the following operations.

1) Listing mask level

Log in as an administrator. In the debugger window, select [Debug/Mask Level/List Mask Level] to open the mask level query result window. The information of the masked level is displayed, as shown in Figure 3-31.

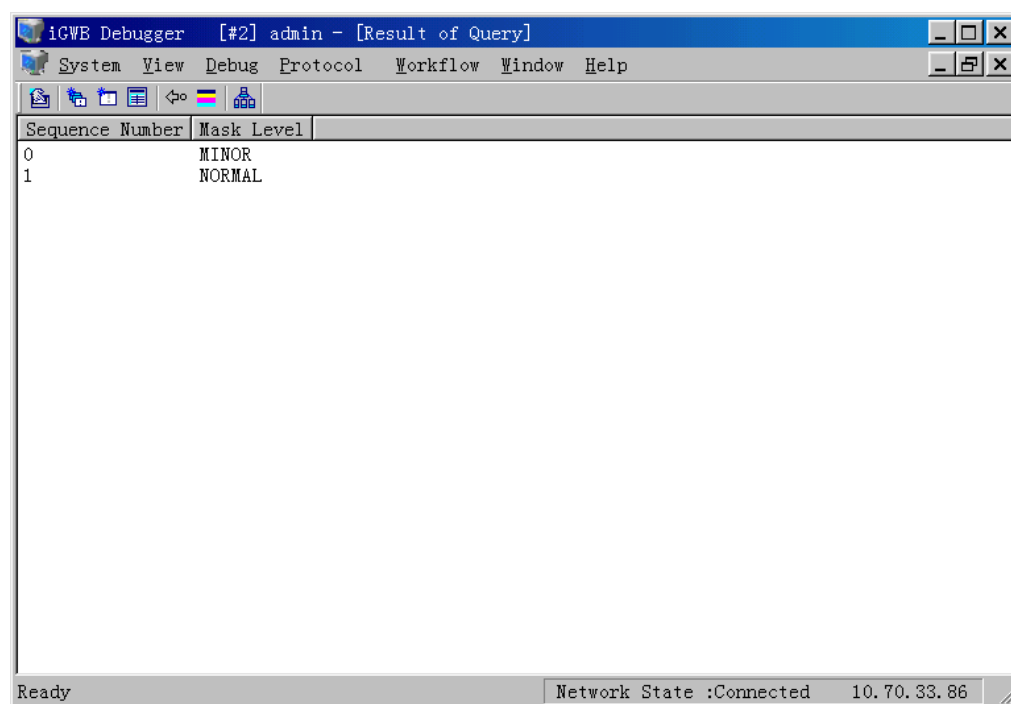


Figure 3-31 Query results of mask level

2) Setting mask conditions

Log in as an administrator. In the debugger window, select [Debug/Mask Level/Set Mask Level]. The [Add Mask Conditions] dialog box is displayed. See Figure 3-32.

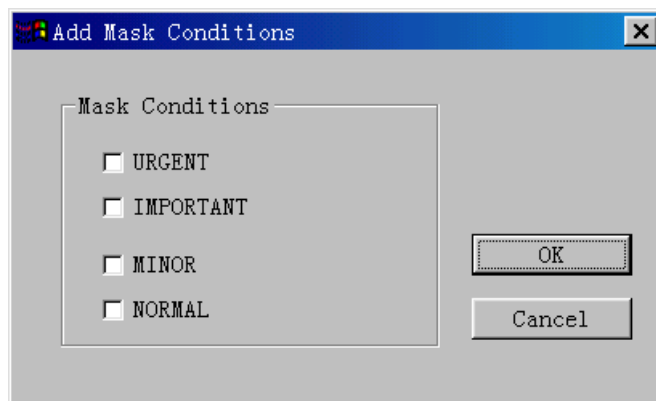


Figure 3-32 [Add Mask Conditions] dialog box

Select a mask condition as required. Click <OK>. A confirmation dialog box is displayed. Then the information of the selected debugging level is masked.

3) Deleting mask conditions

Right-click in the query result window. A shortcut menu is displayed, as shown in Figure 3-33.

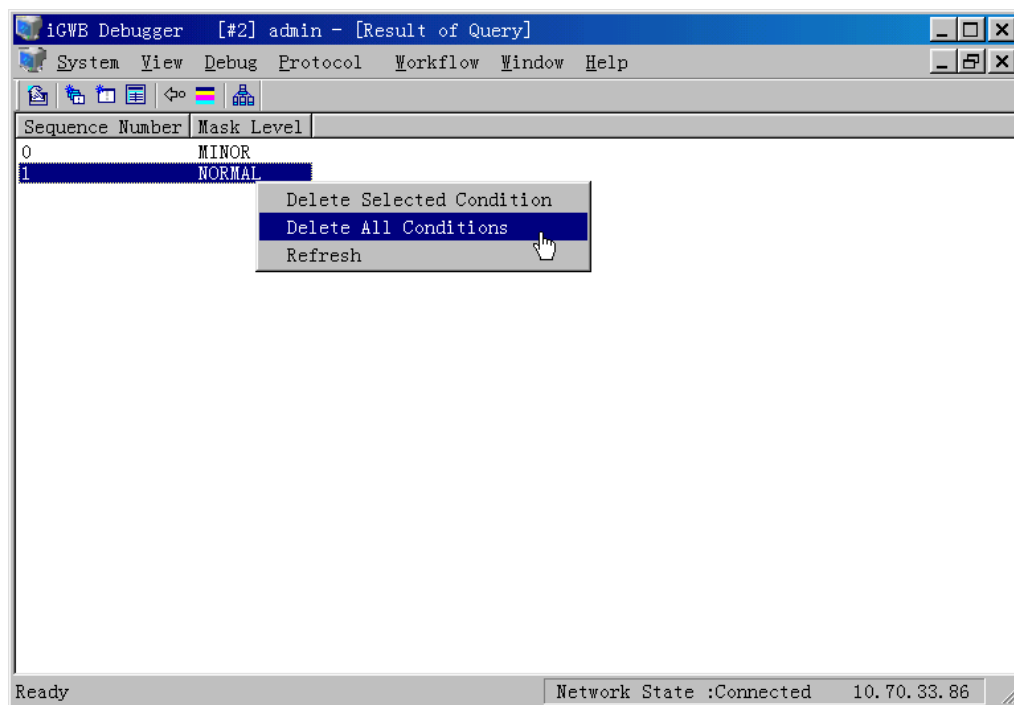



Figure 3-33 Right-click menu in mask level query result window

- To delete all mask conditions, click [Delete All Conditions] and confirm it.
- To delete a specified mask condition, click [Delete Selected Condition] and confirm it.
- To refresh the mask information list, click [Refresh].

IV. Setting debugging level color

The debugging information can be displayed in different colors according to different levels. This operation is used to change the displayed color of each level.

In the debugger window, select [System/Set Debug Color], or click the  icon on the toolbar. A [Set Debug Colors] dialog box is displayed, as shown in Figure 3-34.

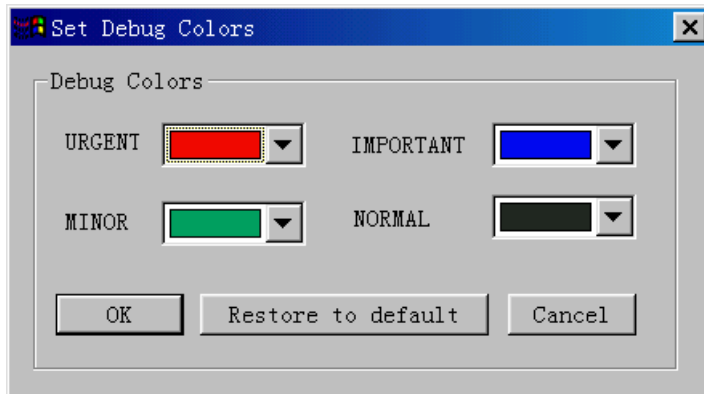


Figure 3-34 [Set Debug Colors] dialog box

Set the color for each level using the drop-down list. To restore the colors to the default settings, click <Restore to default>. Click <OK> to complete the setting.

3.4.2 Protocol Trace Information


The messages exchanged between the iGWB and the SoftX3000 can be traced for troubleshooting use.



Caution:

Only administrator has the authority to perform the following operations.

I. Browsing protocol trace information

Log in as an administrator. In the debugger window, select [Protocol/Browse Protocol Message], or click the  icon on the toolbar. The real-time protocol trace information window is displayed.

II. Saving protocol trace information in real time

Log in as an administrator. In the debugger window, select [Protocol/Save Protocol Message]. The reported protocol information can be saved in real time to a specified file.

3.4.3 Workflow Information


The messages exchanged between the iGWB and the SoftX3000 can be traced for troubleshooting use.



Caution:

Only administrator has the authority to perform the following operations.

I. Browsing workflow information

Log in as an administrator. In the debugger window, select [Workflow/Browse Workflow Message] or click the  icon on the toolbar. The real-time workflow information window is displayed.

