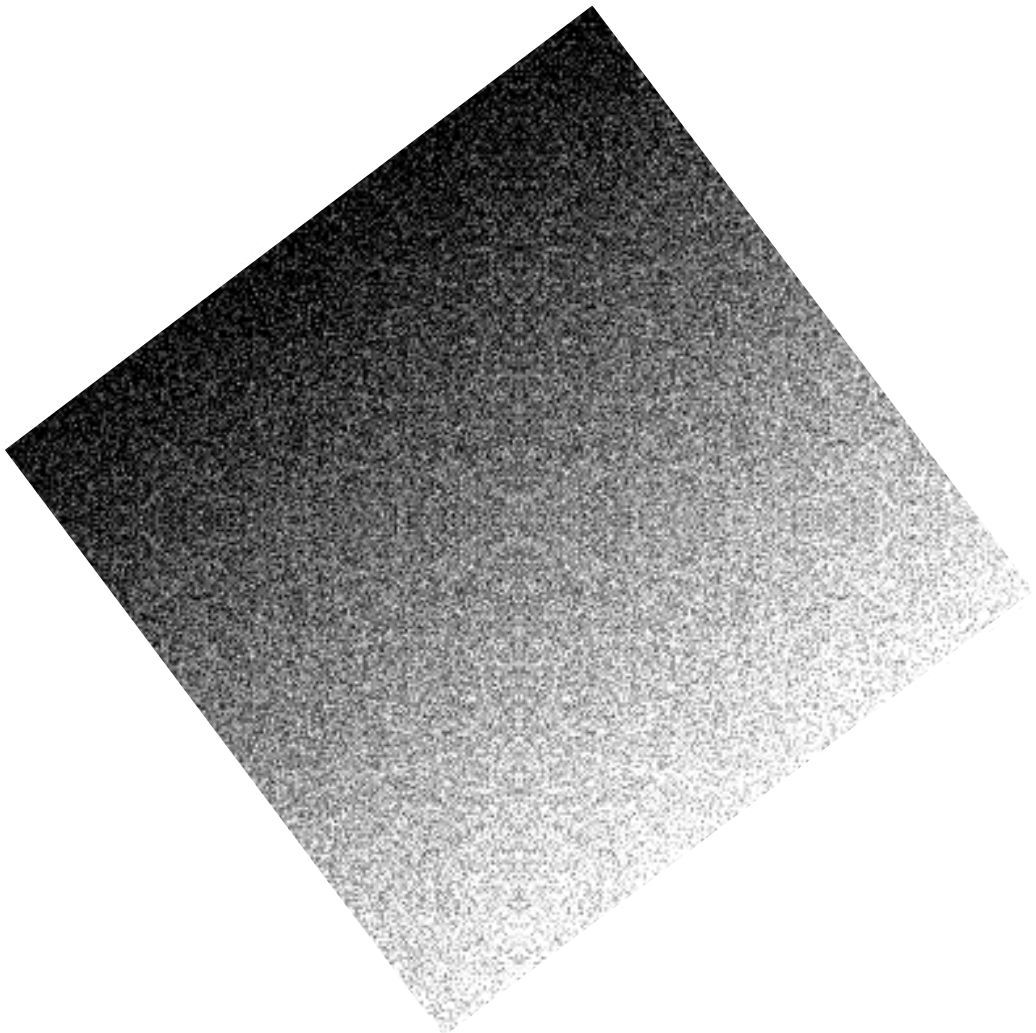
Intelligent Decision Server

IBM

Installing IDS LAN Components

Version 1



GC26-8877-00

Intelligent Decision Server

IBM

Installing IDS LAN Components

Version 1

GC26-8877-00

Note

Before using this information and the product it supports, be sure to read the general information under “Notices” on page vi.

First Edition (October 1996)

This edition applies to Version 1 of Intelligent Decision Server, 5639–IDS, and to any subsequent releases until otherwise indicated in new editions or technical newsletters. Make sure you are using the correct edition for the level of the product.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© **Copyright International Business Machines Corporation 1996. All rights reserved.**
Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Notices vi
Trademarks vi

About This Book viii
Who Should Read This Book viii
How to Use This Book viii
We'd Like Your Comments ix

Chapter 1. Introduction to Installing the Intelligent Decision Server 1
The IDS Structure 1
IDS Services 2
IDS Assignable Assets 4

Chapter 2. Preparing for Installation 7
Collecting Information 7
Hardware and Software Requirements 7
Hardware Requirements 7
Software Requirements 10

Chapter 3. Installing and Initializing the Primary File Server 11
Installing the Primary Server 11
Stopping the IDS Installation 14
Removing IDS 14
Initializing the Primary File Server 14
Logging onto the Primary File Server 15
Initializing Additional File Server Volumes 16

Chapter 4. Installing and Initializing an Auxiliary File Server 17
Installing an Auxiliary File Server 17
Initializing Auxiliary File Server Volumes 19

Chapter 5. Installing Other IDS Services 21

Chapter 6. Installing the IDS Developer's Desktop 24
Installing from the IDS CD-ROM 24
Creating an Installation Diskette 26
Starting the IDS Developer's Desktop 26

Chapter 7. Installing and Configuring ODAS Components 28
Adding ODAS 29
Installing ODAS Administration and Client Test Applications 30
Starting ODAS 30
Logging On to the ODAS Administration Application 30
Administration Interface 31
Resizing Columns 32

© Copyright IBM Corp. 1996

Configuring the ODAS Server 32
Installing ODAS Clients 33
Testing the Connection to ODAS on Windows 34

Chapter 8. Configuring Nodes and Adding Users and Tools 36
Planning 36
Opening the SA Tool 36
Registering Workstations as Nodes 37
Adding Users and Tools 39
Registering User IDs 39
Assigning Tools to a Registered Node 40
Assigning Tools to a User ID 40

Chapter 9. Adding IDS Services to a Server or Node 42
Opening the Asset Manager 42
Adding the Mail Service 42
Configuring the Mail Service 45
Adding the Auxiliary File Service 46
Adding the Print Service 47
Adding the Print Service Manager 47
Adding the Print Service Execution Engine 49
Adding the Printer Host 51
Adding the Capsule Service 53
Adding the Capsule Service Manager 53
Adding the Capsule Service Execution Engine 54
Adding the Conversion Service 56
Adding the Conversion Service Manager 56
Adding the Conversion Service Execution Engine 58
Adding the Remote Mail Gateway Service 59
Adding the OS/2 Database Gateway Service 61
Configuring a Database Gateway Service 65
Other Database Tasks 70

Appendix A. Planning an IDS Network 72
What Is a Network? 72
What Skills Are Required for Planning IDS LANs? 72
Basic Network Design 73
Physical Medium 74
Network Topology 74
Connective Devices 77
Designing IDS Networks 81
Selecting the Physical Medium and the LAN Protocol for Your IDS Network . 82
Using Bridges in IDS Networks 85
Using Routers in IDS Networks 87
Using Routable Desktops in IDS Networks 88
Expanding Your Network with Realms 89
Integrating IDS into Existing Networks 92
Adding IDS to a Multiprotocol Environment 93

Evaluating Your Environment 93

Glossary 96

IDS Publications 99

Index 101

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Subject to IBM's valid intellectual property or other legally protectable rights, any functionally equivalent product, program, or service may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A.

Licensees of this program who wish to have information about it for the purpose of enabling (1) the exchange of information between independently created programs and other programs (including this one) and (2) the mutual use of the information that has been exchanged, should contact:

IBM Corporation
555 Bailey Avenue, W92/H3
P.O. Box 49023
San Jose, CA 95161–9023

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

Trademarks

The following terms are trademarks of IBM Corporation in the United States or other countries or both:

ACF/VTAM	DXT	PROFS
AIX	Enterprise System/9000	PS/2
Application System/400	ES/9000	QMF
APPN	IBM	RACF
AS/400	MVS/ESA	RISC System/6000
Capsule	MVS/XA	RS/6000
DATABASE 2	OfficeVision	S/390

© Copyright IBM Corp. 1996

DataJoiner	OfficeVision/VM	SQL/DS
DB2	Operating System/2	System/360
DB2 for OS/2	Operating System/400	System/370
DB2/6000	OS/2	Virtual Machine/Enterprise Systems Architecture
DFSORT	OS/400	VM/ESA
Distributed Relational Database Architecture	Personal System/2	VTAM
DRDA	Presentation Manager	Win-OS/2

C-bus is a trademark of Corollary, Inc.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Microsoft, Windows, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

About This Book

This book discusses how to design an Intelligent Decision Server (IDS) network, and provides instructions for installing the basic IDS components and performing administration tasks necessary to fully enable your IDS network.

Who Should Read This Book

This book should be read by people who are responsible for:

Planning and designing an IDS network: You should be familiar with the general principles of TCP/IP and LAN administration.

Installing and setting up servers: You should be familiar with the general principles of system and LAN administration.

Network administration tasks, such as creating user IDs and granting tool access: You should be familiar with the general principles of system and LAN administration.

Installing a developer's desktop on a workstation: You should be familiar with using a workstation.

How to Use This Book

The following lists details the sections of the book you should focus on, depending on your task:

Planning an IDS network

Appendix A, “Planning an IDS Network” on page 72. Complete the planning tasks in this appendix before installing the IDS LAN components.

Installing the primary file server

Chapter 3, “Installing and Initializing the Primary File Server” on page 11

Chapter 8, “Configuring Nodes and Adding Users and Tools” on page 36

Chapter 9, “Adding IDS Services to a Server or Node” on page 42

Installing an auxiliary file server

Chapter 4, “Installing and Initializing an Auxiliary File Server” on page 17, with necessary administration tasks in:

Chapter 8, “Configuring Nodes and Adding Users and Tools” on page 36

Chapter 9, “Adding IDS Services to a Server or Node” on page 42

Installing other services

Chapter 5, “Installing Other IDS Services” on page 21, with necessary administration tasks in:

© Copyright IBM Corp. 1996

Chapter 8, “Configuring Nodes and Adding Users and Tools” on page 36

Chapter 9, “Adding IDS Services to a Server or Node” on page 42

Installing a developer's desktop

Chapter 6, “Installing the IDS Developer's Desktop” on page 24, with necessary administration tasks in Chapter 8, “Configuring Nodes and Adding Users and Tools” on page 36.

We'd Like Your Comments

Your feedback is important to us in providing you with the most accurate and high-quality information. If you have any comments about this book or any other IDS documentation, please visit our Website at:

http://www.dss.ibm.com

There you'll find the Feedback Connection page where you can enter comments and send them to us.

Chapter 1. Introduction to Installing the Intelligent Decision Server

This chapter describes the Intelligent Decision Server (IDS) network and how the IDS services interact. For an overview of each IDS service, see “IDS Services” on page 2. For an overview of LAN and connectivity concepts and how they apply to an IDS network, see Appendix A, “Planning an IDS Network” on page 72.

The IDS Structure

The Intelligent Decision Server (IDS) is a network computing server designed to support a wide range of clients and provide a collection of services that give important function to the IDS network. The client-server environment lets you distribute your data over workstations directly or remotely connected to the IDS network and enables these services on one workstation or disperses them.

An IDS network is a collection of one or more *realms* on the same network. Each realm is a logical grouping of IDS services that includes its own *primary file server*. The primary file server manages data for other IDS services in the same realm. Thus, you can have multiple primary file servers on the same network, but only one per realm. For an example of logically grouped IDS services, see Figure 1 on page 2.

When a primary file server is installed, all the basic services required for running an IDS network are automatically installed. These services include the:

- Primary file service
- Directory service
- Asset management service
- Developer's desktop
- Other services

All other services use these services, which are installed on the primary file server. Before other services can run, the primary file server must be installed and running. The base services also provide function for network clients (nodes and users) and the tools necessary to administer and maintain the network. For example, the primary file server is used to assign *assets* to users and nodes. Assets are services, such as the capsule service, and tools or tool sets, such as the Text and Query tools.

Auxiliary file servers can also be installed on the realm. With the auxiliary file server, you can create additional disk-storage space. Each realm supports up to seven auxiliary file servers with three file service volumes each, for a possible total of 24 volumes.

The IDS developer's desktop is an interface used primarily to develop applications and to access and run IDS services; administrators use the developer's desktop to manage services and assets for the realm.

For users to access the network through the developer's desktop, they must have an IDS user ID, or the workstation must be registered as a *node*. A workstation becomes a

© Copyright IBM Corp. 1996

node when an administrator registers it with the asset manager and assigns a specific set of functions, or assets, to it.

Figure 1 illustrates an IDS network with one realm, in which several services and desktops are connected to a host through an Ethernet LAN.

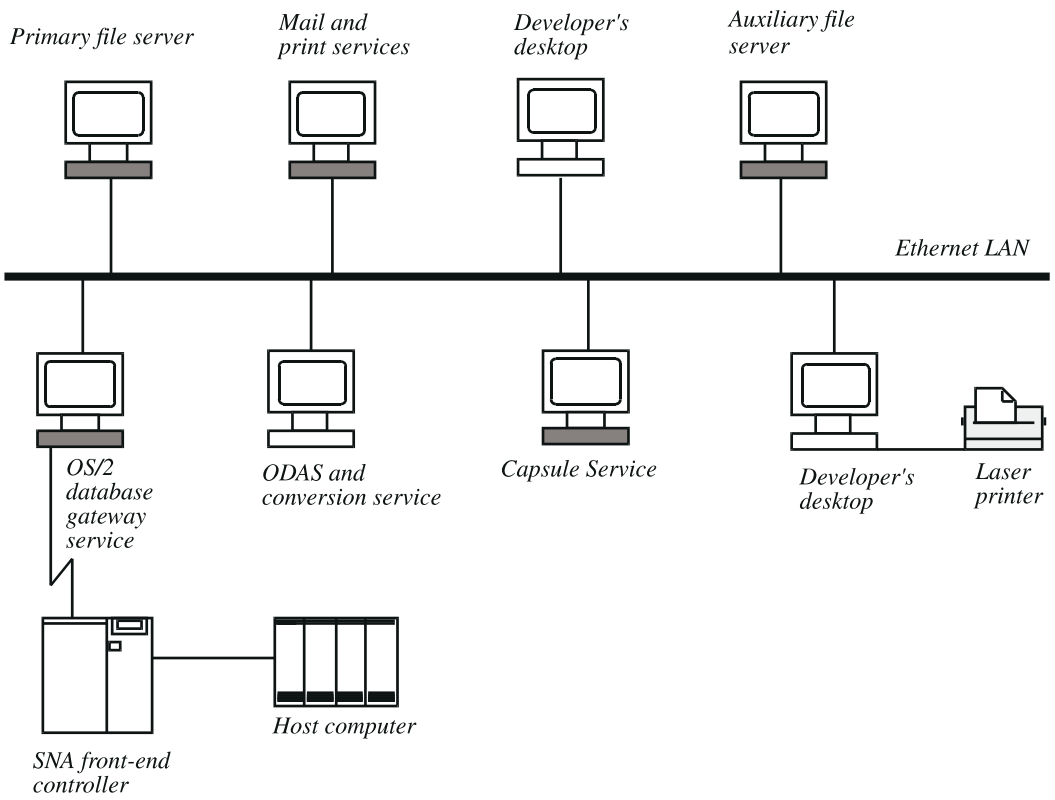


Figure 1. Sample IDS network

IDS Services

IDS is made up of many services that can reside on one workstation or be distributed across many workstations. By distributing services across multiple workstations, you can expand your network and interact with mainframe computers residing on networks. All services require that the primary file server be installed and running, except the services automatically installed on the primary file server. The following list provides a brief descriptions of all IDS services. For detailed descriptions of the services, see the *System Administration Guide and Reference* .

Asset Management Service

The asset management service (also called the asset manager) controls the allocation of services and tools for nodes and users within the realm.

Services can be assigned to nodes; tools can be assigned to nodes and users. Services and tools can only be assigned with the asset manager, which is accessible from a developer's desktop.

Capsule Service

With the capsule service, users can submit capsule applications from a desktop, which then execute on an appropriate service.

Conversion Service

The conversion service converts data shared between IDS and other sources into a format appropriate to each. This service is a prerequisite service for the Open Data Access Service (ODAS).

Developer's Desktop Service

The IDS developer's desktop is an interface used primary to develop applications and to access and run IDS services; administrators use the developer's desktop to manage services and assets for the realm.

Directory Service

The directory service tracks nodes and services that are connected to the realm.

File Services

The primary file service manages data for other IDS services in the same realm. A realm number is assigned to each primary file server. During installation, auxiliary file servers and developer's desktops must be assigned the same realm number as the primary file server.

With the auxiliary file server, you can create additional file service volumes (disk space). Each realm supports up to seven auxiliary file servers with three file service volumes each, for a possible total of 24 volumes.

Mail Service

The mail service sends and receives mail between realms that are connected to an IDS network or to a mail gateway for distribution to another network.

Open Data Access Service (ODAS)

A service that allows popular applications, such as Lotus Notes, web browsers, and ODBC applications, to access IDS. For this service to run, the conversion service must be installed on the same realm.

OS/2 Database Gateway Service

The OS/2 database gateway service is a generic gateway that provides access to local or remote relational database management systems. The IBM Communications Manager must be available for some of the gateways to function.

This service supports the following database gateway types:

DB2

DB2 for OS/2

DRDA

MVS CAS

Printer Host

The printer host receives formatted documents from the print service and sends them to the OS/2 printing queue. For the printer host to function, the print service must be installed on the same realm.

Print Service

The print service formats IDS documents and submits them to the printer host queue. The documents are then printed from the printer host. For the print service to run, the printer host must be installed on the same realm.

Remote Mail Gateway Service

The remote mail gateway service formats, converts, and transfers mail between a cc:Mail** post office and an IDS mail service. For this service to function, the conversion service must be installed on the same realm.

IDS Assignable Assets

Table 1 lists all IDS assets that can be assigned to a user ID or to a node from the asset manager. This table can help you plan asset management.