The screenshot shows the 'Workflow' tab in the iCWB Debugger. It displays a table with the following data:

Sender PID	Sender MID	Receiver PID	Receiver MID	APP Type	MML
PT_OUTSIDE	MT_UNKNOWN	PT_OM	MT_MMLSERVER	7	1
PT_OM	MT_MMLSERVER	PT_OUTSIDE	MT_UNKNOWN	7	1
PT_OUTSIDE	MT_UNKNOWN	PT_OM	MT_MMLSERVER	7	2
PT_OM	MT_MMLSERVER	PT_OUTSIDE	MT_UNKNOWN	7	2
PT_CLSTR	MT_CLSTR	PT_OM	MT_PERF	0	0
PT_CLSTR	MT_CLSTR	PT_OM	MT_PERF	0	0
PT_AP_BASE1	MT_UNKNOWN	PT_OM	MT_MMLDEBUG	8	0

At the bottom of the window, the status bar shows 'Ready' and 'Network State :Connected 10.70.33.86'.

Figure 3-35 Workflow information browse window

II. Saving workflow trace information in real time

Log in as an administrator. In the debugger window, select [Workflow/Save Workflow Message]. The reported workflow information can be saved in real time to a specified file.

Chapter 4 System Maintenance

4.1 System User

The iGWB has two user roles that have two different authority levels. See Table 4-1.

Table 4-1 User authority roles

Role	Description
Administrator	The administrator is automatically generated while installing the system. This role has the highest authorities.
Normal user	The normal user is generated by the system user or other user who has the authority to create users. The name and authorities of a normal user are allocated by his creator, or modified by the system user or a user having the modification authority after being created.

4.2 Routine Maintenance

Routine maintenance is the basis to ensure that the equipment can be operating securely, stably, and reliably for a long term. The routine maintenance of the iGWB is associated with system running, hard disk detection, and operation tasks.

I. System running

Table 4-2 Routine maintenance tasks regarding system running

Maintenance task	Operation guide	Reference standard
Checking process running status	In Windows 2000, start [Windows Task Manager]. Click the [Processes] tab. In the [Processes] tab, check whether the cls_proc.exe, ap_proc.exe, knl_proc.exe, and om_proc.exe processes are running.	For an active dual-system node, all processes must be running. 1) For an inactive node, only the cls_proc.exe process is running. 2) The number of the ap_proc.exe processes on an active node should be the same as the settings of the [Common]/APCount item in the igwb.ini file.

Maintenance task	Operation guide	Reference standard
Checking dual-system heartbeat state	Start the iGWB maintenance console. Select [Operation/State Query] to check the heartbeat state. The normal heartbeat state should be displayed as "2/2".	This operation is available only to dual-system hardware configurations, not to single-system office. In the heartbeat state display "2/2", the denominator indicates the total number of the heartbeat links and the numerator indicates the number of the currently available heartbeat links. The two numbers should be equal.
Checking bill collection of billing center	Log in to the iGWB. Start the Windows Explorer. Open the E:\Backsave\Second\AccessPointName\PathName folder to check whether bills of more than one day are accumulated.	1) For "AccessPointName", refer to the settings of the [AccessPoint%d]/APName item in the igwb.ini file. If there are several access points, check them one by one. 2) "PathName" refers to the other folders except "default" in the E:\backsave\second\AccessPointName directory, corresponding to different types of final bills. There might be one or several folders. Check them one by one.
Checking file system status	Log in to the active node of the iGWB dual-system system. Check whether the D: and E: disks on the hard disk array can be accessed and whether the access authority allows "write".	This operation is applicable to the iGWB running on 32-bit Windows operating system with dual-system hardware configurations. If the hard disk array is shared, only the active dual-system nodes can get access to the D: and E: disks. If the hard disk array is not shared, both active and inactive nodes can get access to the D: and E: disks.

II. Hard disk detection

Table 4-3 Routine maintenance tasks regarding hard disk

Maintenance task	Operation guide	Reference standard
Checking access permission to hard disk	Log in to the iGWB. Check whether the security authorities of the C:, D:, and E: disks are correct. For a dual-system system, check both devices.	Start the Windows Explorer. Right-click the C: disk icon. From the shortcut menu, select [Sharing], and the [Sharing] window is displayed. Click <Permissions>. Check whether administrators are added with the complete control authority. If not added, add an administrator and assign the complete control authority to the administrator. Perform the same operations on the D: and E: disks. Repeat Steps 1 and 2 on the standby device.

Maintenance task	Operation guide	Reference standard
Checking hard disk space	Start the iGWB maintenance console. Select [Operation/State Query]. Check the size of the available front disk space and back disk space.	<p>On the iGWB maintenance console, disk space is expressed as "n/m", in which m represents the total capacity in MBs, and the numerator n indicates the usable space in MBs.</p> <p>When the available disk space is less than 800MB (the minimum alarming space) by default, the system generates an alarm prompting that the medium space is insufficient.</p> <p>When the available disk space is less than 400MB (the minimum switchover space) by default, the system generates an alarm prompting that the media space is insufficient. For the dual systems with the non-sharing hard disk array, the systems will be switched over. If it is a single system, the system cannot receive charging tickets (bills).</p>
Checking hard disk fault	Check whether the hard disk array of the iGWB server is operating well.	Observe the hard disk status indicator on the hard disk array. If the indicator is red, it indicates that the hard disk is faulty and must be replaced.

III. Operation tasks

Table 4-4 Routine maintenance tasks regarding system operation

Maintenance task	Operation guide	Reference standard
Viewing bill	Start the iGWB maintenance console. View the bill files to check whether there are incorrect bills.	If a bill cannot be resolved, the iGWB maintenance console will prompt the error.
Checking trace information	Log in to the iGWB. Check whether the latest contents of the files in the "Trace" folder all indicate normal.	<ol style="list-style-type: none"> 1) This operation must be performed on both nodes of the dual iGWB systems. 2) Each file in the "Trace" folder corresponds to a process. 3) Not all the contents in the trace files indicate abnormal. Analysis is required. Refer to section 4.4.3 .

Maintenance task	Operation guide	Reference standard
Checking debugging information and checking exception alarm	Start the iGWB debugging console. Check whether the debugging information outputs indicate normal and whether there are exception alarms.	<p>1) Open the debugging information output window of the debugging console. Observe whether there are abnormal outputs.</p> <p>2) Open the protocol information output window of the debugging console. Observe whether there are bill reception and exception alarms.</p> <p>3) Open the workflow information output window of the debugging console. Observe whether there are abnormal outputs.</p> <p>Note: The outputs in the debugging information window will be refreshed frequently when the traffic is increasing, which might influence your observation. Consequently, use the preceding observation methods when appropriate, for example, when the traffic is light.</p>
Switchover test	In dual-system environments, test whether the active and standby devices can be switched normally.	<p>Manually switch over the iGWB servers.</p> <p>Detect whether the standby device can be activated within five minutes.</p> <p>Manually switch over the iGWB servers again. Detect whether the active device will be activated and whether the standby device will be deactivated.</p> <p>Note: Switchover test might influence the normal operation of the system. Do not use it frequently.</p>

4.3 Software Upgrade

4.3.1 Overview of Software Upgrade

There are two types of software upgrade of the iGWB, namely ordinary upgrade and special upgrade.

An ordinary upgrade does not change the existing directory structure or program structure of the original version. The ordinary upgrade does not influence any data regarding the original version, either. After the ordinary upgrade, the system continues to operate from the status of the original version, and the sequence number of bill file is incremented continuously.

A special upgrade causes the change of the interface between the iGWB and the SoftX3000 or between the iGWB and the billing center. The change of the interface

between the iGWB and the SoftX3000 refers to the change of the format for the charging tickets. Consequently, the length of a charging ticket is changed. The change of the interface between the iGWB and the billing center refers to the change of the format for the bill files. In a special upgrade, the igwb.ini file must be set again. If the system status file is not deleted, however, the sequence number of bill file will be incremented continuously.



Caution:

- Before a special upgrade, ensure that the billing center can normally fetch bills from the iGWB and all the bills have been fetched by the billing center. Otherwise, bills might be lost.
 - The status file of the system is stored on E:\Statusfile by default. The backup of the status file is stored on E:\Statusfileb. In a special upgrade, read the installation guide to determine whether to delete the status file.
-

4.3.2 Ordinary Upgrade

In an ordinary upgrade, upgrade the standby iGWB server and then the active iGWB server. Services are not interrupted during the upgrade process.

- 1) Use the integrated switcher to switch the input and output to the standby iGWB server.
- 2) Select [Start/Programs/Administrative Tools/Services]. The [Services] window is displayed, as shown in Figure 4-1.