Table 1 (Page 1 of 3). Assignable Assets

Asset Name	Description
Administrator Tools	Desktop logon, 911 report generator, Transformer and Network Diagnostics tools, conversion-table utility, MakeSecure, MakeUnSecure, SetQuota and UpdateQuota transformers.
AIX Database Gateway Service	Database gateway service for ORACLE**, Red Brick**, or SYBASE** AIX and DB2 for AIX database gateways.
Auxiliary File Service	File services running on workstations other than the primary file server.
Capsule Service Execution Engine	A process that executes one capsule application at a time. Each execution engine returns results to its capsule service manager.
Capsule Service Manager	Controls Capsule service's execution engines.
Conversion Service Execution Engine	A process that runs one conversion job at a time, converting spreadsheets or other items between different formats. Each execution engine returns results to its conversion service manager.
Conversion Service Manager	The manager controls the conversion service execution engines.
DB2 Sessions	Simultaneous sessions through an OS/2 database gateway for access to DB2 databases.
DataJoiner AIX Sessions	Simultaneous sessions through an AIX database gateway service for access to DataJoiner databases.
DB2 for OS/2 Sessions	Simultaneous sessions through an OS/2 database gateway for access to DB2 for OS/2 databases.
DB2 for OS/2-DRDA Sessions	Simultaneous sessions through an OS/2 database gateway for access to DB2 for OS/2 databases using Distributed Relational Database Architecture (DRDA).

Table 1 (Page 2 of 3). Assignable Assets

Asset Name	Description
DB2 for AIX Sessions	Simultaneous sessions through a UNIX gateway for access to RS/6000 databases.
Directory Service	The service for name resolution and other functions of realm administration; each realm has one directory service.
Executive	Desktop logon, Layout (viewing only), Reporter (viewing only), Capsule Service tool, Spreadsheet, Text, Plot, Browser, Data Entry, Format, Logging, PC Application, PC Data, PC Directory, Screen Capture, Calculator, Dictionary, Mail Tray, Envelope, and Discard tools, plus licenses to execute any tool within a Capsule application.
Expert Plus	Everything in the Explorer Plus tool set plus Basic, DBA, Forms Design, SQL Entry, and Transformer tools; SetDBAccess, and Capsule transformers (Join, MultiJoin, Merge, Append, Message, Append Message, Post Message, CAS, Compress, Concatenate, Clean, Conditional Clean, Convert Basic, Copy, Clear Contents, Data Format, Date Format, Error Log, Function, Header, Label, Split Header, Multiple Split, Page Break, Period Table, Pivot, Random Number, Replace, Row Clean, Row Select, Select, Multiple Select, Sort, Substitute, Switch, Text Switch, Text to Spreadsheet, Transpose, Word Count, and Write SQL transformers); In and Out transformers for Capsule applications; administrative transformers MakeSecure and MakeUnSecure; and Capsule Placeholder and Reference icons.
Explorer Plus	Everything in the Executive tool set plus the Query tool and full use of Reporter and Layout.
HP-UX Database Gateway Service	Database gateway service for one or more ORACLE, Red Brick, or SYBASE HP-UX database gateways.
Mail Service	The service that distributes mail within an IDS realm.
MVS CAS Sessions	Simultaneous sessions through the Cooperative Access Services gateway for communicating with MVS systems.
ODAS Gateway Sessions	ODAS gateway services and simultaneous sessions through the Open Data Access Server gateway.
ODAS	A service that allows popular applications, such as Lotus Notes, Web browsers, and ODBC applications, to access IDS.
ORACLE AIX Sessions	Simultaneous sessions through an AIX database gateway service for access to ORACLE RS/6000 databases.
ORACLE HP-UX Sessions	Simultaneous sessions through an HP-UX database gateway service for access to ORACLE HP 9000 databases.
ORACLE Solaris Sessions	Simultaneous sessions through a Sun/Solaris database gateway service for access to ORACLE Sun/Solaris databases.
OS/2 Database Gateway Service	Database gateway service for one or more OS/2 database gateways (OS/400, DB2, or DB2 for OS/2).
Print Service Execution Engine	A process that runs one printing job at a time. Each execution engine returns results to its print service manager.
Print Service Manager	The manager controls the print service execution engines.
Printer Host	The workstation a printer is attached to.

Table 1 (Page 3 of 3). Assignable Assets

Asset Name	Description
Redbrick AIX Sessions	Simultaneous sessions through an AIX database gateway service for access to Red Brick RS/6000 databases.
Redbrick HP-UX Sessions	Simultaneous sessions through an HP-UX database gateway service for access to Red Brick HP 9000 databases.
Regression and Time Series Analysis Transformers	AutoCorrelation, Correlation, AutoRegression, Regression, Elementary, Forecast, Moving, and Seasonality transformers.
Remote Mail Gateway	The mail gateway that formats, converts, and transfers mail between a cc:Mail Post Office or an IDS Mail Service and IDS desktops.
Significance and Sample Testing Transformers	ANOVA, ChiSquare, CrossTab, IPMean, Kruskal, KSTest, NPCorrelation, NPIndependent, and NPPaired transformers.
Solaris Database Gateway Service	Database gateway service for one or more ORACLE or SYBASE Sun/Solaris database gateways.
SYBASE AIX Sessions	Simultaneous sessions through an AIX database gateway service for access to SYBASE RS/6000 databases.
SYBASE HP-UX Sessions	Simultaneous sessions through an HP-UX database gateway service for access to SYBASE HP 9000 databases.
SYBASE Solaris Sessions	Simultaneous sessions through a Sun/Solaris database gateway service for access to SYBASE Sun/Solaris databases.

Chapter 2. Preparing for Installation

This chapter describes tasks that need to be performed before the Intelligent Decision Server is installed and lists hardware and software requirements.

Collecting Information

The IDS installation SmartGuide provides defaults for network information based on the TCP/IP address of the workstation that will become the primary file server. The only information you need before installing IDS is:

Disk space requirements. Determine how much disk space you'll need for your IDS volumes, based on anticipated needs.

File descriptor size for each volume, except the first volume on the primary file server

A volume is a virtual disk drive, similar in function to a hard disk partition.

The *file descriptor* size for the first volume on the primary file server is automatically set to 10. File descriptors function like a directory for a hard drive, keeping descriptive information for each file. The percentage you specify for file descriptors is a percentage of the volume devoted to file descriptors.

For subsequent volumes, you can choose the file descriptor size. A file descriptor size between 40 to 70 is typical. The descriptor can be adjusted at any time to accommodate any necessary changes. For more information on file descriptions, see the *System Administration Guide and Reference* .

If you do not use the defaults provided by the IDS installation application, you'll also need to know the following information:

Unique realm number

Unique name for each file service volume, except the first, which is always System

Important: The realm number assigned to the primary file server must be used for all other services on the same realm.

Hardware and Software Requirements

Each IDS component has specific hardware and software requirements. Make sure your system meets the requirements for each component before you begin installation.

Hardware Requirements

The following requirements are broken down by RAM and disk space requirements, then by service. All IDS services require a minimum of 20 MB of disk space for IDS services.

© Copyright IBM Corp. 1996

Disk Space Requirements

The minimum and recommended disk space requirements for IDS services are listed in Table 2. The listed disk sizes include space for OS/2 and the service. Additional space is always preferable.

For file services, each IDS volume can be as large as 1.2 GB with up to 3 IDS volumes per server. Each volume must be on a separate hard disk partition. Each realm can support up to 24 IDS volumes: 3 volumes for the primary file service and 21 volumes for the 7 auxiliary file services.

Important: All IDS services require a minimum of 20 MB of disk space for IDS services.

Table 2. Disk space requirements

Service	Minimum for Installation	Recommended
Auxiliary file server	20 MB	150 MB default, up to OS limit
Capsule Service	160 MB	160 MB
Conversion service	100 MB	160 MB
Developer's desktop	10 MB	120 MB, up to the OS limit
Directory service	160 MB	Up to the OS limit
Mail service	100 MB	150 MB
Open data access service	160 MB	160 MB
OS/2 database gateway service	200 MB	Up to the OS limit
Primary file server, system volume	95 MB	150 MB default, up to OS limit
Primary file server, additional volumes	20 MB	150 MB default, up to OS limit
Print service	160 MB	160 MB
Remote mail gateway service	120 MB	120 MB

Monitor Requirements

Only two IDS services have requirements for monitor displays:

Primary file server: A monitor with 1024×768×256 or higher display resolution

Developer's desktop: A monitor with 1024×768×256 or higher display resolution

RAM Requirements

Each IDS service requires a minimum amount of RAM and disk space but operates more efficiently with more than that minimum. When you install more than one IDS service on the same workstation, the required amount of RAM and disk space changes.

For example, if you have the conversion service installed on a workstation with 16 MB of RAM and you add the ODAS, you'll need an additional 4 MB of RAM for the workstation, minimum, for a total of 20 MB of RAM. Because the services share some of the same resources, when you install more than one service in a computer, the second and

subsequent services require less RAM and disk space than each would require when installed alone. Table 3 on page 9 lists the minimum and recommended amounts of RAM per service, and per additional service on the same workstation.

Important: The conversion service, print service, and capsule execution service all require execution engines (for information on execution engines, see Chapter 9, "Adding IDS Services to a Server or Node" on page 42). If a workstation has more than one service with an execution engine, add an additional 1 MB of RAM per execution engine.

Table 3. RAM requirements

Service	Stand-alone		Additional per service	
	Minimum	Recommended	Minimum	Recommended
Auxiliary File Service	12 MB	16	4 MB	8 MB
Capsule Service	16 MB	32-64 MB	4 MB	8 MB
Conversion service	16 MB	24-32 MB	4 MB	8 MB
Developer's desktop	8 MB	16 MB	2 MB	8 MB
Directory service	12 MB	16 MB	4 MB	8 MB
Mail service	8 MB	12 MB	2 MB	4 MB
Open data access service	12 MB	16 MB	4 MB	8 MB
OS/2 database gateway service	12 MB	16 MB	4 MB	8 MB
Primary file server	24 MB	32 MB	4 MB	8 MB
Print service	16 MB	24 MB	4 MB	8 MB
Remote mail gateway service	12 MB	16 MB	0 MB	4 MB

Combining Services

Avoid combining services on a workstation that intensively use the same type of resources, such as I/O and RAM, unless you have plenty of that resource.

Table 4 lists IDS services and the primary type of activity (such as I/O, processor, disk, or RAM).

Table 4 (Page 1 of 2). Service activity

Service	Type of activity
Asset Management service	RAM
Capsule service	Depends on the types of capsule applications that are submitted to the capsule service
Conversion service	Depends on the types of icons being converted
File services	I/O, disk, and RAM
Mail service	I/O and RAM

Table 4 (Page 2 of 2). Service activity

Service	Type of activity
Remote mail gateway service	I/O, disk, and RAM
Printer host	I/O, disk, and RAM
Print service	Depends on the types of jobs being printed
Desktop	RAM and processor

Software Requirements

The IDS networks using TCP/IP protocol require IBM's TCP/IP Version 2.0 or later with the latest corrective service diskette. This stack can coexist with other protocols such as IPX or IDS NPD. Other TCP/IP-based applications and services can coexist on the same computer and network as IDS-based desktops and services.

Recommendation: Use TCP/IP Version 3 to minimize compatibility difficulties.

The following requirements are broken down by what you will need for each IDS component. All IDS services require 20 MB disk space for the product software.

General IDS service requirements:

- OS/2 Warp or later
- TCP/IP for OS/2, Version 2 or later

IDS developer's desktop:

- OS/2 Warp or later
- TCP/IP for OS/2, Version 2 or later

OS/2 database gateway service:

- Communications Manager
- To access sample databases, DB2 for OS/2 Warp or later

Chapter 3. Installing and Initializing the Primary File Server

This chapter guides you through installing the basic services for the primary Intelligent Decision Server (IDS) and through initializing the primary file server service volumes. The primary file server must be installed before other services, such as the developer's desktop, can be installed.

The primary file server manages data for other IDS services in the same realm. You must have one primary file server for each realm. Each realm supports up to seven auxiliary file servers with three file service volumes each, for a potential of 24 file service volumes. If your network is heavily used and has multiple desktops, you should dedicate one workstation as the primary file server. In addition to the primary file service, the asset management service, the directory service, and developer's desktop are installed during primary file server installation.

Before you install the primary file server, complete the tasks listed in Chapter 2, “Preparing for Installation” on page 7.

To install and initialize a primary server, complete the tasks in the following sections of this chapter:

1. “Installing the Primary Server”
2. “Initializing the Primary File Server” on page 14
3. If you defined additional file server volumes, “Initializing Additional File Server Volumes” on page 16

After you set up your primary file server, complete the following administration tasks:

Register workstations in the IDS network as nodes in the asset manager, as described in “Registering Workstations as Nodes” on page 37

Add IDS services to servers and nodes, as described in Chapter 9, “Adding IDS Services to a Server or Node” on page 42

Add users to the asset manager, as described in Chapter 8, “Configuring Nodes and Adding Users and Tools” on page 36

Assign tools to a user or node, as described in Chapter 8, “Configuring Nodes and Adding Users and Tools” on page 36

Create developer desktops on the IDS network, as described in the *System Administration Guide and Reference*

Installing the Primary Server

To install the primary file server:

1. Load the IDS Installation CD into the CD-ROM drive on the target workstation.

   In the following instructions, F is used to represent the CD-ROM drive letter.

2. Open an OS/2 window.

© Copyright IBM Corp. 1996

3. From the F:\SERVER directory on the CD-ROM, type install then press Enter.

   The Instructions window opens.

4. Click on the **Continue** button. The Installation window opens.
5. Click on the **Update CONFIG.SYS** box to automatically update the CONFIG.SYS file.

   If you do not place a check in the box, you will need to update your CONFIG.SYS file manually. An updated file, called CONFIG.ADD, will be placed in the installation directory. Compare the changes in this file to your current CONFIG.SYS file.

6. Click **OK**. The Installation-Directories window opens.
7. Select the components you want to install from the list box, such as IDS Software and IDS Documentation.

   If you select only IDS Documentation, continue up to step 10. The books will install, but the IDS SmartGuide will not display to guide you through software instillation.

8. In the **Installation Directory** box, type the path for the directory where you want the primary file service installed. The default directory is C:\IDSSRV.
9. Verify that the target drive contains enough available disk space:

   a. Click on the **Disk space** button. The Disk Space window opens. The available drives and available disk space displays.

      If the “Bytes needed” to install the selected components exceeds the “Bytes available,” specify a different drive with enough disk space from the Install-Directories window.

      Important: The "Bytes needed" to install the selected components includes only the minimum space required for IDS; the space needed for file service volumes is not included. For recommendations on disk space requirements, see “Hardware and Software Requirements” on page 7.

   b. Click **OK** to return to the Install-Directories window.

10. Click on the **Install** button. The Install-Progress window opens.

    As files install on your server, the progress bar updates. During this process, you can click on the **Help** button to display online help, or click on the **Stop** button to cancel installation.

    When the progress bar indicates the installation is approximately half done, the IDS Services Installation SmartGuide opens the Welcome page. On any page in the SmartGuide, you can click on:

    <<**Back** to display and change previous pages (except on the first page)

    Next>> to display the next SmartGuide page

    Stop to cancel installation

    Help to display online help for the SmartGuide page

11. From the Welcome page, click on the **Next>>** button. The File Service Type page opens.
12. Select the **Primary File Server** button if it is not already selected, then click on the **Next>>** button. The Realm Number page opens with a default value shown in the **IDS realm number** field.
13. Record the default value, or set and record your own value; this value is used when installing an auxiliary file server, installing other services, and installing a developer's desktop.

    The realm number identifies a server to other IDS servers and desktops. The default realm number is taken from the last segment of the TCP/IP address.

    Recommendation: Use the default setting to simplify installation of other services and for easier information tracking.
14. Click on the **Next>>** button. The File Server Volumes page opens.
15. Define from one to three file server volumes:
    a. Select a volume number.

       Each volume number can be used only once, and only one volume can be assigned per hard disk partition. Up to three volumes can be defined.

       If enough disk space is not available to install a file service volume, the volume numbers cannot be selected.
    b. In the **Drive** field, select a drive letter.
    c. In the **Name** field, use the default name or type a different name for the file server volume.

       Recommendation: Use the default name for the file server volume to simplify installation and to make information tracking easier.

    Repeat steps 15a through 15c to define additional file server volumes. The first volume you define is automatically initialized when you start IDS. If you define additional volumes, you need to initialize them separately. See “Initializing Additional File Server Volumes” on page 16.
16. Click on the **Next>>** button. The File Server Volume Size page opens.
17. Specify the size for each file server volume you defined on the previous page:
    a. Select the number for the volume you want to size. The displayed drive letter and name automatically update for the volume you selected.
    b. Click and hold on the slider arm, then move it left or right to set the appropriate volume size. You can also use the ← and → buttons to set the slider arm.

    Repeat steps 17a through 17b to specify the size for additional volumes.
18. Click on the **Done** button.

The SmartGuide closes and the Install-Progress window reopens and updates the status bar as files copy. When the installation successfully completes, an Installation and Maintenance window opens and displays the elapsed time.

19. Click on **OK**.

    The installation program closes. The Intelligent Decision Server folder is placed on your desktop.

20. Reboot your server.

The primary file server installation is complete.

Stopping the IDS Installation

If a **Cancel** button is available, you can click on it at any time. Answer the prompts that display, then the installation application exits to the OS/2 Window or IDS Installation window, depending on where you are in the installation.

If you are working in the IDS Services Installation SmartGuide, click on the **Stop** button at any time. The installation application exits to the OS/2 window.

If a progress window is open, click on the **Stop** button at any time. A window opens, asking if you want to stop the installation. Confirm the prompt. The progress bar in the Install - progress window moves backward as files are removed. The installation application then exits to the OS/2 window.

Removing IDS

If you need to remove IDS from your server, automated removal features are included in the installation software.

To remove IDS:

1. Open an OS/2 window and navigate to the IDS installation directory. If you accepted the default, the directory is C:\IDSSRV.
2. Type install then press Enter. The Instructions window opens.
3. Click on the **Continue** button. The Installation Options window opens.
4. Click on the **Delete the installed product and re-install** button, then click on the **Continue** button. The Delete window opens.
5. Click on the **Select all** button, then click on the **Delete** button.
6. The Install - progress window opens, and the progress bar moves backward as files are removed. After IDS is removed, the application exits to the OS/2 Window.