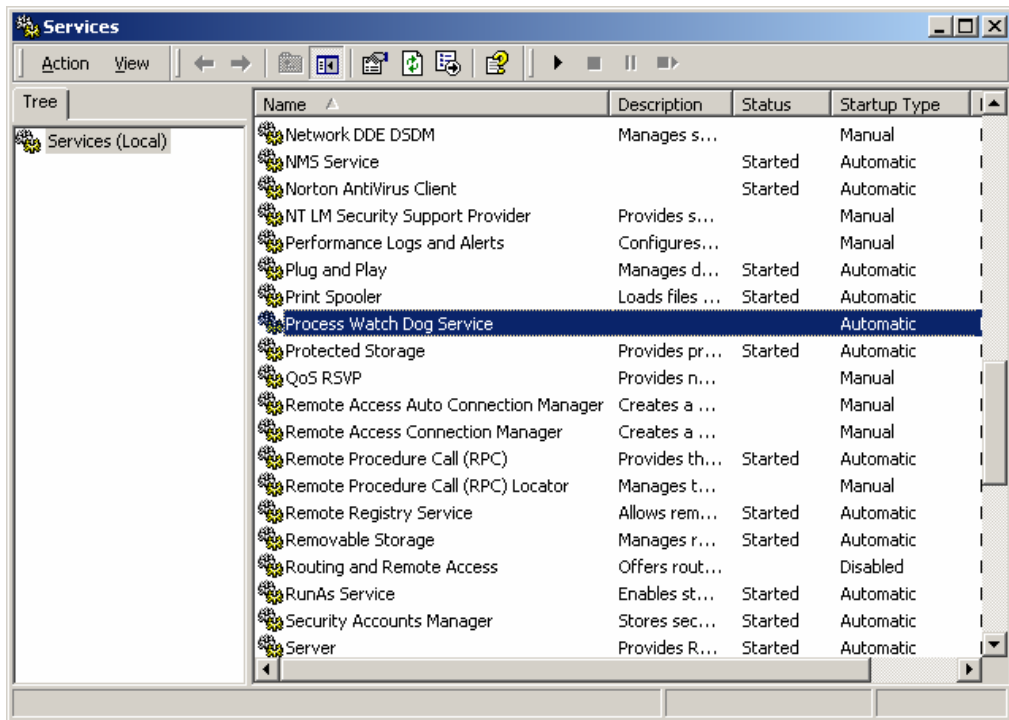


Figure 4-1 [Services] window

- 3) Right-click the [Process Watch Dog Service] icon. From the shortcut menu, select [Properties]. The [Process Watch Dog Service Properties] window is displayed. Click the [Stop] button to stop the service.
- 4) Select [Start/Programs/iGateway Bill V200 Server/Stop iGWB]. It is found that there is no bulb in the status bar.
- 5) Back up the original installation files. It is recommended to rename the original installation directory root for backup purposes. For example, the original installation directory root is C:\igwb. Rename it to C:\igwbbak.
- 6) Refer to Chapter 2 “System Installation” of this manual to install the new version of the iGWB server. After the installation, replace the igwb.ini file on the installation directory with the igwb.ini file (in Config\Ini) on the backup directory.
- 7) Open the [Process Watch Dog Service Properties] window. (Refer to Steps 2 and 3.) Click the [Start] button to start the Process Watch Dog service. The software upgrade of the standby iGWB server is completed.
- 8) Switch the input and output to the active iGWB server. Repeat Steps 2 to 7 to upgrade the software of the active iGWB server.
- 9) The upgrade is completed. Restart the servers.

4.3.3 Special Upgrade

To conduct a special upgrade, proceed as follows:

- 1) On the bill console, select [Operation/Upgrade]. Confirm the operation to execute the auxiliary upgrade command.

 **Caution:**

The upgrade operation can be continued only after the client prompts "Auxiliary Upgrade Complete". Otherwise, bills might be lost.

- 2) Wait for the billing center to fetch all bills from the active and standby iGWB servers.
- 3) Use the integrated switcher to switch the input and output to the standby iGWB server.
- 4) Stop the Process Watch Dog service and the iGWB system. (Refer to Steps 2 to 4 in section 4.3.2 Ordinary Upgrade.)
- 5) Back up the original installation files. (Refer to Step 5 in section 4.3.2 Ordinary Upgrade.)
- 6) Refer to Chapter 2 "System Installation" of this manual to install the new version of the iGWB server. After the installation of the new version, re-configure the igwb.ini file on the installation directory (c:\igwb\config\ini by default) according to the version installation guide. Either, you can modify the igwb.ini file on the backup directory according to the updates of the version and then replace the igwb.ini file on the installation directory with it.
- 7) Start the Process Watch Dog service. (Refer to Step 7 in section 4.3.2 Ordinary Upgrade.) The software upgrade of the standby iGWB server is completed.
- 8) Start the standby iGWB server, and then select [Operation/Switch] on the CDR console to switch to the standby iGWB server manually.
- 9) Switch the input and output to the active iGWB server. Repeat Steps 2 to 8 to upgrade the software of the active iGWB server.
- 10) The upgrade is completed. Restart the servers.

4.4 Troubleshooting

4.4.1 Introduction to Fault Positioning Information

Fault positioning information about the iGWB falls into the following types:

- Device maintenance and fault positioning interfaces provided in the design of the iGWB software, such as trace information, parameter configurations, and log.
- Fault positioning measures provided by the operating system, such as ifconfig/ipconfig, netstat, and ping.

I. Fault positioning information provided by the iGWB software

1) Trace information

Trace information plays an important role in positioning a fault. Each piece of trace information is expressed in the following format:

Trace generation time Module number writing the trace Trace contents

Trace records are significant debugging information for the running of the system. Trace is not equal to abnormality. Usually a large number of trace records are generated when the system is started or shut down. A few trace records are generated during the system is operating normally.

The iGWB application has four types of processes, namely dual-system process (cls_proc.exe), kernel process (knl_proc.exe), access point process (ap_proc.exe), and operation and maintenance process (om_proc.exe). In the actual running, the dual-system process, kernel process, and operation and maintenance process have only one respective process instance, but the access point process can start one or more process instances depending on the parameter configurations. Each process instance of the iGWB creates a trace file. The following is the format for naming trace files of the dual-system process, kernel process, and operation and maintenance process:

ProcessName_trace.txt

For example, the trace file of the operation and maintenance process is named om_proc_trace.txt.

Because the access point process might have several process instances, the access point ID is added in the trace file name for identification purposes. The specific format is as follows:

ap_procAccessPointID_trace.txt

For example, the trace file of the first access point is named ap_proc1_trace.txt.

In addition, the size of each trace file is limited to 6 MB. If the trace file exceeds this limit, the application changes its extension from "txt" to "tmp", and then creates a new trace file.

All trace files of the iGWB are stored in the trace folder on the installation directory (C:\igwb by default).

2) Configuration information

Because a large number of faults are caused by parameter configuration errors, it is recommended to analyze both parameter configuration files and trace information. Configuration information of the iGWB includes parameter configuration information and bill format configuration information. The parameter configuration information is

stored in the \config\ini\igwb.ini file on the installation directory. Currently, that is the only parameter configuration file. The bill format configuration information is stored in the \config\format on the installation directory.

3) Bill files

To remove a bill exception of the iGWB, analyze the original bill file and the final bill file.

The original bill files and the final bill files of the iGWB are respectively stored in D:\Frontsave and E:\Backsave.

4) Log

Log records the operations performed on the device through the maintenance console. Log is helpful in positioning faults.

Log files are stored in D:\Other\Log. The system creates a log file every day. The generation date is used as the file name. The characters "log" are used as the extension of the file. Log file of the iGWB is stored for one month by default. After expiration, the log file will be deleted automatically.

5) State query

The iGWB provides the state query function to facilitate routine maintenance, but the function is not very helpful in positioning faults.

On the maintenance terminal, you can query the current running state of the iGWB. Table 4-5 lists the state available.

Table 4-5 Common running state of the iGWB

State	Description
Active and standby nodes	0 represents the active node, and 1 represents the standby node.
Heartbeat state	Heartbeat state is expressed as "n/m", in which the denominator m indicates the total number of the heartbeat links and the numerator n indicates the number of the currently available heartbeat links. Usually two heartbeat links are configured, that is, m is equal to 2. If n is equal to 0, it indicates that the heartbeat is abnormal; otherwise, the heartbeat is normal. Note: If n is not equal to 0 and m is not equal to n, it indicates that part of the heartbeat links is faulty. To ensure the reliable running of the system, check the heartbeat links and recover the faulty link.
CPU usage	The iGWB supports displaying a maximum of two CPU usages. If only one CPU is configured, "-" is displayed in the place of the second CPU usage.
Disk usage	The iGWB supports querying the total space and usable space of the front disk and the back disk, which is expressed as "n/m". In "n/m", the denominator m indicates the total space of the disk in MBs and the numerator n indicates the usable space of the disk in MBs.

State	Description
Memory usage	The iGWB supports querying the usage of the physical memory, which is expressed as "n/m". In "n/m", the denominator m indicates the total size of the physical memory in MBs and the numerator n indicates the usable size of the physical memory in MBs.

To start the state query function, select [Operation/State Query] on the iGWB client. In the [State Query] window, click the Set Property icon. The [Setting Properties] dialog box is displayed. Set the [Save Status] to "Open", and the status information will be saved in the StatsInfo.txt file on the installation directory of the maintenance terminal.

II. Information provided by the operating system

The operating system provides the following information:

1) IP address configuration

To obtain the IP address configuration, run `#ipconfig -all`.

2) Network connection state

To obtain the current network connection state, run `#netstat -na`.

To dump the outputs for future reference, run `#netstat -na > 20031105.txt`. It is recommended to name the dumping file the operation date. For example, "20031115" indicates that operation was performed on Nov 15th 2003.

3) System log

To obtain the system log, start the Event Viewer and dump the Application Log and the System Log, as shown in Figure 4-2.