Initializing the Primary File Server

Before you can initialize the primary file server, you must install the primary server as described in “Installing the Primary Server” on page 11.

1. If you did not reboot the server after completing the instructions in “Installing the Primary Server” on page 11, do so now.

2. Make sure the IDS Installation CD is still in the CD-ROM drive.
3. Double-click on the Start IDS Server icon in the Intelligent Decision Server folder.

   Automated installation and initialization procedures begin that might take up to a half hour. During this process, the IDS system volume is configured and loaded. Status messages display in the OS/2 window. After the automated process completes successfully, the IBM Intelligent Decision Server Desktop window opens.

The primary file server installation and initialization is complete. If you defined multiple file server volumes, you need to initialize them with a different procedure, as described in “Initializing Additional File Server Volumes” on page 16.

Logging onto the Primary File Server

After the primary file server initializes, the IBM Intelligent Decision Server Desktop window opens.

To log on to the server for the first time:

1. At the user ID prompt, type:

   system

   Then press enter. The password prompt appears.

   Important: The user ID is case sensitive; type it exactly as shown.
2. At the password prompt, type:

   original

   Then press Enter. The IDS developer's desktop opens.

   Important: The password is case sensitive; type it exactly as shown.

To change the user ID and password, see the *System Administration Guide and Reference* .

While you are working with the primary file server, you might find it convenient to configure nodes and add new users and tools at this time. See Chapter 8, “Configuring Nodes and Adding Users and Tools” on page 36.

To log off of the developer's desktop:

1. Close any open windows by clicking once on each window name.
2. Click on the **Special Button**, which looks like an asterisk in the lower right corner of the developer's desktop. A menu opens.
3. Select **Log Off** from the menu. The desktop closes and returns to the IBM Intelligent Decision Server Desktop window.
4. Double-click on the upper left corner of the IDS logon window. The window closes.

Initializing Additional File Server Volumes

The primary file server volume initializes when IDS is started for the first time. If you defined additional file server volumes, you need to initialize them with a different procedure:

1. If IDS is not running, start it by double clicking on the Start IDS Server icon inside the Intelligent Decision Server folder on the OS/2 desktop.
2. From the OS/2 Window List, select the fscnsl.exe OS/2 window. The window becomes visible.
3. At the User ID prompt, type system and press Enter.
4. At the SA=> prompt, type the following command:

   erase a2 /s:nnnn

   Where:

   A = the file server designation

   2 = the volume number designation

   Important: Do not use a1. That designation is reserved for the IDS system volume.

   nnnn = the percentage of file descriptors to allocateThen press Enter. A prompt opens, asking if you're sure you want to erase the disk.

   Any number of file descriptors between 40 to 75 is typical. For more information on file descriptors, see the *System Administration Guide and Reference* .
5. To initialize the file server volume, type y, then press Enter. If you do not want to initialize the file server volume at this time, type n.

   Erasing the file server volume will take only a few minutes. No other prompts or update messages display during this process. After the process completes, the following message displays:

   Slot A2: Offline
6. After the message from the previous step displays, activate the volume by typing the following command:

   online a2

   Then press Enter. The following message displays:

   Slot A2: Online.A2: done

   The file service volume is now initialized.

Chapter 4. Installing and Initializing an Auxiliary File Server

This chapter guides you through installing an Intelligent Decision Server (IDS) auxiliary file server. For the auxiliary file server to run, it must be connected to an IDS network and must be registered within that network.

The primary file server manages data for other IDS services in the same realm. With the auxiliary file server, you can create additional disk-storage space.

To set up an auxiliary file server, complete the following tasks:

1. Install the auxiliary file server, as described in "Installing an Auxiliary File Server."
2. Register the server as a node in the asset manager, as described in "Registering Workstations as Nodes" on page 37.
3. Add the auxiliary file service to the node through the Asset Manager, as described in "Adding the Auxiliary File Service" on page 46.
4. Initialize auxiliary file server volumes, as described in "Initializing Auxiliary File Server Volumes" on page 19

Installing an Auxiliary File Server

To install an auxiliary file server:

1. Load the IDS Installation CD into the CD-ROM drive on the target workstation.

   In the following instructions, F is used to represent the CD-ROM drive letter.
2. Open an OS/2 window.
3. From the F:\SERVER directory on the CD-ROM, type install then press Enter.

   The Instructions window opens.
4. Click on the **Continue** button. The Installation window opens.
5. Click on the **Update CONFIG.SYS** box to automatically update the CONFIG.SYS file.

   If you do not place a check in the box, you will need to update your CONFIG.SYS file manually. An updated file, called CONFIG.ADD, will be placed in the installation directory. Compare the changes in this file to your current CONFIG.SYS file.
6. Click **OK**. The Installation-Directories window opens.
7. Select the components you want to install from the list box, such as IDS Software and IDS Documentation.

   If you select only IDS Documentation, continue up to step 9. The books will install, but the IDS SmartGuide will not display to guide you through software installation.
8. In the Installation Directory box, type the path for the directory where you want the auxiliary file server installed. The default directory is C:\IDSSRV.
9. Verify that the target drive contains enough available disk space:

© Copyright IBM Corp. 1996

a. Click on the **Disk space** button. The Disk Space window opens. The available drives and available disk space displays.

   If the “Bytes needed” to install the selected components exceeds the “Bytes available,” specify a different drive with enough disk space from the Install-Directories window.

   Important: The "Bytes needed" to install the selected components includes only the minimum space required for IDS; the space needed for file service volumes is not included. For recommendations on disk space requirements, see “Hardware and Software Requirements” on page 7.

b. Click **OK** to return to the Install-Directories window.

10. Click on the **Install** button. The Install-Progress window opens.

    As files install on your server, the progress bar updates. During this process, you can click on the **Help** button to display online help, or click on the **Stop** button to cancel installation.

    When the progress bar indicates the installation is approximately half done, the IDS Services Installation SmartGuide opens the Welcome page. On any page in the SmartGuide, you can click on:

    <<**Back** to display and change previous pages (except on the first page)

    Next>> to display the next SmartGuide page

    Stop to cancel installation

    Help to display online help for the SmartGuide page

11. From the Welcome page, click on the **Next>>** button. The File Service Type page opens.
12. Select the **Auxiliary File Server** button, then click on the **Next>>** button. The Realm Identifiers page opens.
13. In the **IDS realm number** field, type the realm number that was used for the primary file server.

    The IDS realm number uses the realm number that was assigned to the primary file server. For more information on the values specified for the primary file server, see “Installing the Primary Server” on page 11.

14. Click on the **Next>>** button. The Allocate File Server Volumes page opens.
15. Define from one to three file server volumes:

    a. Select a volume number.

       Each volume number can be used only once, and only one volume can be assigned per hard disk partition. Up to three volumes can be defined.

       If enough disk space is not available to install a file service volume, the volume numbers cannot be selected.

    b. In the **Drive** field, select a disk drive.

c. In the **Name** field, use the default name or type a different name for the file server volume.

Recommendation: Use the default name for the file server volume to simplify installation and to make information tracking easier.

Repeat steps 14a through 14c to define additional file server volumes.

16. Click on the **Next>>** button. The File Server Volume Size page opens.
17. Specify the size for each file server volume you defined on the previous page:
    a. Select the number for the volume you want to size. The displayed drive letter and name automatically update for the volume you selected.
    b. Click and hold on the slider arm, then move it left or right to set the appropriate volume size. You can also use the ← and → buttons to set the slider arm.
18. Click on the **Next>>** button. The Select Desktop Option page opens.
19. Click on the **Start IDS desktop** box to start an IDS desktop session with the IDS services. If you do not want an IDS desktop on the auxiliary server, leave the box blank.

    Recommendation: Check the box to start a desktop with the services. Configuring the services using desktop tools is usually easier than using the command line.
20. Click on the **Done** button.

    The SmartGuide closes, and the Install-Progress window reopens and updates the status bar as files copy. When the installation successfully completes, an Installation and Maintenance window opens and displays the elapsed time.
21. Click on **OK**. The window clears. The installation is complete.

For instructions on stopping the installation, updating the file server, or deleting the server, see Chapter 3, “Installing and Initializing the Primary File Server” on page 11.

Initializing Auxiliary File Server Volumes

Before the auxiliary file server can be initialized, it must be registered as a node, and the auxiliary file service must be added to the node through the Asset Manager, as described in “Registering Workstations as Nodes” on page 37 and “Adding the Auxiliary File Service” on page 46.

To initialize an auxiliary file server volume:

1. If IDS is not running, start it by double clicking on the Start IDS Server icon inside the Intelligent Decision Server folder on the OS/2 desktop.
2. From the OS/2 Window List, select the fscnsl.exe OS/2 window. The window becomes visible.
3. At the User ID prompt, type system and press Enter.

4. At the Password prompt, type original and press Enter.
5. At the SA=> prompt, type the following command:

   erase b1 /s:nnnn

   Where :

   B = the file server designation

   1 = the volume number designation

   nnnn = the percentage of file descriptors to allocate

   Then press Enter. A prompt opens, asking if you're sure you want to erase the disk.

   Any number of file descriptors between 40 to 75 is typical. For more information on file descriptors, see the *System Administration Guide and Reference* .

   Important: The designation ("b1" in the preceding example) can change depending on the order in which the auxiliary file servers come on line. The status command in the file service interface lists all the available volumes, their names, and their status.
6. To initialize the file server volume, type y, then press Enter. If you do not want to initialize the file server volume at this time, type n.

   No other prompts or update messages display during this process. When the process completes, the following message displays:

   Slot B1: Offline
7. After the message from the previous step displays, activate the volume by typing the following command:

   online b1

   Then press Enter. The following message displays:

   Slot B1: Online.B1: done

The volume is now initialized. Repeat steps 5 through 7 for each additional volume you want to initialize.

Chapter 5. Installing Other IDS Services

This chapter guides you through installing the other available Intelligent Decision Server (IDS) services onto a workstation that will not be a file server.

Important: Do not perform the tasks in this chapter to install these services on a primary or auxiliary server; these services are automatically installed on the primary and auxiliary file server during installation.

The services installed during this procedure are:

Capsule

Conversion

Mail

ODAS

OS/2 database gateway

Print

Printer host

Remote mail gateway

After these services are installed, they must be added to the workstation, as described in Chapter 9, “Adding IDS Services to a Server or Node” on page 42.

To install the other IDS services on a workstation:

1. Load the IDS Installation CD into the CD-ROM drive on the target server.

   In the following instructions, F is used to represent the CD-ROM drive letter.
2. Open an OS/2 window.
3. From the F:\SERVER directory on the CD-ROM, type install then press Enter.

   The Instructions window opens.
4. Click on the **Continue** button. The Installation window opens.
5. Click on the **Update CONFIG.SYS** box to automatically update the CONFIG.SYS file.

   If you do not place a check in the box, you will need to update your CONFIG.SYS file manually. An updated file, called CONFIG.ADD, will be placed in the installation directory. Compare the changes in this file to your current CONFIG.SYS file.
6. Click **OK**. The Installation-Directories window opens.
7. Select the components you want to install from the list box, such as IDS Software and IDS Documentation.

   If you select only IDS Documentation, continue up to step 10. The books will install, but the IDS SmartGuide will not display to guide you through software installation.

© Copyright IBM Corp. 1996

8. In the Installation Directory box, type the path for the directory where you want the services installed. The default directory is C:\IDSSRV.
9. Verify that the target drive contains enough available disk space:
   a. Click on the **Disk space** button. The Disk Space window opens. The available drives and available disk space displays.

      If the “Bytes needed” to install the selected components exceeds the “Bytes available,” specify a different drive with enough disk space from the Install-Directories window.

      Important: The "Bytes needed" to install the selected components includes only the minimum space required for IDS; the space needed for file service volumes is not included. For recommendations on disk space requirements, see “Hardware and Software Requirements” on page 7.
   b. Click **OK** to return to the Install-Directories window.
10. Click on the **Install** button. The Install-Progress window opens.

    As files install on your server, the progress bar updates. During this process, you can click on the **Help** button to display online help, or click on the **Stop** button to cancel installation.

    When the progress bar indicates the installation is approximately half done, the IDS Services Installation SmartGuide opens the Welcome page. On any page in the SmartGuide, you can click on:

    <<**Back** to display and change previous pages (except on the first page)

    Next>> to display the next SmartGuide page

    Stop to cancel installation

    Help to display online help for the SmartGuide page
11. From the Welcome page, click on the **Next>>** button. The File Service Type page opens.
12. Select the **Other Services** button, then click on the **Next>>** button. The Realm Number page displays.
13. Type an appropriate value into the **IDS Realm Number** field.

    The IDS realm number is the realm number that was assigned to the primary file server. For more information on the values specified for the primary file server, see “Installing the Primary Server” on page 11.
14. Click on the **Next>>** button. The Select Desktop Option page opens.
15. Click on the **Start Developer's desktop** box to start a developer's desktop session with the IDS services. If you do not want a desktop on the auxiliary server, leave the box blank.

    Recommendation: Check the box to start a desktop with the services. Configuring the services using desktop tools is usually easier than using the command line.

16. Click on **Done**.

    Files begin copying to the workstation. When the installation successfully completes, an Installation and Maintenance window opens the elapsed time.

17. Click on **OK**.

The installation is complete, and the software to run the services has been installed on the workstation.

Before these services will function, the workstation must be registered as a node if it hasn't been already. For more information, see “Registering Workstations as Nodes” on page 37. And the services must be added to the workstation. For information, see Chapter 9, “Adding IDS Services to a Server or Node” on page 42.

Chapter 6. Installing the IDS Developer's Desktop

This chapter guides you through installing the Intelligent Decision Server (IDS) developer's desktop. The procedure for installing a developer's desktop is the same if the target workstation is local (directly connected to the network) or remote (accessing the network through remote connections).

Before you install the IDS developer's desktop, you must know the name of the primary file server that the desktop will access. The primary file server name, or realm name, is the TCP/IP host name. Ask your system administrator for this information.

The following tasks must be completed before the developer's desktop can be used:

1. Install the developer's desktop service as described in this chapter
2. Make sure the workstation has been registered as a node, as described in Chapter 8, “Configuring Nodes and Adding Users and Tools” on page 36
3. Ask your system administrator to create:

   A user ID for the person using the workstation

   An IDS network desktop for the user ID

The developer's desktop installation SmartGuide uses the same network information that was used to install the primary file server. If default values were used to install the primary file server, use the defaults provided by the desktop SmartGuide.

If the primary file server was installed with custom values, enter the same custom values into the fields.

Installing from the IDS CD-ROM

1. Load the IDS Installation CD into the CD-ROM drive on the target server.

   In the following instructions, F is used to represent the CD-ROM drive letter.
2. Open an OS/2 window.
3. From the F:\DESKTOP directory on the CD-ROM, type install then press Enter.

   The Instructions window opens.
4. Click on the **Continue** button. The Installation window opens.
5. Click **OK**. The Installation-Directories window opens.

   The **Update CONFIG.SYS** box is unavailable because the CONFIG.SYS file does not need to be updated when a desktop is installed.
6. Select the components you want to install from the list box, such as IDS Software and IDS Documentation.

   If you select only IDS Documentation, continue up to step 9. The books will install, but the IDS SmartGuide will not display to guide you through software instillation.

© Copyright IBM Corp. 1996

7. In the **Installation Directory** box, type the path for the directory where you want the developer's desktop installed. The default directory is C:\IDSDSK.
8. Verify that the target drive contains enough available disk space:
   a. Click on the **Disk space** button. The Disk Space window opens. The available drives and available disk space displays.

      If the “Bytes needed” to install the selected components exceeds the “Bytes available,” specify a different drive with enough disk space from the Install-Directories window.

      Important: The "Bytes needed" to install the selected components only includes the minimum space required for IDS; the space needed for file service volumes is not included. For recommendations on disk space requirements, see “Hardware and Software Requirements” on page 7.
   b. Click **OK** to return to the Install-Directories window.
9. Click on the **Install** button. The Developer's Desktop Installation SmartGuide displays the Welcome page.
10. Click on the **Next>>** button. The Server Name page displays.
11. Type the name of the primary file server into the **Primary server name** field.

    The primary file server name, or realm name, is the TCP/IP host name. Ask your system administrator for this information.
12. Click on the **Next>>** button. The Realm Number page displays with a default realm number.
13. Accept the value displayed in the **Realm number** field or specify a different value:

    If the primary file server was installed using default values, accept the realm number displayed in the field by clicking on the **Next>>** button.

    If the primary file server was installed with custom values, enter the same realm number used for the primary file server, then click on the **Next>>** button.

    For more information on the values specified for the primary file server, see “Installing the Primary Server” on page 11.

    The Subnet Mask page displays.
14. Accept the value displayed in the **Primary server subnet mask** field or specify a different value:

    If the primary file server was installed using default values, accept the subnet mask displayed in the field by clicking on the **Done** button.

    If the primary file server was installed with custom values, enter the same subnet mask used for the primary file server, then click on the **Done** button.

    Files copy to the workstation and the installation completes.

The Developer's Desktop folder appears on your OS/2 desktop. You do not need to reboot after installing the IDS developer's desktop.

Creating an Installation Diskette

The developer's desktop can be installed from the IDS CD-ROM or from an installation diskette.

To create an installation diskette:

1. Load the IDS Installation CD into the CD-ROM drive on the target workstation.

   In the following instructions, F is used to represent the CD-ROM drive letter.
2. Open an OS/2 window.
3. From the F:\DESKTOP\IMG directory on the CD-ROM, type `install` then press Enter.
4. Insert a blank double-sided, high density diskette into the diskette drive.
5. Run the LOADDSKF utility to create the installation disk by typing the following command:

   ```
   loaddskf idsdsk1.img a:
   ```

   Where A: represents your diskette drive.

   The necessary files are copied to your diskette. When the files finish copying, the diskette is ready for use.

To install the IDS developer's desktop from the diskette you just created:

1. Insert the installation diskette in the diskette drive of the target workstation.

   In these instructions, A is used to represent the diskette disk drive.
2. Open an OS/2 window.
3. From the command line, type:

   ```
   a:\install
   ```

   Then press Enter. The Instructions window displays.

   Continue the installation from step 4 in “Installing from the IDS CD-ROM” on page 24.

Starting the IDS Developer's Desktop

Before you can start the IDS Developer's Desktop for the first time, the primary file server specified during desktop installation must be running so that files can be downloaded. The workstation must be registered as a node, or you must also have an IDS user ID. For more information, see Chapter 9, “Adding IDS Services to a Server or Node” on page 42 and the *System Administration Guide and Reference* .

To start the desktop:

1. From the OS/2 desktop, double-click on the Developer's Desktop folder. The folder opens.

2. Double click on the Start IDS Desktop icon. Additional files from the server are copied to your workstation. This process can take several minutes.

   The IDS primary file server specified during desktop installation must be running for the desktop to start successfully.

3. Type your user ID into the field and press Enter.
4. Type you password into the field and press Enter. The developer's desktop opens.

Chapter 7. Installing and Configuring ODAS Components

The Open Data Access Service (ODAS) is automatically installed on a workstation with the primary file server, auxiliary file server, and other service installation options. To use ODAS, additional ODAS components must be installed and configured, as described in this chapter.

ODAS allows common applications, such as Lotus Notes, Web browsers, and ODBC applications, to access and run processes on the Intelligent Decision Server. You can also develop custom applications that use ODAS to access IDS. The ODAS components are:

- Open Data Access Service
- ODAS Administration application
- ODAS Client
- ODAS Test application

Before ODAS can be used, the following tasks must be completed as described in this chapter:

- Add and activate the service using the asset manager
- Install the ODAS Administration and Test Applications
- Configure the ODAS server
- Install the ODAS clients on workstations as needed in your environment
- Test the ODAS client connections

You can install the ODAS client on the following platforms:

- OS/2
- AIX
- WIN-OS/2 or Windows 3.1
- Windows 95
- Windows NT
- SUN

You can use the ODAS Administration and Test applications in Windows 3.1 or WIN-OS/2 environments to test the ODAS client connection. The test application is useful when developing custom applications for ODAS or configuring applications with the IDS Open Clients.

© Copyright IBM Corp. 1996

For information about administering ODAS, see the *System Administration Guide and Reference* . For information on installing IDS Open Clients, including those for the Web, Lotus Notes, and common ODBC applications, see *Installing and Configuring IDS Open Clients* . For information about developing custom applications, see *Developing Applications with Open Data Access Service* .

Adding ODAS

To add ODAS and register it with the asset manager:

1. In the Asset Manager list of registered IDS nodes, find the name of the node to which you want to add ODAS. Ensure that the network address in the list matches that of the actual node, then select that node.
2. Click on the **Show Details** button to display information about the node. The Asset Mgmt - Node Details window opens.
3. From the **Add Service** menu, select **Open Data Access Service**. The selected service is displayed in the **Add Service** field.
4. Click on the **Add Service** button. The Asset Mgmt - Service Details window opens.
5. In the **Service Name** field, type the name you want to assign to ODAS, such as Marketing ODAS.

   The name can include blank characters and punctuation, but must be no more than 63 characters long. Have a systematic naming scheme for your services, especially if you have more than one of the same kind of service.
6. In the **Locked Memory** field, leave the default value of 0.
7. In the **Service Status** field, leave the default setting of **Active**.

   If you want to register the service, but disable its use for the time being, select **Inactive**. The *System Administration Guide and Reference* discusses the Active and Inactive settings in more detail.
8. In the **Auto Start** field, leave the default Open Data status of **On** if you want the service to start automatically when the service is registered and whenever the server is booted; otherwise, change the status to **Off**.
9. In the **Auto Restart** field, change the status to **On** if you want the service to restart automatically whenever the server has stopped for any reason (including intentional shutdowns). Otherwise, leave it at its default value of **Off**.
10. In the **Number of Licenses** field, leave the default as it is.
11. In the window header, click on the **Register Service Information** button. The Asset Management window expands to show the session name for ODAS.
12. In the **Session Type** column, select **ODAS Sessions**.
13. Click on the **Show Details** button from the expanded portion of the window. The Asset Mgmt - Type Details window opens.
14. In the Asset Mgmt - Session Type Details window, type the maximum number of simultaneous user-access sessions you want.

You can assign the ODAS asset to any number of servers, but you are limited in the number of ODAS sessions that can be assigned to those servers.

15. In the window header, click on the arrow button.
16. Select **Register Session Information** from the menu.
17. Close the Asset Mgmt - Session Type Details window. In the expanded portion of the Asset Mgmt - Service Details window, the number of sessions has changed to the number of sessions you specified.
18. Close the Asset Mgmt - Service Details window. The Asset Mgmt - Node Details window reopens. ODAS appears as an asset, enabling use of the service on that node.

Installing ODAS Administration and Client Test Applications

To monitor and control activity on your ODAS server you must install the ODAS Administration application. The ODAS Client Test application is installed when you install the ODAS Administration application. You can install the Client Test Application without installing the ODAS Administration application. An ODAS Error Codes object is provided with these applications.

To install the ODAS Administration and Test Applications:

1. Insert the installation CD in the workstation CD-ROM drive.
2. From the Windows Program Manager window, choose **Run** from the **File** menu.
3. Type

   x:\odasclnt\win16\setup

   where *x* is the letter of the CD-ROM drive.
4. Following the instructions in the windows to complete the installation.

Starting ODAS

To start ODAS, open the IBM program-group icon, and double-click on the Open Data Access Service icon.

Logging On to the ODAS Administration Application

To log on to and start the ODAS Administration application on an ODAS client or server:

1. If you are logging on from an OS/2 server, start WIN-OS2 from the OS/2 desktop.

   If you are using a Windows client, start Windows.
2. From the Program Manager window, double-click on the IBM icon.

   The IBM program-group window opens.

3. From the IBM program-group window, double-click on the Open Data Access Administration icon.

   The Open Data Access Administration interface window opens.

4. Click on the **OK** button to continue.

   The Open Data Access Administration logon window opens.

5. At the **Server** field, type the name of the ODAS server you want to administer.

   The server name is the name by which the server is known on the TCP/IP network. If the server you want to administer is configured as part of a service pool, specify the name of the pool's primary server.

6. In the **Desktop** field, type your desktop name or the name of a desktop that has administrative privileges on the server you want to administer.

   Until a server is configured otherwise, the system desktop is the only desktop that has administrative privileges.

7. At the **Password** field, type the password for the desktop you specified.

8. Click on the **Logon** button to start the session.

   The application connects to the specified service, logs on to the specified desktop, and enables administrative privileges on the server.

   If an error occurs during this process, an error message appears.

From the Pool Status window, you can perform the administration functions of ODAS described in “Resizing Columns” on page 32 and “Configuring the ODAS Server” on page 32. For reference information on using the ODAS administrator, see the *System Administration Guide and Reference* .

Administration Interface

The administration interface is provided by the ODAS Administration application. This application enables you to configure and monitor one or more ODAS servers. It can be installed on any ODAS client and used to remotely administer ODAS servers on the network, or it can be installed on a server and used to administer the local service.

The Administration application permits you to log on to ODAS, which can consist of one or more ODAS servers, to perform the following tasks:

Display service status

Display active sessions

Display a history of service activity

Configure the service

Each server is administered separately, but the administrator can easily move between servers in the service pool.

Resizing Columns

Most of the windows within the Administration application contain columns of text that can be resized. In some cases, the text might be truncated.

To resize the columns:

1. Place your cursor on the first character of the column name. The cursor should change to a double-ended arrow.
2. When that arrow appears, click and hold down mouse button one until you see a vertical line on the left side of the selected column.
3. While you are still holding down the mouse button, resize the column to the width you desire. Then release the mouse button.

Configuring the ODAS Server

After ODAS starts, you can configure the server to access other servers so you can retrieve, manipulate, and send information between those servers and your IDS desktop. Specifically, you must configure the:

ODAS primary server

Capsule server to which you want to connect

Conversion server to which you want to connect

Configuration is done in the Server Configuration window of the Open Data administration application.

To configure the ODAS Server:

1. Log on to the administration application and open the Pool Status window.
2. Select the server you want to configure from the list of servers in the pool.
3. Click on the **Configure** button. The Server Configuration window opens.
4. In the Pooling Mode area of the window, specify whether you are configuring a primary server or a secondary server.

   A primary ODAS server manages session assignments for all other services in the service pool. All ODAS clients specify the name of the primary ODAS server to which they connect.

   If this is the only server in the service pool, or if it will be the primary ODAS server, select **Primary**. Primary appears in the **Name** field within the Pool Primary Server area of the window.

   If the server is part of a pool that already has a primary server, select **Secondary**. You must enter a name in the **Name** field within the **Pool Primary Server** area, or an error message appears when you try to save your configuration parameters.
5. In the **Name** field within the Capsule Service area of the window, type the name of the capsule server to which you want to connect.

6. In the **Name** field within the Conversion Service area of the window, enter the name of the conversion server to which you want to connect.
7. In the **Sessions** field within the Conversion Service area of the window, type the number of conversion sessions (or concurrent conversion resources) you want to allocate to the ODAS server.
8. Click on the **Set** button to save the values.
9. Click on the **Close** button to close the Server Configuration window.

Installing ODAS Clients

When you install the IDS Lotus Notes Client, the IDS ODAS Client, or the IDS Web Client, the ODAS client is installed automatically. You need to perform the ODAS client installation, described in this section if you plan to develop custom applications.

To install the ODAS client on OS/2:

1. Insert the IDS Installation CD into the CD-ROM drive.
2. At an OS/2 command prompt, type:

   x:\odasclnt\os2\install.cmd

   where:

   x is the letter of the CD-ROM drive.
3. Follow the instructions presented to complete the installation.

To install the ODAS client on AIX:

1. Insert the IDS Installation CD into the CD-ROM drive.
2. At an OS/2 command prompt, navigate to the ODASCLNT\AIX directory.
3. At the command prompt, type:

   tar -xvf /cdrom/odasclnt/aix/odasclnt.tar

   where *cdrom* is the mount point of your CD-ROM drive. Then press Enter.

To install the ODAS client on a Solaris or Sun operating system:

1. Insert the IDS Installation CD into the CD-ROM drive.
2. At an OS/2 command prompt, navigate to the ODASCLNT\SUN directory.
3. At the command prompt, type:

   tar -xvf /cdrom/odasclnt/sun/odasclnt.tar

   where *cdrom* is the mount point of your CD-ROM drive. Then press Enter.

To install the ODAS client on a WIN-OS/2 or Windows 3.1 workstation:

1. Insert the IDS Installation CD into the CD-ROM drive.
2. At an OS/2 command prompt, type:

x:\odasclnt\win16\setup.exe

where:

x is the letter of the CD-ROM drive.

3. Follow the instructions presented to complete the installation.

   You will be prompted to install the ODBC Administration and Test applications as options.

To install the ODAS client on Windows 95:

1. Insert the IDS Installation CD in the CD-ROM drive.
2. From the Windows 95 **Start** menu, choose **Run**.
3. In the **Run Command** field type:

   x:\odasclnt\win32\setup.exe

   where:

   x is the letter of the CD-ROM drive.
4. Follow the presented instructions to complete the installation.

Testing the Connection to ODAS on Windows

You can test ODAS client connections running on WIN-OS/2 or Windows 3.1, including ODAS clients installed with the IDS Open Clients. To test your ODAS client, you can perform three tests: a connection test, a capsule submission test, and a file transfer test. The capsule you test with can be a generic test capsule, the Coffee or Banking samples provided on the guest desktop, or one that you have created on the IDS desktop.

To test the ODAS Client connection:

1. Locate and double-click on the Open Data Access Client Test icon. The Open Data Access Client Test Program window opens.
2. Type the name of the ODAS server to test in the **Open Data Access Server** field.
3. Type the name of the desktop to test in the **Desktop Name** field. You can use the guest desktop.
4. Type the desktop password in the **Password** field. The password for the guest desktop is guest.

To test a connection:

5. Click on **Start Testing**. The ODAS Test Status window opens.

   This window contains an **Action** field and a **Result** field where action refers to the test being performed and results refers to the test results.

   If the connection is working, the results of the connect and logon on test will be OK.

If an error occurs, an error code displays in the Submit Capsule failed window. To look up this error, click on **Help**.

6. Click **OK** to return to the ODAS Test Status window.

To test a capsule submission:

7. In the Open Data Access Client Test Program window, select **Submit one from scratch** to submit the supplied Test capsule. Or select **Submit one from the desktop** to test the connection with a capsule application that you have created.

   If you choose to use a capsule you have created, you will be prompted to enter the path of the capsule icon. To use the Coffee Sample test capsule, for example, type:

   \Sample Applications\Coffee Demo\Causals w/ Graph

   Important: The capsule path prompt is case sensitive.

8. Click on **Start Testing**. The ODAS Test Status window opens.

   If the capsule submission is successful, the Submit Capsule field results will be OK.

   If an error occurs, an error code displays in the Submit Capsule failed window. To look up this error, click on **Help**.

9. Click **OK** to return to the ODAS Test Status window.

To test a file transfer:

10. In the Open Data Access Test Program window, select **Transfer the capsule run log** to transfer the run log from a capsule you ran in the previous steps, or select **Transfer a file from the desktop** to transfer an arbitrary file.

    If you choose to transfer a file, you will be prompted for the file path name. Use the backslash (\) to specify file drawers and folders.

    Both options will place the file in your Windows/System directory with the file name test.txt.

Chapter 8. Configuring Nodes and Adding Users and Tools

Your IDS system has a primary file service, one or more developer's desktops, and perhaps an auxiliary file server. Before users or desktops can access services and tools, they must be registered and assigned assets.

Planning

Before you begin, be sure you have the following information available for reference:

The IDS network number and realm number

Names of all of your services and desktops

If you are using TCP/IP addresses and protocol, the token-ring or Ethernet addresses of workstations in your IDS network.

Your asset changes are stored in the asset manager's memory and become effective as soon as you apply or enable them. In most cases, however, the changes are not saved until you close the asset management interface, except for changing the interface password, which is immediately written to the configuration disk.

Opening the SA Tool

All tasks in this chapter are performed with the SA Tool.

To open the SA Tool:

1. If you are not logged on to IDS, do so now.
2. From the developer's desktop, double click on the System icon. The System window opens.
3. Double click on the File Drawers icon. The File Drawers window opens.
4. Click on the Administrator Icons icon. The Administrator Icons window opens.
5. Click on the SA Tool icon. The SA Tool opens, as shown in Figure 2 on page 37.

© Copyright IBM Corp. 1996

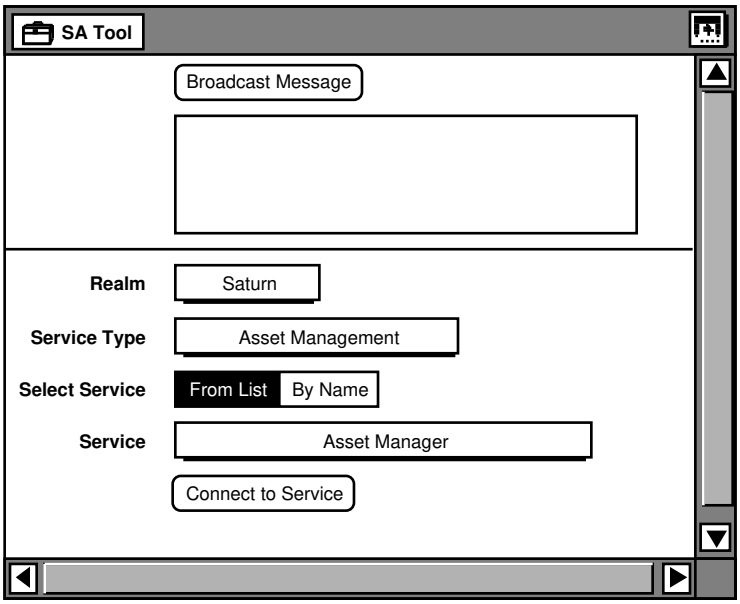


Figure 2. SA Tool Window

Registering Workstations as Nodes

Assets and tools, such as mail, database gateway, and capsule service, can be registered to nodes or users. If tools are registered to users, you don't need to register the user's workstation as a node. However, if you have unregistered users who need to access the IDS system, you can assign tools to the workstation. But before you can assign tools to a workstation, the workstation must be registered as a node. For more information on assigning tools to nodes or users, see “Adding Users and Tools” on page 39.

To register a workstation as an IDS node:

1. Choose **Asset Management** from the **Service Type** field in the SA Tool window, as shown in Figure 2. The Asset Manager window opens.