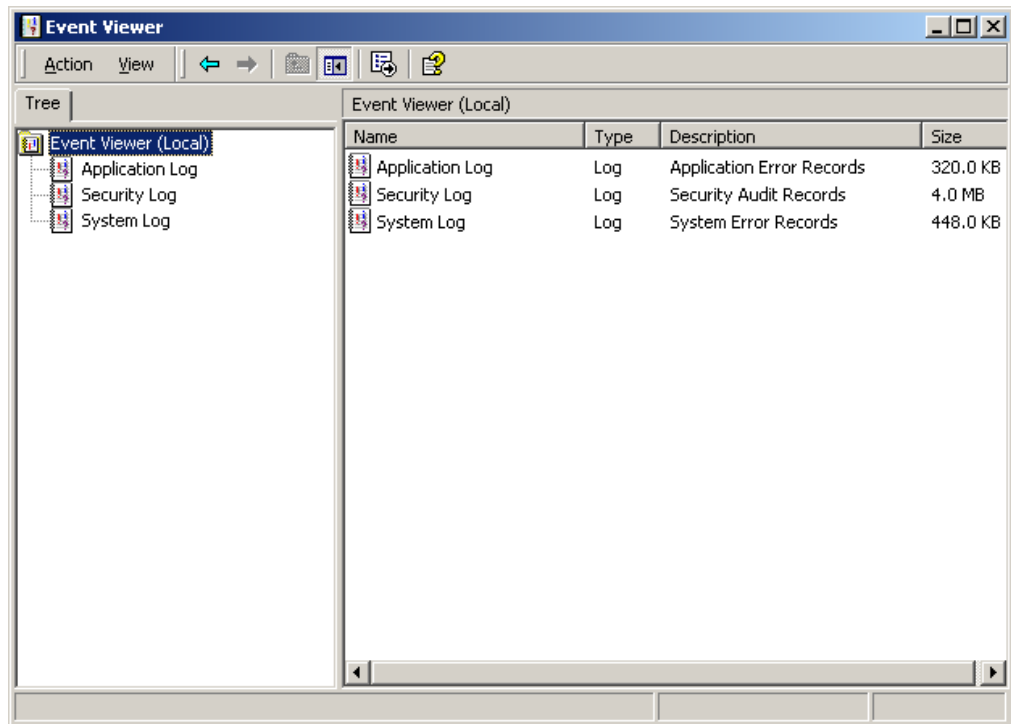


Figure 4-2 Dumping system log through Event Viewer

4) Process running status

To check whether the processes of the iGWB are running, start the Windows Task Manager and click the [Processes] tab, as shown in Figure 4-3.

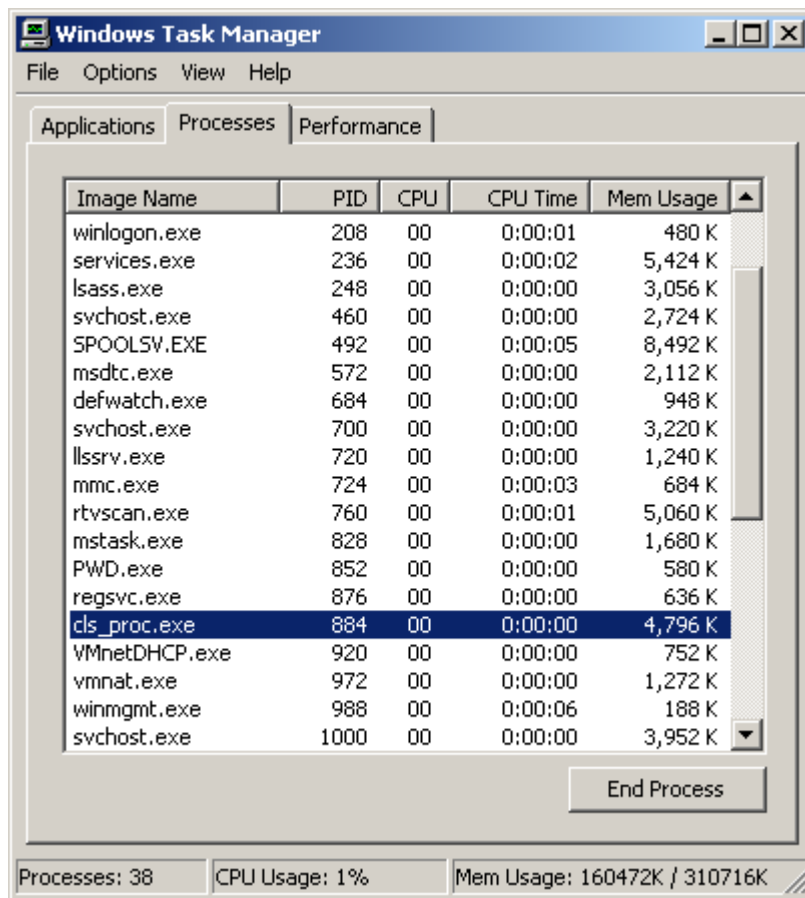


Figure 4-3 Checking process status with Windows Task Manager

Note:

- On a Windows-based platform, only the cls_proc.exe process is running at the inactive node, and the cls_proc.exe, knl_proc.exe, om_proc.exe, and ap_proc.exe processes are all running at the active node.
 - In addition to the query of the process existence, query several times and observe whether the process ID (PID) is changed. That is because the monitor process might frequently start the abnormal process in the event of abnormality, which causes the PID to increase even though the process exists.
-

4.4.2 Collection of Fault Positioning Information

Collection of fault positioning information depends on the running of the system and the type of the fault. The following section presents the required information according to the type of the fault.

I. Interface communication fault

This type of fault refers to the faults occurring to the interface between the SoftX3000 and the iGWB or the interface between the iGWB and the billing system. To remove such a fault, the following information should be provided:

- 1) Parameter configuration file—igwb.ini
- 2) All trace files
- 3) IP address configuration (ipconfig/ifconfig) and network connection state (netstat) of the operating system

II. Bill exception

This type of fault refers to the exceptional billing information found when you are viewing the bills or the billing complaints from subscribers. To remove such a fault, the following information should be provided:

- 1) Parameter configuration file—igwb.ini
- 2) Bill format configuration files (all files in \config\format of the installation directory)
- 3) Original and final bill files containing the exceptional billing information

III. Start failure

This type of fault refers to the various exceptions occurring to the start process of the iGWB application. To remove such a fault, the following information should be provided:

- 1) Parameter configuration file—igwb.ini
- 2) Bill format configuration files (all files in \config\format of the installation directory)
- 3) All trace files
- 4) IP address configuration (ifconfig/ipconfig) of the operating system

IV. Hardware fault

Provisioning of the hardware fault positioning system depends on the log function of the operating system. It is required to dump the Application Log and the System Log in the Event Viewer and observe whether the hard disk status indicator on the hard disk array is normal. If the hard disk status indicator is red, it indicates that the hard disk is damaged.

4.4.3 Common Trace Information and Related Maintenance

During the iGWB is running, some significant running information and fault information is recorded in the trace files in C:\igwb\Trace.

The common trace information and the related maintenance measures are presented as follows:

I. Usable front disk space insufficient for the minimum alarming space

Open the C:\igwb\Config\igwb.ini file. Check the FrontSaveRootDir and MinDiskAlarmRoom configuration parameters under the DiskFile configuration item. Confirm the disk storing the original bills (front disk bills) and the size of the minimum alarming space. Check the available space of the corresponding disk. If the available disk space is insufficient, consider to reduce the value of the DiskFile/DeadLineOfAutoDel configuration item or delete unnecessary bill files.

If they are not configured, the default values for the parameters are D:\Frontsave and 800MB respectively.

II. Usable back disk space insufficient for the minimum alarming space

Open the C:\igwb\Config\igwb.ini file. Check the BackSaveRootDir and MinDiskAlarmRoom configuration parameters under the DiskFile configuration item. Confirm the disk storing the final bills (back disk bills) and the size of the minimum alarming space. Check the available space of the corresponding disk. If the available disk space is insufficient, consider to reduce the value of the DiskFile/DeadLineOfAutoDel configuration item or delete unnecessary bill files.

If they are not configured, the default values for the parameters are E:\Backsave and 800MB respectively.

III. Usable backup medium space insufficient for the minimum alarming space

Open the C:\igwb\Config\igwb.ini file. Check the MinBakDeviceRoom parameter under the NetBackup and BackupTask? configuration items, in which the question mark "?" represents the specific backup task number. Check the available space of the corresponding disk. If the available disk space is insufficient, consider to replace the backup medium.

The default value for the MinBakDeviceRoom parameter is 50 MB.

IV. Usable front disk space insufficient for the minimum switchover space

Open the C:\igwb\Config\igwb.ini file. Check the FrontSaveRootDir and MinDiskHandoverRoom configuration parameters under the DiskFile configuration item. Confirm the disk storing the original bills (front disk bills) and the size of the minimum switchover space. Check the available space of the corresponding disk. If the available disk space is insufficient, consider to reduce the value of the DiskFile/DeadLineOfAutoDel configuration item or delete unnecessary bill files.

If they are not configured, the default values for the parameters are D:\Frontsave and 400MB of total space respectively.