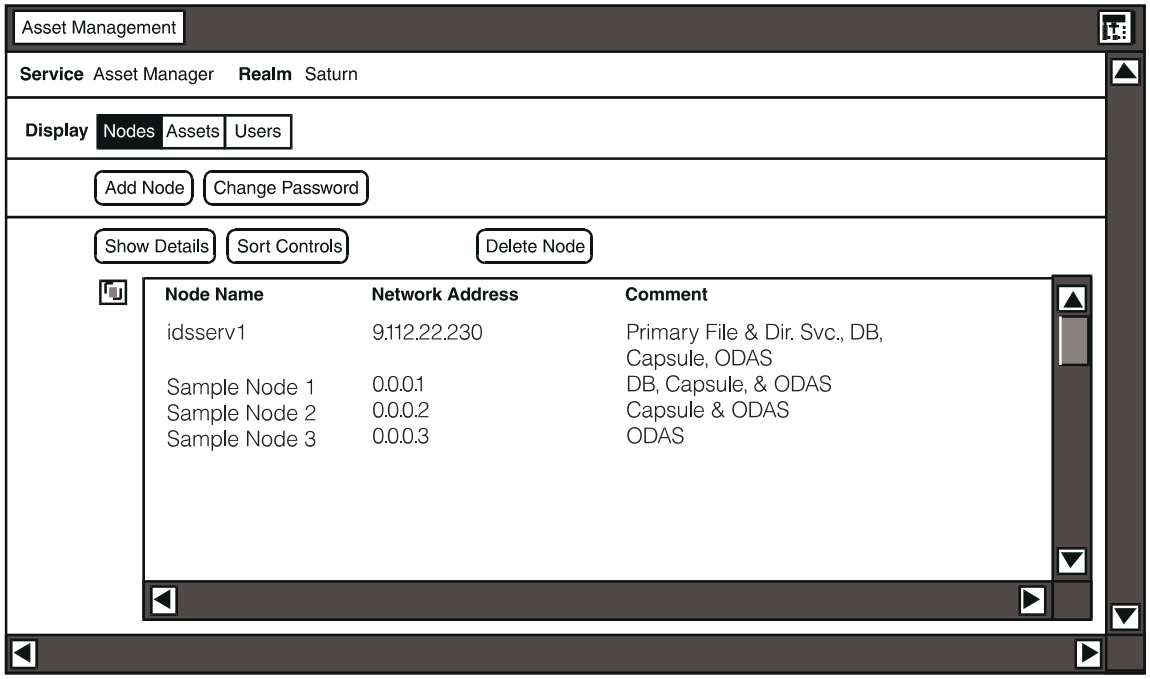


Figure 3. Asset Management Window, displaying Nodes

2. From the **Display** field, click on the **Nodes** button. Node information displays. The primary file server and any sample nodes display in the nodes list.
3. If the IDS node you want to register is not in the list, click on the **Add Node** button. The Node Details display.
4. In the Network Address field, enter the TCP/IP address for the node, such as 123.234.56.78.
5. In the **Node Name** field, enter a unique name to be associated with the workstation. You should have a systematic naming scheme for all of your nodes, based on the user's name, the location, or some other key.
6. In the **Comment (optional)** field, enter any text that will help you further identify the person or group to whom the workstation belongs. The comment must be no more than 63 characters long.
7. If you want to register the node, but keep it unusable until some future time, click on the **Inactive** button. In general, leave this setting as active. The *System Administration Guide and Reference* discusses active and inactive states in more detail.
8. Click on the **Register Node Information** button.

   The node is registered and can be seen in the node list from the Asset Management window.
9. Close the Node Details window and return to the Assent Management window.

Adding Users and Tools

Assets are licensed tools or sets of tools that can be assigned to a specific *node* or to a user ID. A node is a workstation registered in the IDS network to the asset manager, and can have tools assigned to it. Where you assign tools depends on how the IDS system is used. If tools are assigned to a user ID, the user can use the tools on any node in the IDS realm. If you assign tools to a node, anyone can use those tools on that node.

When a *registered user* uses a registered node (both the user and node have tools assigned to them), the user's ID controls which tools are usable; the node's tools are ignored. A registered user has a user ID and a desktop name registered in the Asset Manager's user list.

If someone uses a workstation that is not registered, the person must be a registered user to access the IDS system. For example, you might assign the SA tool and Administrator tools to your user ID so you can access these system administration assets from any workstation. Alternatively, if several people share a workstation, you might register that workstation as a node and assign the appropriate tools to the node, rather than to individual user IDs.

Registering User IDs

A user ID must be registered before assets can be assigned to it. A desktop and user ID can be used for:

A user

An administrative position, such as system administrator or database administrator

A group of users

To register a user ID:

1. In the Asset Management window of the SA tool, click on **Users**.
2. Click on **Add User**. The User Details window opens.
3. In the **User ID** field, type the new user logon ID. The ID can be up to 63 characters long.

   You must also create a desktop for the user with the same name as the user ID. For more information see the *System Administration Guide and Reference* .
4. In the **Comment (optional)** field, type any text that identifies the ID owner—a full name, job title, or group description such as a department name.

   The comment can be up to 63 characters long.
5. To register the user ID but make it unusable, click on **Inactive**.

   For example, you might create an ID for a new employee but not activate the ID until an appropriate time. The *System Administration Guide and Reference* discusses the active and inactive options in more detail.

6. Click on **Register User Information**, in the window header. The user ID and information is registered.

   You must click on **Register User Information**. If you just close the window, nothing is registered.

7. Close the User Details window by clicking on the window name. The new user ID is now listed in the Asset Management window.
8. Make sure a desktop exists with the same name as the newly added user ID.

Assigning Tools to a Registered Node

To add a tool or tool set to a registered node:

1. From the Asset Management window, click on **Nodes**.
2. Select the node you want to assign tools to.
3. Click on the **Show Details** button. The Node Details window opens.
4. Click on the button next to the **Add Tool** button to display the menu.
5. Select the tool or tool set you want to assign to the selected node.
6. Click on the **Add Tool** button. The tool or tool set you selected is now in the list of assigned assets.

To assign another tool or tool set to the same node, repeat steps 4 to 6.

Assigning Tools to a User ID

To add a tool or tool set to a user ID:

1. From the Asset Management window, click on **Users** button. The Asset Mgmt-User Details window opens.

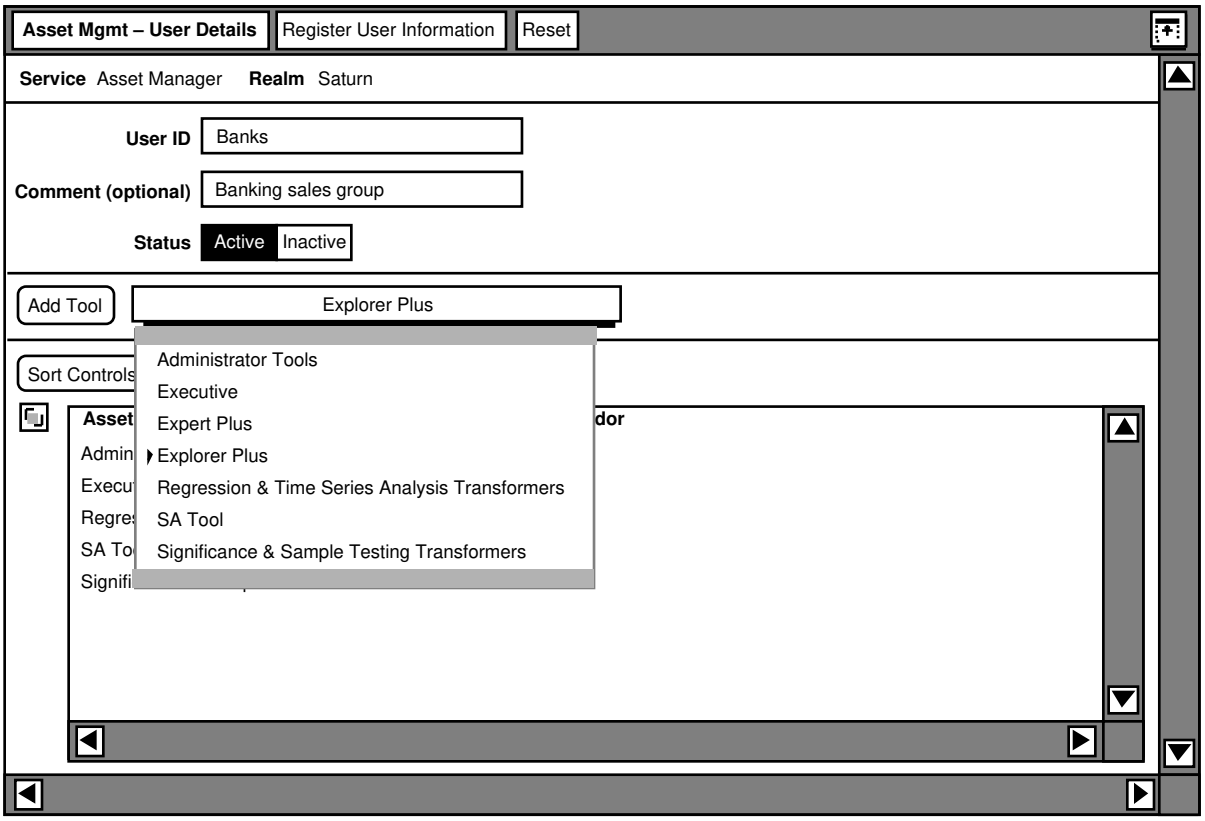


Figure 4. User Details window

2. Select the user ID you want to assign tools to.
3. Click on **Show Details**. The user details display.
4. Click on the button next to the **Add Tool** button to display the menu, as shown in Figure 4.

   Select the tool or tool set you want to assign to the selected user ID.
5. Click on the **Add Tool** button. The tool or tool set you selected is now in the list of assigned assets.

To assign another tool or tool set to the same node or user ID, repeat steps 4 to 5.

Chapter 9. Adding IDS Services to a Server or Node

This chapter guides you through adding Intelligent Decision Server (IDS) services, such as the mail service or capsule service, to a server or node. These services are automatically installed during primary file service and auxiliary file service installation or are installed on a workstation as described in Chapter 5, “Installing Other IDS Services” on page 21. Before services can be used, they must be added or activated in the asset manager as explained in this chapter. Some services also require additional configuration steps.

Opening the Asset Manager

All services are added through the Asset Manager Nodes Details window. If you do not have the Asset Manager Node Details window open:

1. Open the SA Tool as described in “Opening the SA Tool” on page 36 if it is not already open.
2. From the **Service Type** menu, select **Asset Management**.
3. Click on the **Connect to Service** button. The Asset Management password window opens.
4. Type your password into the field and press Enter. The Asset Management window opens.
5. From the Node list, select the node you want to work with.
6. Click on the **Show Details** button. The Nodes Detail window opens.
7. Continue with the section in this chapter that describes adding the appropriate service.

Adding the Mail Service

The mail service sends and receives mail between any realms that are connected to an IDS network or to a mail gateway for distribution to another network.

This service requires the presence on the realm of the primary file, asset management, directory, and desktop services to start up successfully.

To enhance performance, the mail service and the post office should reside on the same node. Whenever the location of the mail post office is changed, the mail service automatically stops. If this happens, copy any remaining mail folder from the old post office to the new location and restart the mail service. For an overall description of the entire IDS mail system, see the *System Administration Guide and Reference* .

To add a mail service to a registered node:

1. Pull down the menu next to the **Add Service** button, as shown in Figure 5 on page 43.

© Copyright IBM Corp. 1996

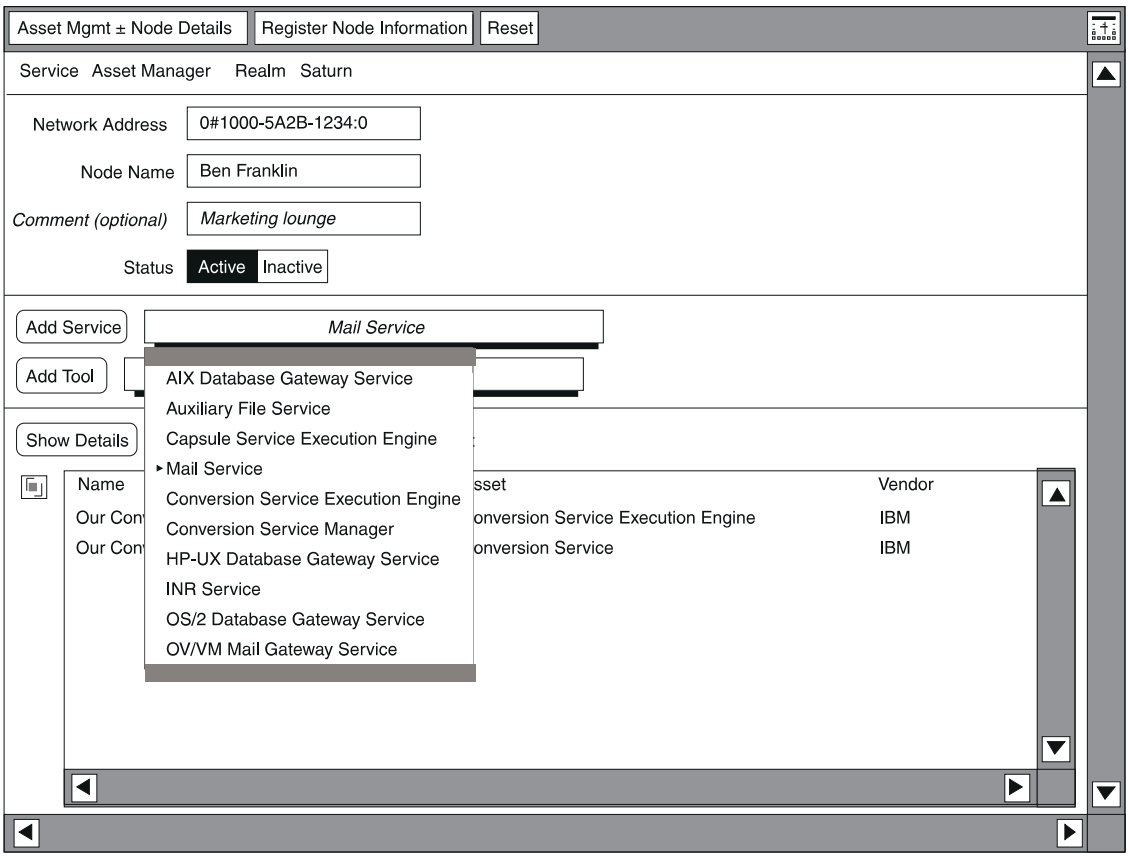


Figure 5. Add Service menu

2. Choose **Mail Service** from the menu.
3. Click on the **Add Service** button. The Service Details window opens, as shown in Figure 6 on page 44.

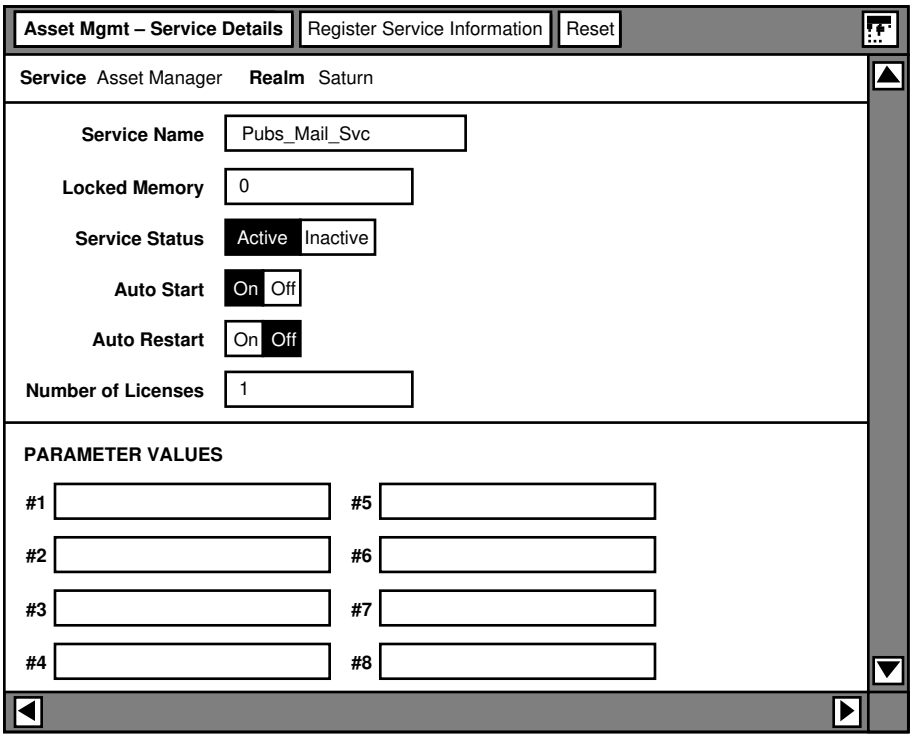


Figure 6. Service Details Window

4. In the **Service Name** field, type the unique name you want to assign to the new service, such as Pubs_Mail_Svc.

   The name can include blank characters, apostrophes, and other punctuation, but must be no more than 63 characters.

   You should have a systematic naming scheme for your services, especially if you have more than one of the same kind of service. For example, you might name two auxiliary file services Marketing MS and Sales MS.

5. In most situations, leave 0 as the default value in the **Locked Memory** field.
6. If you want to register the service but keep it unusable until some future time, click on **Inactive**. Usually, though, you should leave this setting in its active default. The *System Administration Guide and Reference* discusses active and inactive states in more detail.
7. If you want the service to start automatically after it's registered and when the server is booted, leave **Auto Start** field at its default value of **On**; otherwise, choose **Off**.
8. If you want the service to restart automatically whenever it has stopped, choose **On** in the **Auto Restart** field; otherwise, leave the **Auto Restart** field its default of **Off**.

9. Leave the **Number of Licenses** field as it is.
10. Click on the **Register Service Information** button in the window header.

You have now successfully added the mail service.

Configuring the Mail Service

The mail service requires configuration before it can be used. Your tasks include configuring the Post Office location and the lifetime for undeliverable mail.

Using the Mail Interface

After the mail service has been assigned to a node, it will start. However, before it can be used, you must set a few simple configuration parameters through the SA Tool's mail console. When you create a mail service, you must set a few simple configuration parameters through the SA Tool's mail console.

To use the mail console:

1. Open the SA Tool and connect to the mail console.
2. Click on **Set Configuration**. The Configuration window opens.
3. Consult the following sections to decide what information you want to enter.
4. Enter the required information or accept the default values, as shown in Figure 7.

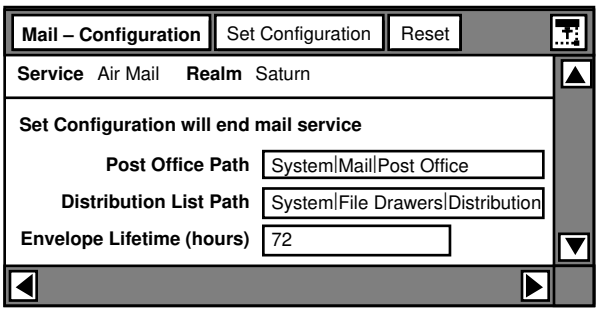


Figure 7. Configuration window

5. Click on **Set Configuration**. The mail service registers the new information and then stops.

   You must click on **Set Configuration** to make the changes effective. If you just close the window, nothing is done.

   An Important Message dialog box opens that reads:

   Mail
   Service is disconnected. Please restart the service.

6. Use the Node-Management console to restart the mail service with the new configuration. Connect the Node Management console of the node to which the mail service is assigned. Select Mail Gateway service, then click on the **Start Service** button.