V. Usable back disk space insufficient for the minimum switchover space

Open the C:\igwb\Config\igwb.ini file. Check the BackSaveRootDir and MinDiskHandoverRoom configuration parameters under the DiskFile configuration item. Confirm the disk storing the final bills (back disk bills) and the size of the minimum switchover space. Check the available space of the corresponding disk. If the available disk space is insufficient, consider to reduce the value of the DiskFile/DeadLineOfAutoDel configuration item or delete unnecessary bill files.

If they are not configured, the default values for the parameters are E:\Backsave and 400MB respectively.

VI. Access point type, access point type being %d

Open the C:\igwb\Config\igwb.ini file. Check whether the APType parameter under the AccessPointN configuration item is correct. If not correct, correct the setting of the parameter.

AccessPointN is the parameter related to a specific access point, in which N is the ID of the access point in the range of 1 to m and m is the value of the APCount parameter under the Common item.

APType refers to the type of the access point which must be entered correctly. The value 0 represents the C&C08 switch provided by Huawei. The value 1 represents a Global System for Mobile Communications (GSM) or Code Division Multiple Access (CDMA) product. The value 2 represents a signaling transfer point (STP). The value 3 represents a General Packet Radio Service (GPRS) product. The value 4 represents a Wideband Code Division Multiple Access (WCDMA) product. The value 5 represents a softswitch product.

VII. Failure of reading IP address from MML server (default value %s)

Open the C:\igwb\Config\igwb.ini file. Check whether the LocalIpToMMLClient parameter under the MML configuration item is correct. If not correct, correct the setting of the parameter.

LocalIpToMMLClient refers to the local IP address of the MML server for the connection to the MML client (the iGWB client), that is, the IP address for the iGWB to connect the network management system.

VIII. Error code %d returned in socket registration when connecting kernel process

Probably the kernel process is not running. To check whether the kernel is running, press <Ctrl + Alt + Del> to display the [Windows Task Manager] window, and click the

[Processes] tab to see whether the kernel process exists. If the process does not exist, it is recommended to restart the iGWB server.

IX. Kernel process not running

For the cause and solution, refer to the problem 8.

X. Failure of opening listening port (IP = %s, Port = %d) with error code %d

Open the C:\igwb\Config\igwb.ini file. Check whether the IP address and the port number of the MML server under the MML configuration item are correct. If not, correct the settings.

LocalIpToMMLClient refers to the local IP address of the MML server for the connection to the MML client (the iGWB client), that is, the IP address for the iGWB to connect the network management system.

LocalPortToCM refers to the MML maintenance port of the MML server. It takes the value of 6000.

LocalPortToAR refers to the MML alarm report port of the MML server. It takes the value of 6001.

LocalPortToRD refers to the MML debugging port of the MML server. It takes the value of 6007.

XI. Activation failure of asynchronous resource (resource name %s and resource type %d)

The asynchronous resource refers to the knl_proc.exe process. In this case, open the trace\knl_proc_trace.txt file to position the failure. In addition, an activation failure of the knl_proc.exe process might be caused by its sub-processes (ap_proc.exe and om_proc.exe), so open the ap_proc_trace.txt and om_proc_trace.txt files for further positioning purposes. For the specific positioning methods, refer to the problems 1 to 10.

XII. Dual-system activation failure

Dual-system activation failure is caused by an activation failure of the asynchronous resource. For the specific methods for positioning an activation failure of the asynchronous resource, refer to the problem 11.

XIII. Unidentified heartbeat type (%s)

Open the C:\igwb\Config\igwb.ini file. Check whether the Type parameter under the LinkN configuration item is correct. If not, correct the setting of the parameter.

The Type parameter refers to the type of the heartbeat link. It can be set only to “UDP” or “COM”. UDP represents a private network link. COM represents a serial port link. Any other settings are incorrect.

XIV. Failure of creating heartbeat link %d (heartbeat name %s and heartbeat type %d)

Check whether the heartbeat link configurations are correct based on heartbeat name or heartbeat type. If the heartbeat type is UDP, the LocalIp and PeerIp parameters must be correctly configured. If the heartbeat type is COM, the Port parameter must be correctly configured.

Such an error is probably caused by the configuration of an inexistent local IP address or port number.

XV. Interruption of heartbeat link %d (heartbeat name %s and heartbeat type %d)

According to heartbeat name or heartbeat type, check whether the cable connection of the network port or serial port used to transmit heartbeat between the dual systems is normal, whether the IP address setting is correct, and whether the peer end is running.

Such an error occurs probably because the peer is not running.

XVI. Starting to perform failover operation (switchover cause %d)

This piece of information indicates that because the local end of the iGWB becomes faulty, it must be switched to the peer. Table 4-6 lists the switchover cause codes.

Table 4-6 Switchover cause table

Switchover cause code	Explanation
0	Failed to write file, which is probably caused by insufficient disk space.
1	Insufficient front disk space, which means that the size of the available space of the disk storing the original bills is less than the minimum switchover space (400MB by default).
2	Insufficient back disk space, which means that the size of the available space of the disk storing the final bills is less than the minimum switchover space (400MB by default).
3	Asynchronous resource failure, which refers to the failure of the knl_proc process. For specific troubleshooting methods, refer to the problem 11 earlier in the trace description.
4	Activation failure of the cls_proc.exe process, which is probably caused by an asynchronous resource activation failure or resource creation failure. Such a failure is positioned according to the specific trace information.

Switchover cause code	Explanation
5	Resource failure. Resource failure includes virtual IP resource failure, volume resource failure, and service failure. Refer to the trace information for the further troubleshooting.
6	Damaged hard disk of the array. Replace the damaged disk.

XVII. Failure of failover operation

Such a fault is probably caused by the faultiness of the local iGWB, in which the local iGWB detects the interruption of all heartbeats. In addition, such a fault occurs because of an activation failure when the peer attempts to activate itself upon receipt of the failover command.

Such a fault is generated by the local iGWB. In this case, confirm that the peer is running, and remove the faults at the peer.

XVIII. Operation failure at failover response end

Such a fault is caused when the local iGWB attempts to activate itself upon receipt of the failover command but fails.

Check other specific trace information to position the activation failure.

XIX. Starting to perform handover operation

Generation of this piece of information is caused by the following:

- 1) The active server is being started.
- 2) The peer iGWB is faulty, and the local end is deactivated.
- 3) The local iGWB receives a manual switchover command from the client.

XX. Multiple failed activation attempts at local node and never activatable unless heartbeat is interrupted

The local end continuously performs activation attempts (three times by default), but all fail. In this case, the local end stops the activation operation, and enters the FAILDOWN state. After one hour, the local end restores to the normal state, and starts the activation operation again. The local end repeats the same until the heartbeat links are restored to be normal.

4.4.4 Frequently Asked Questions

I. Failure of logging in to bill console

- 1) Out-of-service iGWB

When logging in to the bill console, you enter the correct username and password, but the system prompts “Connect Server Failed, Relogin?” It indicates that the iGWB is not running or is running abnormally. In this case, start the iGWB and log in again.

2) Network failure

If a network failure occurs when you are operating the bill console, for example, viewing the bills or logs, the system prompts the corresponding message as shown in Figure 4-4. In this case, check whether the network is normal, or exit the client and re-connect again.



Figure 4-4 Prompt message of bill console in case of a network failure

3) iGWB switchover

If an iGWB switchover happens when you are operating the bill console, the connection between the client and the server is interrupted. After the switchover, log in again.

II. Dual-system switchover

If the iGWB is backing up the bill files when a dual-system switchover happens, the bills stop being backed up. The on-going backup will not continue after the other iGWB starts.

Because the bill files are stored in the respective hard disk arrays of the active and standby iGWBs, the bill data will be distributed after the switchover. To avoid that, insert a new backup medium into the switched iGWB server and back up the bill files that are generated after the switchover. The bills generated before the switchover continues to be backed up after the switched iGWB server restarts. It is recommended to number the backup media in the order of the generation of the bills for identification purposes.

If the stopped backup in the dual-system switchover is an automatic backup, the automatic backup can also be performed correctly in future. If it is a manual backup, the appropriate processing measures must be taken to continue the backup.

III. Incorrect username or password

When you are attempting to log in to the bill console, the system prompts “Log Failed: Password Error”. In this case, the entered password is not correct. Enter the correct password.

When you are attempting to log in to the bill console, the system prompts “Log Failed: Account does not exist”. In this case, the entered username is not correct. Enter the correct username.

IV. iGWB shutdown

Select [Start/Programs/iGateway Bill V200 Server/Stop iGateway Bill] on the active server, and the bulb of the standby server is not on. Restart the active server, but the bulb of the standby server is still off in five minutes.

This is caused by incorrect operation steps. Before stopping the iGWB, stop the “Process Watch Dog Service” first. For details, see 4.3.2 2)

Appendix A iGWB Configuration Instance

You can configure the iGWB running mode to single host or dual system according to actual requirements. This chapter details the instances for these two configuration modes.



Caution:

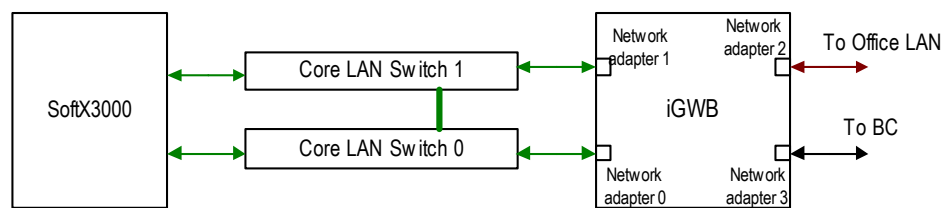
- We should not manually set the virtual IP addresses of iGWB network adapters directly, which will cause iGWB software start unsuccessfully;
- Configure the virtual IP address of the iGWB network adapter indirectly by configuring the igwb.ini file. For details about igwb.ini configuration, see 2.5.2 Modifying Server Software Settings.
- The iGWB reads the igwb.ini file to obtain the information about the virtual IP address to be set, and automatically adds the virtual IP address to the iGWB network adapter accordingly.

A.1 Configuration for Single-host Mode

This section shows the instance of setting the single-host mode from the aspects of networking, IP address setting rules and configuration file contents.

A.1.1 Networking Diagram

Figure A-1 shows the networking of the iGWB working in the single-host mode.



BC: Billing Center

iGWB: iGateway Bill

Figure A-1 Networking for single-host mode

Figure A-2 shows the location of four network adapters in Figure A-1.

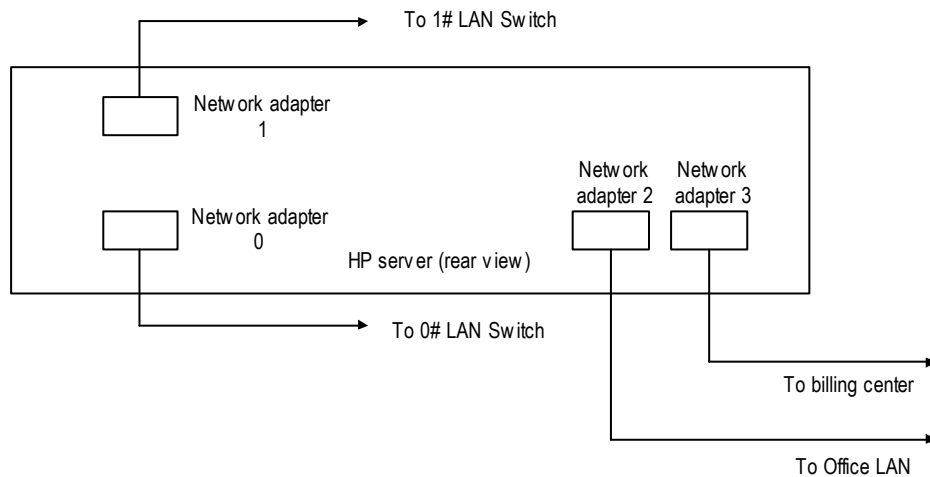


Figure A-2 Location of the network adapters

The IDs of the network adapters of the iGWB in Figure A-2 are as follows:

- Network adapter 0: Netcard0 to 0# LAN Switch
- Network adapter 1: Netcard1 to 1# LAN Switch
- Network adapter 2: Netcard2 to Office LAN
- Network adapter 3: Netcard3 to Billing System

A.1.2 IP Address Configuration of Network Adapters

When the iGWB operates in the single-host mode, you do not need to configure the virtual IP for the network adapters.

Table A-1 describes the IP address configuration of network adapters in Figure A-2.

Table A-1 IP address configuration

Network adapter ID	Peer device	iGWB IP	Remarks
Netcard0 to 0# LAN Switch	To 0# LAN Switch. Communicate with SoftX3000 active plane.	172.20.200.1	Used to communicate with SoftX3000 active plane.
Netcard1 to 1# LAN Switch	To 1# LAN Switch. Communicate with SoftX3000 standby plane.	172.30.200.1	Used to communicate with SoftX3000 standby plane.
Netcard2 to Office LAN	To CDR console and NMS interface. Also work as the first heartbeat path for iGWB dual system.	129.9.1.1	Used to connect Office LAN, communicate with WS. Determine the IP address according to actual conditions.
Netcard3 to Billing Center	To the billing center. Provide the billing interface.	/	Determine the IP address according to actual conditions.

A.1.3 Configuration of iGWB

You need to configure an "igwb.ini" file only when the iGWB operates in the single-host mode,

The content of the "igwb.ini" file is as following:

```
;Configuration for single running server
```

```
;As a configuration template of iGWB, this INI file supposes iGWB's IP addresses are as follows:
```

```
;NIC      iGWB
;0        172.20.200.1
;1        172.30.200.1
;2        129.9.1.1
;3        /
```

```
[Common]
```

```
APCount = 1           ;Accesspoint count
ServerNo = 0          ;Server No., 0-Primary, 1-Secondary
NoClusterMode =1     ;Flag of cluster or not, 1-cluster mode, 0-single-host mode
```

```
;Configuration of accesspoint 1, which means fix network in general.
```

```
[AccessPoint1]
```

```
APType = 5           ;Accesspoint type, 0-128, 1-MSC, 2-STP, 3-GPRS, 4-WCDMA, 5-SOFTX
APName = X3KF        ;Accesspoint name, need no modification
LocallpToEx =172.20.200.1 ;iGWB's IP to connect SoftX 3000(VirtualIP of Resource2)
LocallpToExBak =172.30.200.1 ;iGWB's secondary IP to connect SoftX 3000 (VirtualIP of Resource3)
BillRecSize =156
BinAlarmSend = 1     ;Flag of sending binary alarm, 0-no, 1-yes
BaseID = 3200        ;Binary alarm base ID
SaveSecond = 1       ;Flag of offering the second copy of final bill files, 0-no, 1-yes
MpuWindowSize=300
```

```
[MML]
```

```
LocallpToMMLClient =129.9.1.1 ;iGWB's IP to connect client(VirtualIP of Resource1)
```

A.2 Configuration for Cluster Mode

This section shows the instance of setting the dual system backup mode from the aspects of networking, IP address setting rules and configuration file contents.

A.2.1 Networking Diagram

Figure A-3 shows the networking of the iGWB working in cluster mode.

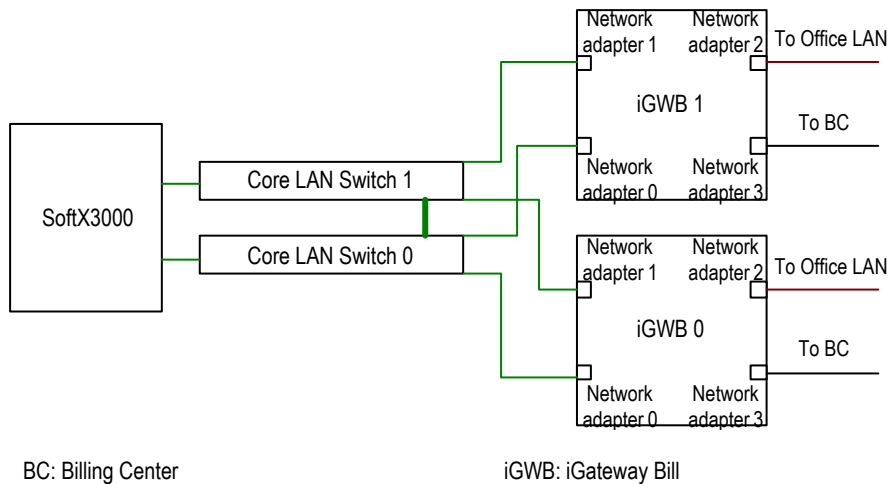


Figure A-3 Networking for cluster mode

Figure A-2 shows the location of four network adapters in Figure A-3.

The IDs of the network adapters of the iGWB in Figure A-2 are as follows:

- Network adapter 0: Netcard0 to 0# LAN Switch
- Network adapter 1: Netcard1 to 1# LAN Switch
- Network adapter 2: Netcard2 to Office LAN
- Network adapter 3: Netcard3 to Billing System

A.2.2 IP Address Configuration of Network Adapters

When the iGWB operates in the cluster mode, you need to configure the virtual IP for the network adapters.

Table A-2 describes the IP address configuration of network adapters in Figure A-3.

Table A-2 IP address configuration

Network adapter ID	Peer device	iGWB 0 IP	iGWB 1 IP	Virtual IP
Netcard0 to 0# LAN Switch	To 0# LAN Switch. Communicate with the active plane of the host.	130.1.2.1	130.1.2.2	172.20.200.1

Network adapter ID	Peer device	iGWB 0 IP	iGWB 1 IP	Virtual IP
Netcard1 to 1# LAN Switch	To 2#LAN Switch. Communicate with the standby plane of the host.	130.1.3.1	130.1.3.2	172.30.200.1
Netcard2 to Office LAN	To CDR console and NMS interface. Also work as the first heartbeat path for iGWB dual system.	130.1.1.1	130.1.1.2	129.9.1.1
Netcard3 to Billing Center	To the billing center. Provide the billing interface.	130.1.4.1	130.14.2-	/

Note:

You should define the virtual IP address and subnet mask of network adapter Netcard2 to Office LAN according to actual conditions.