Setting the Envelope Lifetime

If incoming mail is undeliverable, the mail service holds it in a Delay folder and periodically retries delivery. After a time limit, however, IDS returns the mail to the sender with a message saying that it was unable to deliver the Envelope.

Similarly, if the mail service cannot send outgoing mail to its destination realm or network, a Retry folder holds the mail, and the service retries delivery, until the time limit expires.

The default time limit for both cases is 72 hours. To set this time limit to a different value, type the desired number of hours in the **Envelope Lifetime (hours)** field of the Configuration window and click on **Set Configuration**.

Setting the Post Office Path

You can establish your release 2 Post Office anywhere you like; the default location is System|Mail.

To set the location of the Post Office:

1. If the new Post Office location is to be in a new folder or file drawer, create that folder or file drawer. You do not have to create the Post Office itself.
2. In the Configuration window, type the new path in the Post Office **Path** field. Separate the container names with a vertical bar (|). For example, the default path, as shown in Figure 7 on page 45, says the System disk contains the Mail file drawer, which contains the Post Office folder.
3. Click on **Set Configuration**.

Later, if you want to move the Post Office, follow this same procedure and then open the folders under the old Post Office folder and copy all the mail into the corresponding folders in the new Post Office folder. Opening these folders might require that you log on to the system desktop first.

Important: The new site cannot be System|Post Office; that is a reserved file drawer.

Adding the Auxiliary File Service

Before an auxiliary file service can be used or initialized, the service must be added to the node. To add an auxiliary file service:

1. Pull down the menu next to the **Add Service** button and select **Auxiliary File Service**.
2. Click on the **Add Service** button. The Service Detail window opens.
3. In the **Service Name** field, type the unique name you want to assign to the new service, such as Pubs_Aux_File_Svc. The name can include blank characters, apostrophes, and other punctuation, but must not be longer than 63 characters.
4. In most situations, leave the default in the **Locked Memory** field as it is.

5. If you want to register the service but keep it unusable until some future time, click on **Inactive**. Usually, though, you should leave this setting in its **Active** default. The *System Administration Guide and Reference* discusses active and inactive settings in more detail.
6. If you want the service to start automatically as soon as it is registered and whenever the server is booted, leave **Auto Start** at its default value, **On**; otherwise, click **Off**.
7. If you want the service to restart automatically whenever it has stopped for nearly any reason, click the **On** setting in **Auto Restart**; otherwise, leave it at its default value, **Off**.
8. Leave the **Number of Licenses** field as it is.
9. Click on the **Register Service Information** button in the window header.

You have now successfully added this service.

Adding the Print Service

The print service formats IDS documents and either submits them to the printer host queue for printing or to a specified recipient via electronic mail. Print formatting is performed by the print server, and the actual printing is done through the printer host.

This service requires the presence on the realm of the primary file, asset management, and directory services to start up successfully. Additionally, the printer host must be in operation before documents can be printed.

Adding a print service to a registered node consists of adding a print service manager and a print service execution engine.

Adding the Print Service Manager

1. Pull down the menu next to the **Add Service** button, as shown in Figure 8 on page 48. If no licenses are available for you to assign, the service does not appear in the menu. You might have to scroll the window to see the entire list.
2. Select **Print Service Manager**. After you select a service, it displays in the **Add Service** field, as show in Figure 8 on page 48.

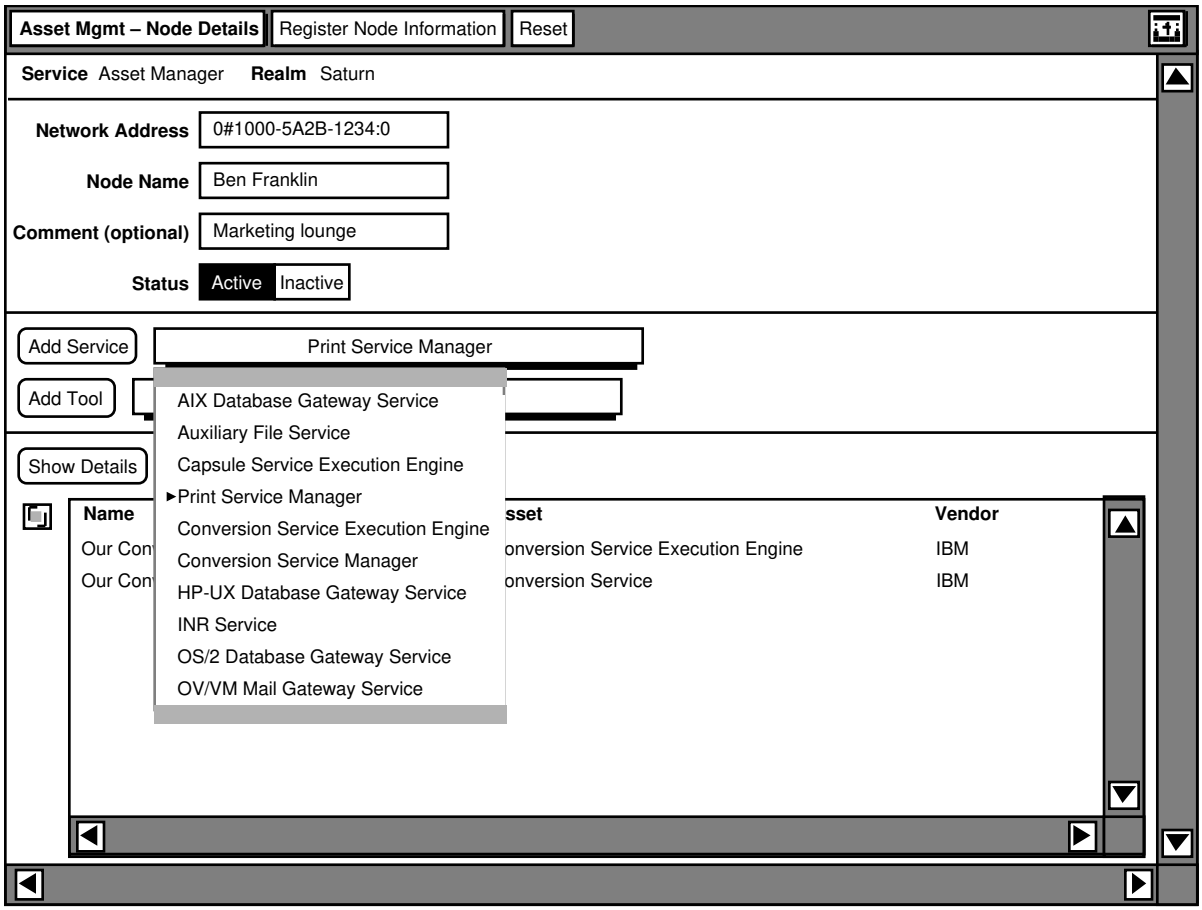


Figure 8. Add Service menu for print service manager

3. Click on the **Add Service** button. The Service Details window opens.
4. In the **Service Name** field, type the unique name you want to assign to the new service, such as Pubs_Print_Svc_Mgr. The name can include blank characters, apostrophes, and other punctuation, but must not be longer than 63 characters.

   As with the nodes, you should have a systematic naming scheme for your services, especially if you have more than one of the same kind of service. For example, you might name two print service managers Marketing PSM and Sales PSM.
5. In most situations, leave 0 as the default in the **Locked Memory** field.
6. If you want to register the service but keep it unusable until some future time, click on **Inactive**. Usually, though, you should leave this setting in its **Active** default. The *System Administration Guide and Reference* discusses active and inactive settings in more detail.

7. If you want the service to start automatically as soon as it is registered and whenever the server is booted, leave **Auto Start** at its default value, **On**; otherwise, click **Off**.
8. If you want the service to restart automatically whenever it has stopped for nearly any reason, click the **On** setting in **Auto Restart**; otherwise, leave it at its default value, **Off**.
9. In the **Number of Licenses** field, type the number of copies of this service you want to run on this computer. In most instances, this is 1. The minimum for any service is 1; the maximum is governed by the amount of memory and processing speed available in the computer.
10. In the **PARAMETER VALUES** field, type a DOS file name for the service's internal database (which IDS will create automatically) in the parameter **#1** field, such as PrintDB. This file name must be 1 to 8 alphanumeric characters. It is often convenient to use the service name, or an abbreviation of it, for this parameter.
11. If you leave the **#5** field blank, the default is for the service to use System|File Drawers|DXS as its working space. For the printing service, this can cause congestion on the primary file server. To avoid this congestion, specify space on some other disk, such as Aux2|File Drawers|DXS. Notice that vertical bars (|) separate the elements of the path.
12. Click on the **Register Service Information** button in the window header to add the print service manager.

You have now successfully added half of this service.

Adding the Print Service Execution Engine

1. Pull down the menu next to the **Add Service** button, as shown in Figure 9 on page 50. If no licenses are available for you to assign, the service does not appear in the menu. You might have to scroll the window to see the entire list.
2. Choose **Print Service Execution Engine**.

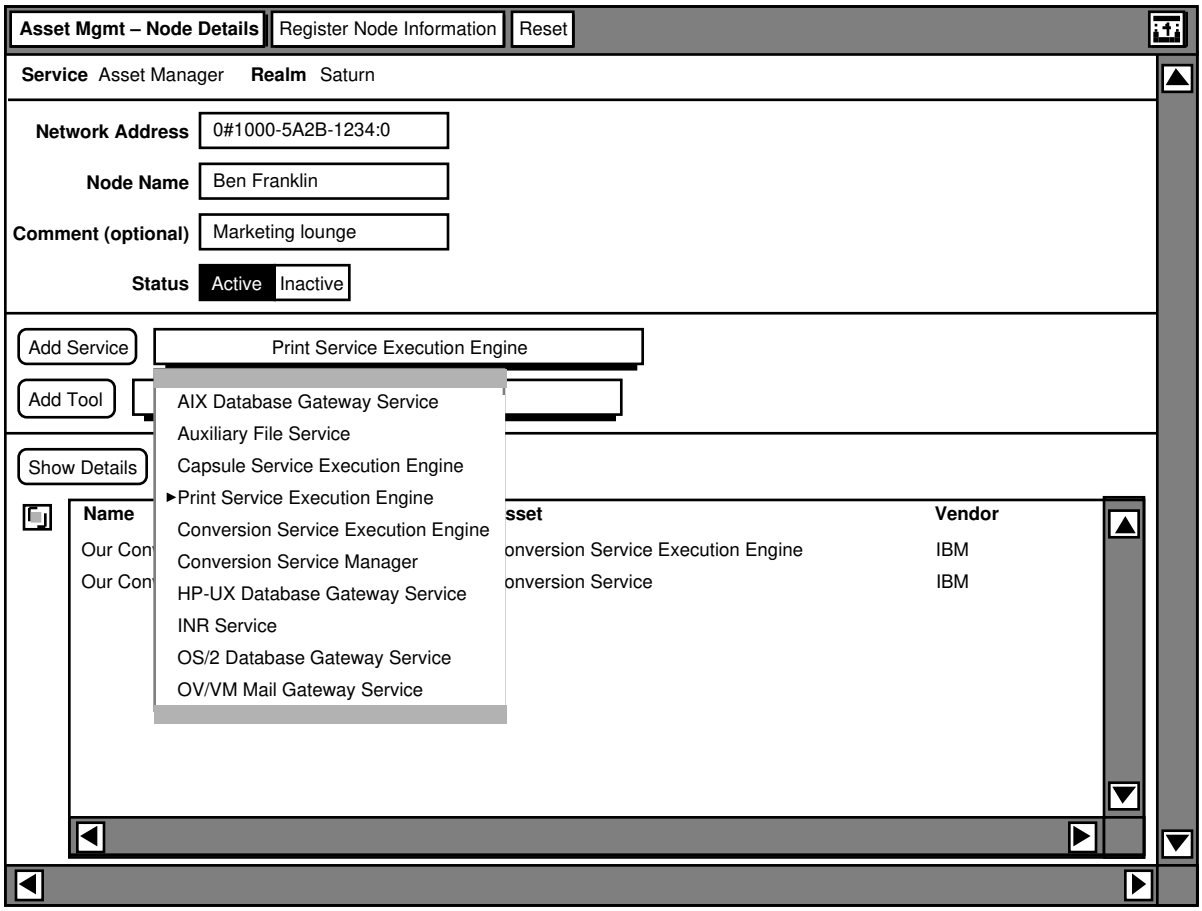


Figure 9. Add Service menu

3. Click on the **Add Service** button. The Service Details window opens.
4. In the **Service Name** field, type the unique name you want to assign to the new service, such as Pubs_Prnt_EE. The name can include blank characters, apostrophes, and other punctuation, but must be no more than 63 characters long.

   As with the nodes, you should have a systematic naming scheme for your services, especially if you have more than one of the same kind of service; for example, you might name two print service execution engines Marketing PSEE and Sales PSEE.
5. In most situations, leave 0 as the default in the **Locked Memory** field.
6. If you want to register the service but keep it unusable until some future time, click on **Inactive**. Usually, though, you should leave this setting in its **Active** default. The *System Administration Guide and Reference* discusses **Active** and **Inactive** settings in more detail.

7. If you want the service to start automatically as soon as it is registered and whenever the server is booted, leave **Auto Start** at its default value, **On**; otherwise, click **Off**.
8. If you want the service to restart automatically whenever it has stopped for nearly any reason, click the **On** setting in **Auto Restart**; otherwise, leave it at its default value, **Off**.
9. In the **Number of Licenses** field, type the number of copies of this service you want to run on this computer. For execution engines, the number is usually between 2 and 10. The minimum for any service is 1; the maximum is governed by the amount of memory and processing speed available in the computer.
10. In field **#5**, specify the name of the corresponding service manager. For example, if your print-service manager is named Pubs_Prnt_Svc_Mgr, then field **#5** must be assigned that name also.
11. Click on the **Register Service Information** button in the window header.

You have now successfully added the remainder of the service.

Adding the Printer Host

If the OS/2 spool directory (the area where OS/2 places the print jobs awaiting the printer's availability) is filled to its capacity, print jobs are disregarded from the OS/2 spool queue and are not printed. You can avoid this problem by ensuring that you have configured enough memory for the OS/2 queue.

To add a printer host to a registered node:

1. Pull down the menu next to the **Add Service** button, as shown in Figure 10 on page 52. If no licenses are available for you to assign, the service does not appear in the menu. You might have to scroll the window to see the entire list.
2. Choose **Printer Host** from the menu. After you choose a service, it displays in the **Add Service** field, as shown in Figure 10 on page 52.

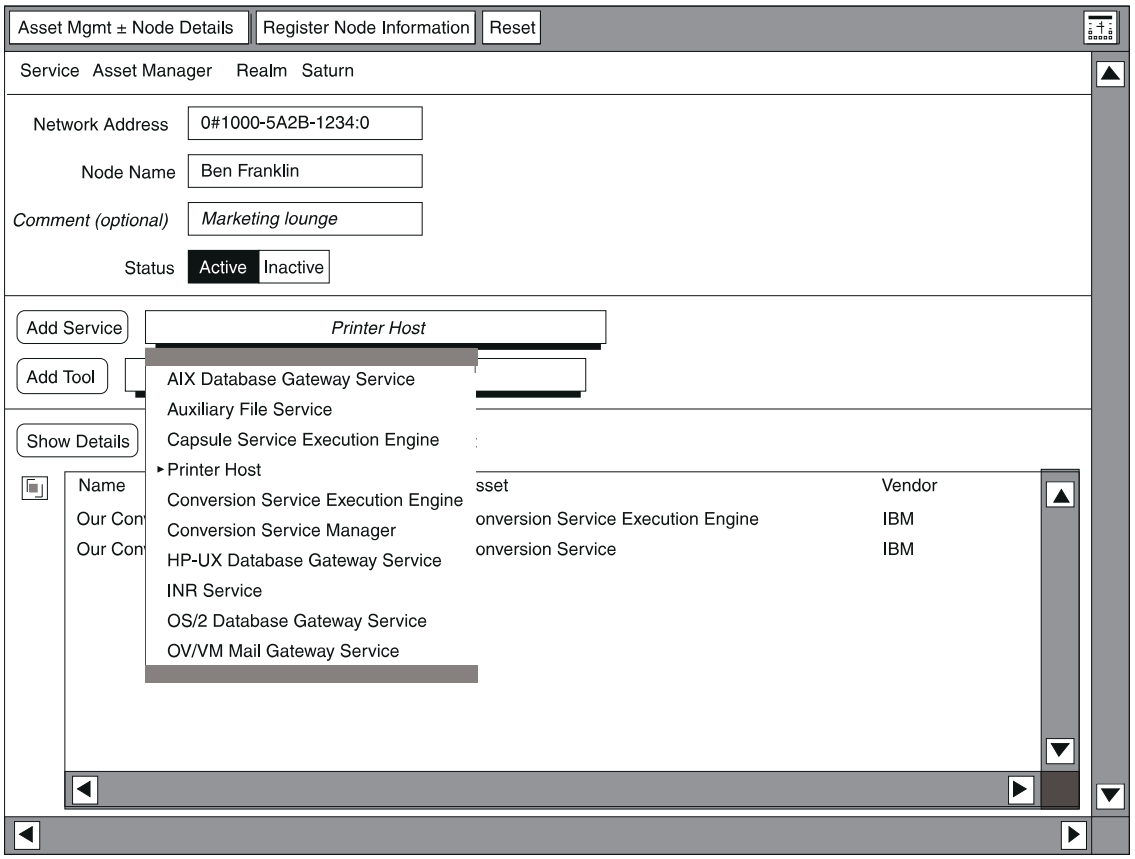


Figure 10. Add Service menu

3. Click on the **Add Service** button. The Service Details window opens.
4. In the **Service Name** field, type the unique name you want to assign to the new service, such as Pubs_Ptr_Host. The name can include blank characters, apostrophes, and other punctuation, but must be no more than 63 characters long.