A.2.3 Configuration of iGWB

When the iGWB operates in the cluster mode, you need configure an "igwb.ini" file for each iGWB server.

The configuration content for the two iGWB servers is different.

I. Configuration of the Primary iGWB

The primary iGWB is the primary server of the mutual backup iGWB servers. It is called "iGWB 0". The content of its "igwb.ini" file is as following:

;As a configuration template of iGWB, this INI file supposes iGWB's IP addresses are as follows:

```
;NIC  iGWB0 OrigIP  iGWB1 OrigIP  Virtual IP
; 1    130.1.1.1     130.1.1.2     129.9.1.1
; 2    130.1.2.1     130.1.2.2     172.20.200.1
; 3    130.1.3.1     130.1.3.2     172.30.200.1
```

;Configuration of primary iGWB(iGWB 0)

[Common]

APCount = 1 ;Accesspoint count

ServerNo = 0 ;Server No., 0-Primary, 1-Secondary

NoClusterMode = 1 ;Flag of cluster or not, 1-cluster mode, 0-single-host mode

;Configuration of accesspoint 1, which means fix network in general.

[AccessPoint1]

APType = 5 ;Accesspoint type, 0-128, 1-MSC, 2-STP, 3-GPRS, 4-WCDMA, 5-SOFTX

APName = X3KF ;Accesspoint name, need no modification

LocallpToEx = 172.20.200.1 ;iGWB's IP to connect fix network exchange(VirtuallIP of Resource2)

LocallpToExBak = 172.30.200.1 ;iGWB's secondary IP to connect fix network exchange(VirtuallIP of Resource3)

BillRecSize = 156 ;Original bill record size(Bytes)

BinAlarmSend = 1 ;Flag of sending binary alarm, 0-no, 1-yes

BaselD = 3200 ;Binary alarm base ID

SaveSecond = 1 ;Flag of offering the second copy of final bill files, 0-no, 1-yes

MpuWindowSize=300

[MML]

LocallpToMMLClient = 129.9.1.1 ;iGWB's IP to connect client(VirtuallIP of Resource1)

[Cluster]

InstallShareDiskArray = 0 ;Flag of using sharing disk array, 0-no, 1-yes

HeartBeatBroken = 300 ;Heartbeat link broken interval(seconds)

HeartBeatCount = 2 ;Heartbeat link count

ResourceCount = 3 ;Resource count

;Configuration of heartbeat link1

[Link1]

Type = UDP ;Heartbeat link type, UDP-private network, COM-serial communication port

Name = UDP_LINK ;Heartbeat link name

LocallP = 130.1.1.1 ;Local heartbeat IP(IP of local NIC1)

PeerIP = 130.1.1.2 ;Peer heartbeat IP(IP of peer NIC1)

;Configuration of heartbeat link2

[Link2]

Type = COM ;Heartbeat link type, UDP-private network, COM-serial communication port

```
Name = COM_LINK           ;Heartbeat link name
Port = 1                   ;Port No., 1-COM1, 2-COM2

;Configuration of resource1
[Resource1]
ResType = IP               ;resource type, IP-virtual IP
ResName = IP_OMC           ;resource name, to connect OMC or Client
OriginalIP = 130.1.1.1     ;original IP, IP of NIC1
VirtualIP = 129.9.1.1      ;virtual IP
VirtualMask = 255.255.0.0  ;subnet mask of virtual IP

;Configuration of resource2
[Resource2]
ResType = IP               ;resource type, IP-virtual IP
ResName = IP_PLANE1        ;resource name
OriginalIP = 130.1.2.1     ;original IP, IP of NIC2
VirtualIP = 172.20.200.1   ;virtual IP
VirtualMask = 255.255.0.0  ;subnet mask of virtual IP
SwitchGroup = 1            ;Only all the resources in the same SwitchGroup No. fail, the switch will be
happened

;Configuration of resource3
[Resource3]
ResType = IP               ;resource type, IP-virtual IP
ResName = IP_PLANE2        ;resource name
OriginalIP = 130.1.3.1     ;original IP, IP of NIC3
VirtualIP = 172.30.200.1   ;virtual IP
VirtualMask = 255.255.0.0  ;subnet mask of virtual IP
SwitchGroup = 1            ;Only all the resources in the same SwitchGroup No. fail, the switch will be
happened
```

II. Configuration of the Secondary iGWB

The secondary iGWB is the secondary server of the mutual backup iGWB servers. It is called "iGWB 1". The content of its "igwb.ini" file is as following:

;Configuration of Secondary iGWB(iGWB 1)

;As a configuration template of iGWB, this INI file supposes iGWB's IP addresses are as follows:

;NIC	iGWB0 OrigIP	iGWB1 OrigIP	Virtual IP
; 1	130.1.1.1	130.1.1.2	129.9.1.1
; 2	130.1.2.1	130.1.2.2	172.20.200.1
; 3	130.1.3.1	130.1.3.2	172.30.200.1

[Common]

APCount = 1 ;Accesspoint count
 ServerNo = 1 ;Server No., 0-Primary, 1-Secondary
 NoClusterMode =1 ;Flag of cluster or not, 1-cluster mode, 0-single-host mode

;Configuration of accesspoint 1, which means fix network in general.

[AccessPoint1]

APType = 5 ;Accesspoint type, 0-128, 1-MSC, 2-STP, 3-GPRS, 4-WCDMA, 5-SOFTX
 APName = X3KF ;Accesspoint name, need no modification
 LocalIpToEx = **172.20.200.1** ;iGWB's IP to connect fix network exchange(VirtualIP of Resource2)
 LocalIpToExBak = **172.30.200.1** ;iGWB's secondary IP to connect fix network exchange(VirtualIP of Resource3)
 BillRecSize = 156 ;Original bill record size(Bytes)
 BinAlarmSend = 1 ;Flag of sending binary alarm, 0-no, 1-yes
 BaseID = 3200 ;Binary alarm base ID
 SaveSecond = 1 ;Flag of offering the second copy of final bill files, 0-no, 1-yes
 MpuWindowSize=300

[MML]

LocalIpToMMLClient = **129.9.1.1** ;iGWB's IP to connect client(VirtualIP of Resource1)

[Cluster]

InstallShareDiskArray = 0 ;Flag of using sharing disk array, 0-no, 1-yes
 HeartBeatBroken = 300 ;Heartbeat link broken interval(seconds)
 HeartBeatCount = 2 ;Heartbeat link count
 ResourceCount = 3 ;Resource count

;Configuration of heartbeat link1

[Link1]

Type = UDP ;Heartbeat link type, UDP-private network, COM-serial communication port

Name = UDP_LINK ;Heartbeat link name

LocalIP = **130.1.1.2** ;Local heartbeat IP(IP of local NIC1)

PeerIP = **130.1.1.1** ;Peer heartbeat IP(IP of peer NIC1)

;Configuration of heartbeat link2

[Link2]

Type = COM ;Heartbeat link type, UDP-private network, COM-serial communication port

Name = COM_LINK ;Heartbeat link name

Port = 1 ;Port No., 1-COM1, 2-COM2

;Configuration of resource1

[Resource1]

ResType = IP ;resource type, IP-virtual IP

ResName = IP_OMC ;resource name, to connect OMC or Client

OriginalIP = **130.1.1.2** ;original IP, IP of NIC1

VirtualIP = **129.9.1.1** ;virtual IP

VirtualMask = **255.255.0.0** ;subnet mask of virtual IP

;Configuration of resource2

[Resource2]

ResType = IP ;resource type, IP-virtual IP

ResName = IP_PLANE1 ;resource name

OriginalIP = **130.1.2.2** ;original IP, IP of NIC2

VirtualIP = **172.20.200.1** ;virtual IP

VirtualMask = **255.255.0.0** ;subnet mask of virtual IP

SwitchGroup = 1 ;Only all the resources in the same SwitchGroup No. fail, the switch will be happened

;Configuration of resource3

[Resource3]

ResType = IP ;resource type, IP-virtual IP

```

ResName = IP_PLANE2           ;resource name

OriginalIP = 130.1.3.2       ;original IP, IP of NIC3

VirtualIP = 172.30.200.1    ;virtual IP

VirtualMask = 255.255.0.0   ;subnet mask of virtual IP

SwitchGroup = 1             ;Only all the resources in the same SwitchGroup No. fail, the switch will be
happened
    
```

A.3 Port Usage

The common ports and their functions are listed below.

I. Ports sued by iGWB

Table A-3 lists the ports used by iGWB while iGWB runs normally.

Table A-3 Ports used by iGWB

Port	Function
21	FTP server (control channel)
20	FTP server (data channel)
137	NetBIOS name service
138	NetBIOS datagram service
139	NetBIOS session service
161	SNMP
162	162 SNMP

II. Ports used by application

Table A-4 lists the ports used by the application while iGWB runs normally.