   As with the nodes, you should have a systematic naming scheme for your services, especially if you have more than one of the same kind of service; for example, you might name two auxiliary file services Marketing PH and Sales PH.
5. In most situations, leave 0 as the default in the **Locked Memory** field.
6. If you want to register the service but keep it unusable until some future time, click on **Inactive**. Usually, though, you should leave this setting in its **Active** default. The *System Administration Guide and Reference* discusses **Active** and **Inactive** settings in more detail.
7. If you want the service to start automatically as soon as the service is registered and whenever the server is booted, leave **Auto Start** at its default value, **On**; otherwise, click **Off**.

8. If you want the service to restart automatically whenever the server has stopped for nearly any reason, click the **On** setting in **Auto Restart**; otherwise, leave it at its default value, **Off**.
9. Leave the **Number of Licenses** field as it is.
10. Leave the **PARAMETER VALUES** field blank.
11. Click on the **Register Service Information** button in the window header to add the printer host.

You have now successfully added this service.

Adding the Capsule Service

The capsule service allows concurrent capsule executions from a single developer's desktop to multiple remote desktop users. This service can be configured to utilize a single computer or to utilize multiple computers for increased capsule execution capacity.

To start up successfully, this service requires the presence on the realm of the primary file, asset management, and directory services. Additionally, the object conversion service must also be installed and working before capsules can be executed.

Adding a capsule service to a registered node consists of adding a capsule service manager and a capsule service execution engine.

Adding the Capsule Service Manager

1. Pull down the menu next to the **Add Service** button. If no licenses are available for you to assign, the service does not appear in the menu. You might have to scroll the window to see the entire list.
2. Choose **Capsule Service Manager** from the menu. After you choose a service, it displays in the **Add Service** field.
3. Click on the **Add Service** button. The Service Details window opens.
4. In the **Service Name** field, type the unique name you want to assign to the new service, such as CapServ1. The name can include blank characters, apostrophes, and other punctuation, but must be no more than 63 characters long.

   As with the nodes, you should have a systematic naming scheme for your services, especially if you have more than one of the same kind of service. For example, you might name two Capsule Services Marketing CS and Sales CS.
5. In most situations, leave 0 as the default in the **Locked Memory** field.
6. If you want to register the service but keep it unusable until some future time, click on **Inactive**. Usually, though, you should leave this setting in its **Active** default. The *System Administration Guide and Reference* discusses active and inactive options in more detail.

7. If you want the service to start automatically as soon as the service is registered and whenever the server is booted, leave **Auto Start** at its default value, **On**; otherwise, click **Off**.
8. If you want the service to restart automatically whenever the server has stopped for nearly any reason, click the **On** choice in **Auto Restart**; otherwise, leave it at its default value, **Off**.
9. In the **Number of Licenses** field, type the number of copies of this service you want to run. In most instances, you would leave the default number of 1, which is the minimum for any service.
10. In the **PARAMETER VALUES** field, type a DOS file name for the service's internal database (which IDS will create automatically) in the parameter **#1** text area, such as CESDB. This file name must be 1 to 8 alphanumeric characters. It is often convenient to use the service name, or an abbreviation of it, for this parameter.
11. If you leave field **#5** blank, the default is for the service to use System|File Drawers|DXS as its working space. For the Capsule Service, this can cause congestion on the primary file server. To avoid this congestion, specify space on some other disk, such as Aux2|File Drawers|DXS. Notice that vertical bars (|) separate the elements of the path.
12. Click on the **Register Service Information** button, in the window header to add the Capsule Service manager.

You have now successfully added half of this service.

Adding the Capsule Service Execution Engine

1. Pull down the menu next to the **Add Service** button, as shown in Figure 11 on page 55. If no licenses are available for you to assign, the service does not appear in the menu. You might have to scroll the window to see the entire list.
2. Choose **Capsule Service Execution Engine** from the menu.

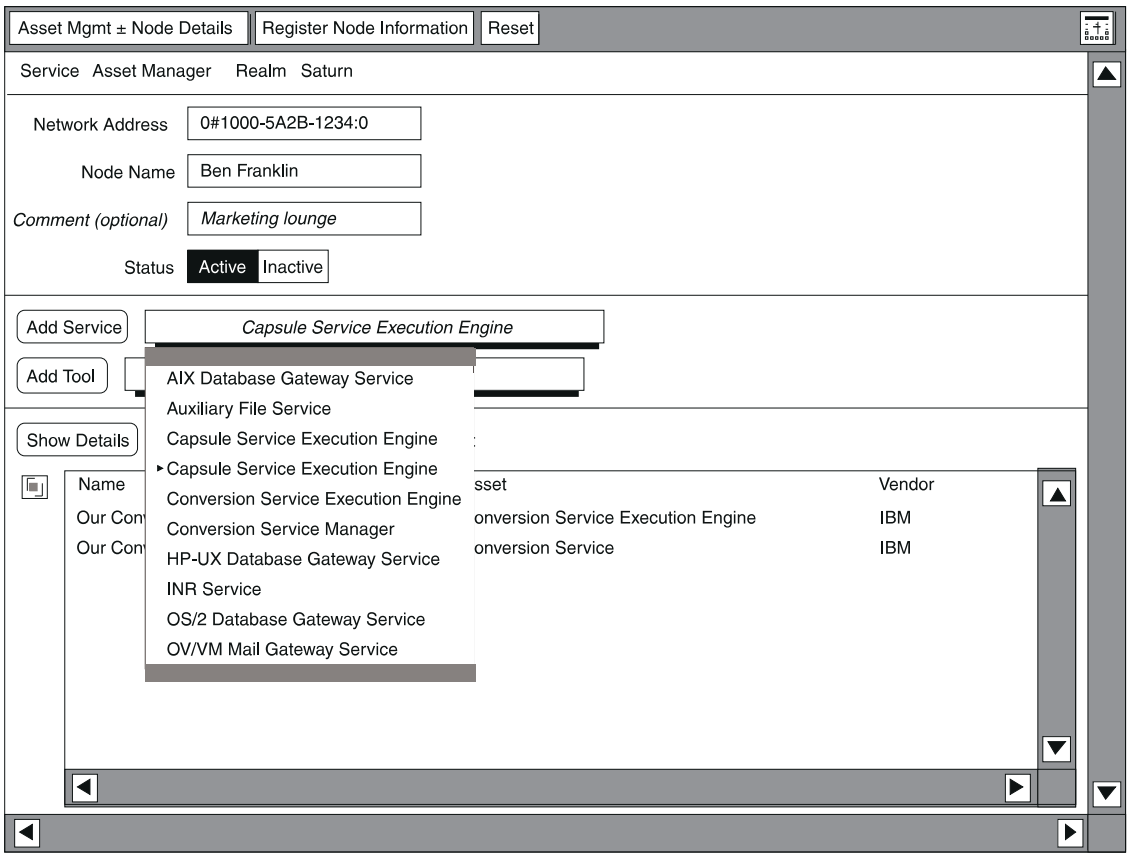


Figure 11. Add Service menu

3. Click on the **Add Service** button. The Service Details window opens.
4. In the **Service Name** field, type the unique name you want to assign to the new service, such as Pubs_Cap_EE. The name can include blank characters, apostrophes, and other punctuation, but must be no more than 63 characters long.

   As with the nodes, you should have a systematic naming scheme for your services, especially if you have more than one of the same kind of service; for example, you might name two print service execution engines Marketing CSEE and Sales CSEE.
5. In most situations, leave the **Locked Memory** field at its default value, 0.
6. If you want to register the service but keep it unusable until some future time, click on **Inactive**. Usually, though, you should leave this setting in its **Active** default. The *System Administration Guide and Reference* discusses active and inactive options in more detail.
7. If you want the service to start automatically as soon as it is registered and whenever the server is booted, leave **Auto Start** at its default value, **On**; otherwise, click on **Off**.

8. If you want the service to restart automatically whenever it has stopped for nearly any reason, click the **On** setting in **Auto Restart**; otherwise, leave it at its default value, **Off**.
9. In the **Number of Licenses** field, type the number of copies of this service you want to run on this computer. For execution engines, the number is usually between 2 and 10. The minimum for any service is 1; the maximum is governed by the amount of memory and processing speed available in the computer.
10. In the parameter #5 text area, specify the name of the corresponding service manager. For example, if your print-service manager is named Cap_Serv1, then field **#5** must be assigned that name also.
11. Click on the **Register Service Information** button, in the window header.

You have now successfully added the remainder of the service.

Adding the Conversion Service

The conversion service is required for ODAS. The conversion service converts data from other sources into a format that can be used by developer's desktops.

Adding a conversion service to a registered node consists of adding a conversion service manager and a conversion service execution engine.

Adding the Conversion Service Manager

1. Pull down the menu next to the **Add Service** button, as shown in Figure 12 on page 57. If no licenses are available for you to assign, the service does not appear in the menu. You might have to scroll the window to see the entire list.
2. Choose **Conversion Service** from the menu. After you choose a service, it displays in the **Add Service** field, as shown in Figure 12 on page 57.

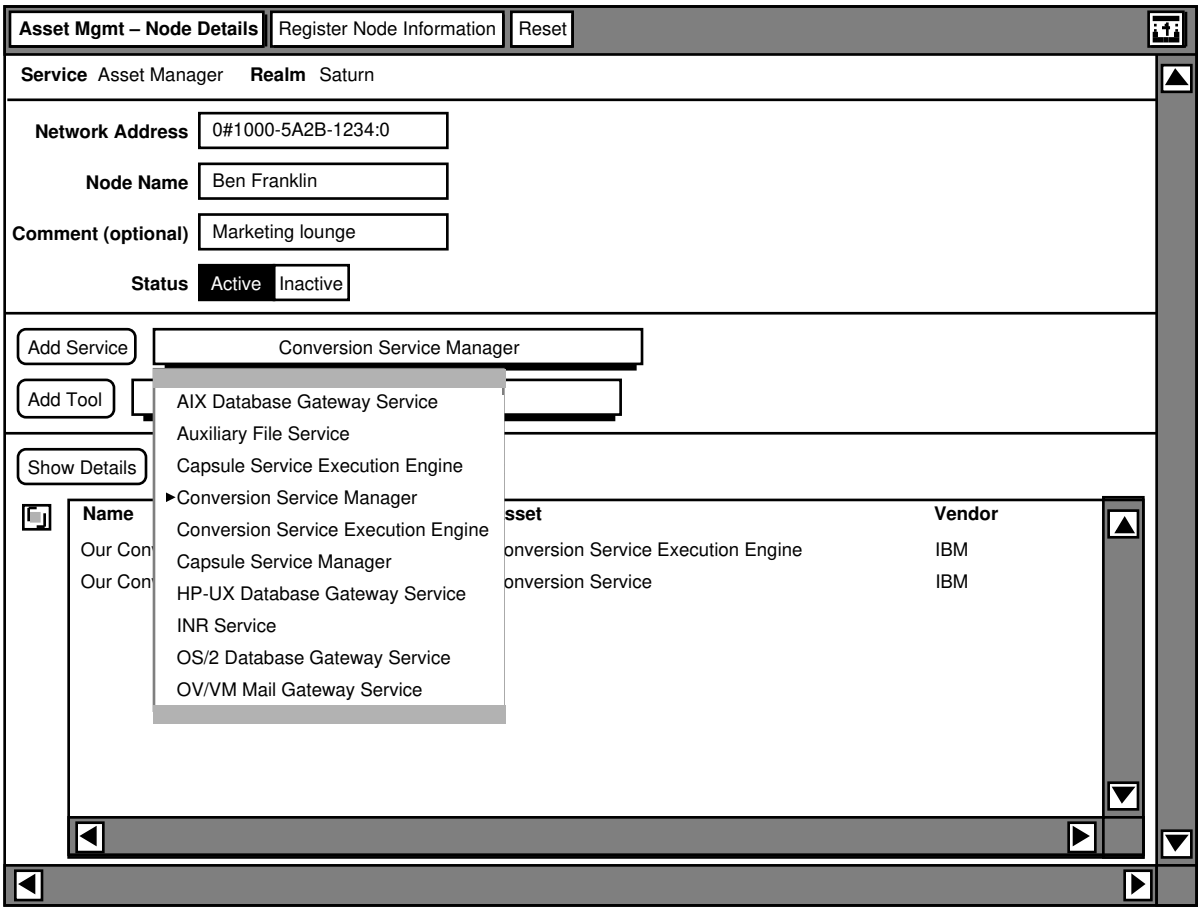


Figure 12. Add Service menu

3. Click on the **Add Service** button. The Service Details window opens.
4. In the **Service Name** field, type the unique name you want to assign to the new service, such as OCS1. The name can include blank characters, apostrophes, and other punctuation, but must be no more than 63 characters long.

   As with the nodes, you should have a systematic naming scheme for your services, especially if you have more than one of the same kind of service; for example, you might name two conversion services Marketing CS and Sales CS.
5. In most situations, leave the **Locked Memory** field at its default value, 0.
6. If you want to register the service but keep it unusable until some future time, click on **Inactive**. Usually, though, you should leave this setting in its **Active** default. The *System Administration Guide and Reference* discusses active and inactive options in more detail.

7. If you want the service to start automatically as soon as the service is registered and whenever the server is booted, leave **Auto Start** at its default value, **On**; otherwise, click **Off**.
8. If you want the service to restart automatically whenever the server has stopped for nearly any reason, click the **On** choice in **Auto Restart**; otherwise, leave it at its default value, **Off**.
9. In the **Number of Licenses** field, type the number of copies of this service you want to run. In most instances, you would leave the default number of 1, which is the minimum for any service.
10. In the **PARAMETER VALUES** field, type a DOS file name for the service's internal database (which IDS will create automatically) in the **#1** field, such as OCSDB. This file name must be 1 to 8 alphanumeric characters. It is often convenient to use the service name, or an abbreviation of it, for this parameter.
11. If you leave field **#5** blank, the default is for the service to use System|File Drawers|DXS as its working space. For the conversion service, this can cause congestion on the primary file server. To avoid this congestion, specify space on some other disk, such as Aux2|File Drawers|DXS. Notice that vertical bars (|) separate the elements of the path.
12. Click on the **Register Service Information** button, in the window header to add the conversion service manager.

You have now successfully added half of this service.

Adding the Conversion Service Execution Engine

1. Pull down the menu next to the **Add Service** button, as shown in Figure 12 on page 57. If no licenses are available for you to assign, the service does not appear in the menu. You might have to scroll the window to see the entire list.
2. Choose **Conversion Service Execution Engine** from the menu. The Add Service window opens.
3. Click on the **Add Service** button. The Service Details window opens.
4. In the **Service Name** field, type the unique name you want to assign to the new service, such as Pubs_Conv_EE. The name can include blank characters, apostrophes, and other punctuation, but must be no more than 63 characters long.

   As with the nodes, you should have a systematic naming scheme for your services, especially if you have more than one of the same kind of service; for example, you might name two print service execution engines Marketing CSEE and Sales CSEE.
5. In most situations, leave the **Locked Memory** field at its default value, 0.
6. If you want to register the service but keep it unusable until some future time, click on **Inactive**. Usually, though, you should leave this setting in its **Active** default. The *System Administration Guide and Reference* discusses active and inactive options in more detail.

7. If you want the service to start automatically as soon as it is registered and whenever the server is booted, leave **Auto Start** at its default value, **On**; otherwise, click on **Off**.
8. If you want the service to restart automatically whenever it has stopped for nearly any reason, click the **On** setting in **Auto Restart**; otherwise, leave it at its default value, **Off**.
9. In the **Number of Licenses** field, type the number of copies of this service you want to run on this computer. For execution engines, the number is usually between 2 and 10. The minimum for any service is 1; the maximum is governed by the amount of memory and processing speed available in the computer.
10. In the field **#5** in the **PARAMETER VALUES** field, specify the name of the corresponding service manager. For example, if your print-service manager is named Pubs_ConvSrv, then field **#5** must be assigned that name also.
11. In the window header, click on **Register Service Information**.

You have now successfully added the remainder of the service.

Adding the Remote Mail Gateway Service

The remote mail gateway service formats, converts, and transfers mail between a cc:Mail Post Office and IDS mail service, and developer's desktops. This service converts the mail messages from the cc:Mail format into a format that is understood by developer's desktops and vice versa.

You should dedicate an object conversion service with two execution engines to this service. For an overall description of the entire IDS mail system, see the *System Administration Guide and Reference* .

To add a remote mail gateway service to a registered node:

1. Pull down the menu next to the **Add Service** button, as shown in Figure 13 on page 60. If no licenses are available for you to assign, the service does not appear in the menu. You might have to scroll the window to see the entire list.
2. Choose **Remote Mail Gateway Service** from the menu. After you choose a service, it displays in the **Add Service** field, as shown in Figure 13 on page 60.