Table A-4 Ports used by the application

Port No.	Function	Parameters modified in the configuration file
6000	The maintenance port open to the client	[MML]LocalPortToCM
6001	The alarm port open to the client	[MML]LocalPortToAR
6002	The performance statistics port open to the NMS	[MML]LocalPortToPF
6007	The debugging port open to the client	[MML]LocalPortToRD

Port No.	Function	Parameters modified in the configuration file
6010	The parameter configuration port open to the client	[MML]LocalPortToCS
6099	The synchronization configuration port open to the NMS	[MML]LocalPortToSynConf
6100	The port that iGWBV300 opens to the alarm box	[MML]LocalPortToAlarmBox
9900	The slide window port that iGWBV300 opens to SoftX3000	[AccessPoint%d]LocalPortToEx LocalPortToExBak
9999	The communication port between internal processes	-

Appendix B Software Directory Description

B.1 Disk Directory Structure of iGWB Server

If you select the default directories during iGWB server installation, the directory structure on the hard disk of the iGWB server is as follows.

I. Structure of iGWB server installation directory

- Directory structure

Table B-1 Directory structure

Path	Description
C:\iGWB	Stores the process executable files, all configuration files and trace files.
C:\iGWB\Config	Stores all configuration files of iGWB.
C:\iGWB\Config\alarm	Stores all alarm configuration files.
C:\iGWB\Config\area	Stores the configurations files for area code and prefix, which are used for number change in some special cases. Judge whether to use these files according to actual conditions.
C:\iGWB\Config\format	Stores the configuration file of the CDR format being used.
C:\iGWB\Config\ini	Stores the parameter configuration file igwb.ini currently.
C:\iGWB\Config\mml	Stores the operation command table of iGWB.
C:\iGWB\Config\resource	Stores Chinese/English resource data, which are used to support bi-lingual operation interface.
C:\iGWB\Config\specailformat	Stores the configuration files of some special CDR formats. To use the special format, copy the corresponding configuration file to the directory C:\iGWB\Config\format.
C:\iGWB\trace	Stores the trace files recording important operation trace information or fault information during operation of iGWB. For more information about analysis and maintenance of the trace files, see 4.3.3 Common Trace Information or Its Maintenance.

- Main files

Table B-2 Main files

Path	Description
C:\iGWB\cls_proc.exe	The executable file of the dual system process. For details, see 1.3 System Software Architecture.
C:\iGWB\lap_proc.exe	The executable file of the access point process. For details, see 1.3 System Software Architecture.
C:\iGWB\knl_proc.exe	The executable file of the kernel process. For details, see 1.3 System Software Architecture.
C:\iGWB\lom_proc.exe	The executable file of the operation maintenance process. For details, see 1.3 System Software Architecture.
C:\iGWB\Config\alarm\alarmconfig.cfg	The alarm parameter configuration file. Through this file, you can see the alarm related parameter, such as severity.
C:\iGWB\Config\area\area.map	The area code configuration table, which is used for number change in some special cases.
C:\iGWB\Config\area\prefix.map	The prefix configuration table, which is used for number change in some special cases.
C:\iGWB\Config\ini\igwb.ini	The file used to set the important parameters of the system, such as the system working mode and external interface. For details, see 2.5.2 Configuring iGWB Server.
C:\iGWB\trace\knl_proc_trace.txt	The trace file of the kernel process.
C:\iGWB\trace\lom_proc_trace.txt	The trace file of the operation and maintenance process.
C:\iGWB\trace\cfg_proc_trace.txt	The trace file of the parameter configuration process.
C:\iGWB\trace\lap_procN_trace.txt	The trace file of the access point process. An access point process may have multiple process instances. Herein, N is the access point ID.

II. Structure of CDR storage directory

- Directory structure

Table B-3 Directory structure

Path	Description
d:\frontsave	The original CDRs of iGWB are stored in the d:\frontsave directory, firstly by access point, for example, X3KF, and then by date under each access point.

Path	Description
e:\backsave	<p>The final CDRs of iGWB are stored in the e:\backsave directory, usually in two copies.</p> <p>1) The CDRs are stored in the directory of e:\backsave\access point\path\date, that is, stored by access point, by path, and then by date.</p> <p>2) The copies are stored in the directory of e:\backsave\Second\point\path, in a slightly different structure. That is, the copies are no longer stored by date. This directory is usually open to the billing center to get CDRs, and the billing center is required to delete its obtained CDRs in real time. That's why there are usually no accumulated CDRs in this directory.</p>

- Main files

Table B-4 Main files

Name and path	Description
d:\frontsave\access point\path\date\b?.bil	<p>SoftX3000 sends a 156-byte CDR to iGWB regularly. Then, iGWB fills the content of the received CDR into the original CDR file till the file size exceeds the specified size, usually 3M. Afterwards, the preceding operations repeat for different original CDR files.</p> <p>The name of the original CDR file is b?.bil. Herein, the question mark ? is the serial number of the CDR, numbered from 000000001 to 999999999 by access point. For example, the file b000000009.bil in the d:\frontsave\X3KF\20040314 directory is the ninth original CDR file generated by the access point X3KF on Mar 14, 2004.</p>
e:\backsave\access point\path\date\b?.dat	<p>iGWB converts the received CDR information and fill it into the final CDR file while generating the original CDR, till the file size exceeds the specified size, usually 1M. Afterwards, the preceding operations repeat for different original CDR files.</p> <p>The name of the original CDR file is b?.dat. Herein, the question mark ? is the serial number of the CDR, numbered from 00000001 to 99999999 by path. For example, the file b00000009.dat in the e:\backsave\X3KF\detail\20040314 directory is the ninth detailed final CDR file generated by the access point X3KF on Mar 14, 2004.</p> <p>Note:</p> <p>1) For different conversion types, the generated CDR files are different.</p> <p>2) In the CDR storage directory, the "access point name" comes from the [AccessPoint%d] /APName setting in the parameter configuration file igwb.ini.</p>

III. Structure of other common directories

- Directory structure

Table B-5 Directory structure

Path	Description
d:\other	Stores the alarm, log and status files.
d:\other\alam	Stores the history alarm information.
d:\other\log	Store the log files. For the log related operations, see 3.3.3 Log Management.
d:\other\mml	Stores the operator information.
d:\other\perf	Stores the performance status information.
d:\StatusFile	Stores the system status files. Two types of subdirectories under this directory, one is the subdirectory named as the access point name, for example X3KF, and the other is the Status subdirectory.
d:\StatusFile\Status	Stores the system status files that are irrelevant to the specific access point, for example, the status file of the backup module and the backup of the front and back disk status files.
d:\StatusFile\access point	Stores the system status files of the corresponding access points.
d:\StatusFile\access point\network	Stores the status files for communication between access point and host.
d:\StatusFile\access point\save	Stores the status files of the front and back disks of the access point.
e:\ StatusFileB	Stores the backup of the d:\StatusFile directory.

- Main files

Table B-6 Main files

Name and path	Description
d:\other\log\?.log	The log file, with the log generated date as its prefix, for example, 20040420.log.
d:\StatusFile\Status\backup_status.bsf	The status file of the backup module.
d:\StatusFile\access point\network\status.dat	The status file for communication between the access point and host.
d:\StatusFile\access point\save\X3KF_FS_MAIN.stf	The status file of the front disk of the access point, for example, X3KF_FS_MAIN.stf is the front disk status file of the access point X3KF.

Name and path	Description
d:\StatusFile\access_point\save\ X3KF_BS_?_MAIN.stf	The status file of the back disk of the access point. Herein, the question mark ? is the path number. For example, X3KF_BS_00_MAIN.stf is the back disk status file of path 0 of the access point X3KF.

B.2 Structure of Client Software Directory

The default installation directory of the iGWB client is c:\igwb_Client where the subdirectory Bin and Data exist. Herein, the Bin subdirectory stores the executable files and dynamic link files, and the Data subdirectory stores the client data files and help files.

- Directory structure files

Table B-7 Structure of the client installation directory

Path	Description
C:\iGWB_Client\bin	Stores the executable files and dynamic link files.
C:\iGWB_Client\data	Stores the client data files and help files.

- Main files

Table B-8 Main files

Path	Description
C:\WINNT\UICONFIG.ini	The client parameter configuration file. Usually, you do not need to modify the configuration of the maintenance and debugging ports of the client manually.
C:\iGWB_Client\bin\Frame.exe	The executable file of the CDR console. This file can be directly run.

Appendix C Acronyms and Abbreviations

Abbreviation	Full name
A	
AP	Access Point
B	
BAM	Back Administration Module
BIOS	Basic Input/Output System
BS	Billing System
BC	Billing Center
C	
CDR	Call Detail Record
F	
FE	Fast Ethernet
FTAM	File Transfer Access Management
FTP	File Transfer Protocol
G	
GMT	Greenwich Mean Time
I	
iGWB	iGateway Bill
IP	Internet Protocol
L	
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LAN	Local Area Network

Abbreviation	Full name
M	
MAC	Media Access Control
MML	Man Machine Language
MSC	Mobile Switching Center
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
N	
NSAP	Network layer Service Access Point
O	
OMC	Operation & Maintenance Center
P	
PCI	Peripheral Component Interconnect
PSAP	Presentation layer Service Access Point
Q	
QoS	Quality of Service
R	
RAID	Redundant Arrays of Inexpensive Disks
S	
SCSI	Small Computer Systems Interface
SMUI	System Management Unit
STP	Signaling Transfer Point
T	
TCP	Transfer Control Protocol
TSAP	Transport layer Service Access Point

Abbreviation	Full name
U	
UDP	User Datagram Protocol