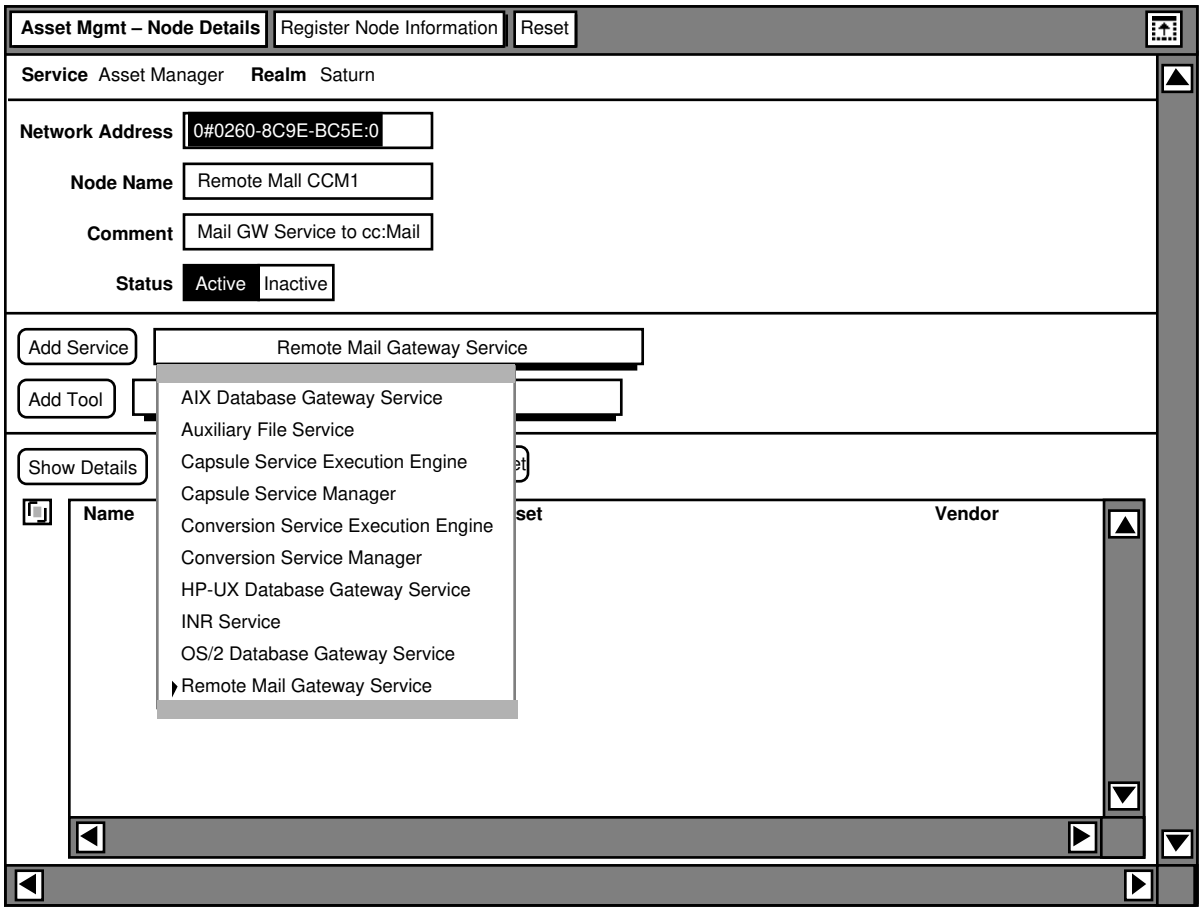


Figure 13. Asset Mgmt - Node Details window, displaying the Add Service menu

3. Click on the **Add Service** button. The Service Details window opens.
4. In the **Service Name** field, type the name you want to assign to the mail gateway service, such as Remote_Mail_CCM1. The name can include blank characters, apostrophes, and other punctuation, but must be no more than 63 characters long. As with the nodes, you should have a systematic naming scheme for your services, especially if you have more than one of the same kind of service; for example, you might have two mail gateway services named Remote_Mail_CCM1 and Remote_Mail_CCM2.
5. In the **Locked Memory** field, leave the default value of 0 as it is.
6. In the **Service Status** field, leave the default setting of **Active** as it is. If you want to register the service but keep it unusable until some future time, click on **Inactive**. The *System Administration Guide and Reference* discusses the active and inactive options in more detail.

7. In the **Auto Start** field, leave the default status set to **On** if you want the service to start automatically as soon as the service is registered and whenever the server is booted; otherwise, change the status to **Off**.
8. In the **Auto Restart** field, change the status to **On** if you want the service to restart automatically whenever the server has stopped for any reason (including intentional shutdowns); otherwise, leave the setting at its default value of **Off**.
9. In the **Number of Licenses** field, type the number of copies of this service you want to run. In most instances, you leave the default number set to 1, which is the minimum for any service.
10. In the **Parameter Values #1** field, type the three-character gateway ID, such as GWA, GWB, or GWC.
11. In the **Parameter Values #2** field, type the full path name of the directory location where the mail gateway service will run and process mail on the workstation. For example:

    d:\mail

    This directory is the gateway's working directory and should have enough memory to allow large messages to be stored and converted in this location.
12. In field **#5**, you can override the default naming format assumed by the conversion service used by this mail gateway service by entering a name of your choice.

    The conversion service associated with the mail gateway service uses a default naming convention based on the gateway service ID . The conversion service for the mail gateway service is named in this format:

    XXXOcs

    where:

    XXX = the three-character gateway ID, such as GWA, GWB, or GWC

    Ocs = a constant in the name of the conversion service
13. Click on the **Register Service Information** button.
14. Close the Service Details window.

    When you close the window, the Asset Mgmt-Node Details window reopens. Notice that the mail gateway service you just added opens as an asset under the **Asset** column, thereby enabling use of the service on that node.

To configure and administer the mail gateway service, see *Configuring and Administering Mail Gateway Service* .

Adding the OS/2 Database Gateway Service

The OS/2 database gateway service is a generic gateway that can be configured to provide developer's desktops access to one or several remote or local database management systems (DBMSs). The IBM Communications Manager/2 must be installed for some gateway services to function.

This service supports the following database gateway types:

DB2

DB2 for OS/2

DRDA

MVS CAS

This service requires the presence on the realm of the primary file, asset management, and directory services to start up successfully.

To add an OS/2 database gateway service to a registered node:

1. Pull down the menu next to the **Add Service** button, as shown in Figure 14 on page 63. If no licenses are available for you to assign, the service does not appear in the menu. You might have to scroll the window to see the entire list.
2. Choose **OS/2 Database Gateway Service** from the menu. After you choose a service, it displays in the **Add Service** field, as shown in Figure 14 on page 63.

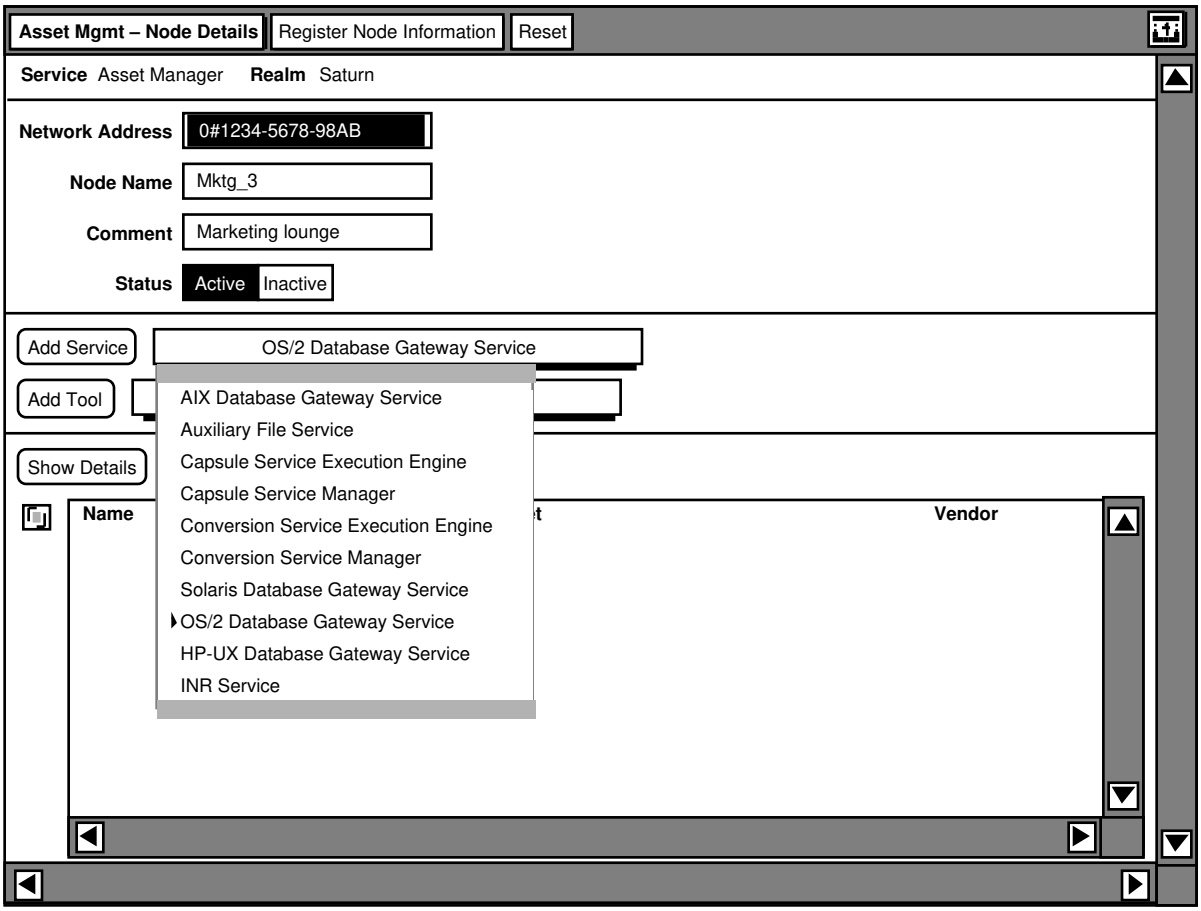


Figure 14. Asset Mgmt - Node Details window, displaying the Add Service menu

3. Click on the **Add Service** button. The Service Details window opens.
4. In the **Service Name** field, type the name you want to assign to the database gateway service, such as Marketing_DB. The name can include blank characters, apostrophes, and other punctuation, but must be no more than 63 characters long.

   As with the nodes, you should have a systematic naming scheme for your services, especially if you have more than one of the same kind of service. For example, you might name two database gateway services Marketing DBG and Sales DBG.
5. In the **Locked Memory** field, leave the default value of 0 as it is.
6. In the **Service Status** field, leave the default setting of **Active** as it is. If you want to register the service but keep it unusable until some future time, select **Inactive**. The *System Administration Guide and Reference* discusses active and inactive options in more detail.

7. In the **Auto Start** field, leave the default status of **On**, if you want the service to start automatically as soon as the service is registered and whenever the server is booted; otherwise, change the status to **Off**.
8. In the **Auto Restart** field, change the status to **On**, if you want the service to restart automatically whenever the server has stopped for any reason (including intentional shutdowns); otherwise, leave it set to **Off**.
9. In the **Number of Licenses** field, type the number of copies of this service you want to run. In most instances, you would leave the default number of 1, which is the minimum for any service.
10. Click on the **Register Service Information** button. The Asset Management window expands to show a list of gateway types for the database gateway service that was selected, such as OS/2 database gateway service.
11. In the Gateway Type column, select the type of database to which you want the gateway to connect, such as **DB2/2 Sessions**.

    One database gateway service can give you access to several types of databases and applications. The only restriction is that a gateway session can either connect to a database service running on UNIX or a database service running on OS/2 operating system, but not both operating systems at once.
12. With a gateway type selected, click on the **Show Details** button. The Asset Mgmt—Gateway Type Details window opens in the top left corner of the screen.
13. In the Asset Mgmt - Gateway Type Details window, type the maximum number of simultaneous user-access sessions of the selected type to be allowed on the gateway you are configuring.
14. Click on the arrow button to display the pull-down menu.
15. Select **Register Gateway Information** from the menu.
16. Close the Asset Mgmt - Gateway Type Details window. In the expanded portion of the Asset Mgmt - Service Details window, notice that the number of sessions (under the **Number of Sessions** column) for the gateway type you selected (such as **DB2/2 Sessions**) has changed to the number of sessions you specified in the Asset Mgmt - Gateway Type Details window.
17. If you want to allow access to another type of gateway accessible through the OS/2 database gateway service, repeat steps 11 through 16. Otherwise, close the Asset Mgmt - Service Details window.

    When you close the window, the Asset Mgmt - Node Details window reopens. Notice that the database gateway service you just added appears as an asset under the **Asset** column, thereby enabling use of the service on that node.

    If you have a UNIX database gateway service already running and if you add additional services to the node on which that service is running, the database gateway service on UNIX must be stopped and restarted.

Configuring a Database Gateway Service

Because some database gateway services reacquire APPC connections to host computers, configuring a gateway service can be a multi-step process. Prior to configuring the gateway service through the **Database Gateway Service** console, you must know the following information:

The types of gateways that were registered with the asset manager

The number of gateway sessions that were registered with the asset manager for the database gateway service

The additional software required for each type of gateway that needs to be configured

Before you add and configure the individual gateways, you should specify the number of database and console sessions for the database gateway service. This task can be performed from the DB Gateways - Service Info window, which contains general information about the service.

To configure gateway sessions:

1. From the Database Gateway Services window, click on the **Show Service Information** button. The DB Gateways - Service Info window opens.
2. Enter the appropriate information into each field requiring input.

   See Table 5 for descriptions of each field within this window and what to type into each of them.

   If you change the value in the **Maximum Database Sessions** entry field, the corresponding Sessions Available display does not change immediately. This is the case even if you close and reopen the DB Gateways - Service Info window. The Sessions Available display is updated within a minute or so.
3. Specify whether you want auto configuration enabled.

   Typically, this choice field is set to **No**. This way, the gateway configuration can be performed and the changes saved. When you are done, this field should then be set to **Yes**; you cannot use the gateway until this field is set to **Yes**. Deferring the setting to **Yes** prevents possible errors during gateway configuration from causing problems.
4. After entering the necessary information, click on the **Set Configuration** button to save the information you specified.
5. Close the DB Gateways - Service Info window.

Table 5 (Page 1 of 2). Descriptions for fields in the DB Gateways - Service Info window

Field	Description
Software Version	Indicates the version of database gateway service software currently running.
Service Up Since	Shows the last time the service was started.

Table 5 (Page 2 of 2). Descriptions for fields in the DB Gateways - Service Info window

Field	Description
Maximum Database Sessions	Specify the maximum number of database sessions the service will support. This is the number of licenses that were actually purchased. The absolute maximum is 150.
Maximum Console Sessions	Specify the maximum number of concurrent console sessions allowed for this service. The default value is one.
Sessions Available	Indicates the total number of sessions configured but not currently active for the service.
Consoles Available	Indicates the total number of console sessions not currently active for the service.
Auto Configuration	Select **Yes** or **No** from the choices. If you select **Yes**, the service will be configured upon start up; if you select **No**, the service will not start up.

Adding and Configuring a Gateway

The parameter values for the fields within the DB Gateways - Gateway Details window must be carefully coordinated with other components, which include other IDS components, the target RDBMS, the IBM Communication Manager/2, and the host software.

To learn more about the process of planning connectivity for database access in IDS installations, see *Planning MVS Host-to-LAN Communications* .

Gateways that require a Systems Network Architecture (SNA) Advanced Program-to-Program Communications (APPC) connection to a host computer have additional fields in the DB Gateways - Gateway Details window. The gateways that require APPC connections to a host system are:

DB2

MVS CAS

Click on the **Add Gateway** button from the DB Gateways - Gateway Config window. A DB Gateways - Gateway Details window opens, which varies depending on the type of gateway that was last selected.

DB2 for OS/2 and DB2 for OS/2 DRDA Gateways: See Table 6 on page 68 for descriptions of each field within this window and what to type into each of them.

1. Type the appropriate information into each field.
2. Click on the **Add Gateway** button at the top of the DB Gateways - Gateway Details window to save your configuration information.

   Repeat all of the steps above for each gateway you create.
3. Close the DB Gateways - Gateway Details window.

A DB2 for OS/2 DRDA gateway is configured to access only one type of DRDA server, which can be a DB2 or SQL/DS server. If you want to access more than one type, you must add a gateway for each type with the correct macro folder (DBS-DB2, DBS-SQLDS, or DBS-OS400) specified for each type.

To connect to a DB2 or SQL/DS DRDA server through a DB2 for OS/2 and Distributed Data Connectivity Services/2 (DDCS/2) connection, the administration for the DB2 for OS/2 DRDA gateway must set up a DB2 for OS/2 database and a User Profile Manager (UPM) user ID that can be configured into the Icon Options windows of the various data access tools. This two-part value must be specified because the design of DDCS/2 and UPM requires that an application (such as an IDS gateway session) must first connect to a DB2 for OS/2 database before it can issue the **CONNECT** command for the DRDA server.

The two-part value is supported in IDS Icon Options windows by the use of two part values for the fields:

local.remote

where:

local = the DB2 for OS/2 specific value

remote = the DRDA service specific value

The two values are separated by a period. This two-part value must be specified in the **Database Name** field, the **User Name** field, and the **Password** field within the Icon Options window. Both the local and remote values must always be specified, even if the values are identical.

To simplify UPM administration, you can create a single local user ID to be specified in all DDCS/2 connected data access icons. Due to limitations on the maximum length of the **User Name** field (which is 11 characters) in the Icon Options window, you should create a two-character local user ID, which would permit two characters for the local user ID, one character for the period, and up to eight characters for the remote user ID.

DB2 and MVS CAS Gateways: When you select a DB2 or MVS CAS gateway, which may require an APPC connection to a host system, the DB Gateways - Gateway Details window opens.

There are four fields specific to a DB2 or MVS CAS gateway. If you are configuring one of these types of gateways, you must provide the appropriate information in the additional fields.

To add one of these gateways:

1. Type the appropriate information into each field.
2. Click on the **Add Gateway** button at the top of the DB Gateways - Gateway Details window to save your configuration information.

See Table 6 on page 68 for descriptions of each field within this window and what to type into each of them.

Repeat steps 1 through 3 for each gateway you create.

3. Close the DB Gateways - Gateway Details window.

SYBASE and Redbrick Gateways: When you select a SYBASE or Redbrick gateway, the DB Gateways - Gateway Details window opens.

There are two fields specific to a SYBASE or Redbrick gateway. When you configure these gateways, you must provide the appropriate information in the additional fields.

To add one of these gateways:

1. Type the appropriate information into each field.
2. Click on the **Add Gateway** button at the top of the DB Gateways - Gateway Details window to save your configuration information.

   See Table 6 for descriptions of each field within this window and what to type into each of them.

   Repeat steps 1 through 3 for each gateway you create.
3. Close the DB Gateways - Gateway Details window.

ORACLE Gateway: When you select an ORACLE gateway, the DB Gateways - Gateway Details window opens.

There are two fields specific to an ORACLE gateway. When you configure this gateway, you must provide the appropriate information in the additional fields.

To add this gateway:

1. Type the appropriate information into each field.
2. Click on the Add Gateway button at the top of the DB Gateways - Gateway Details window to save your configuration information.

   See Table 6 for descriptions of each field within this window and what to type into each of them.

   Repeat steps 1 through 3 for each gateway you create.
3. Close the DB Gateways - Gateway Details window.

Table 6 (Page 1 of 2). Descriptions of the fields appearing in the DB Gateways - Gateway Details window

Field	Description
Gateway Name	Required for all gateway types. Specify the name of the gateway you are adding.
Gateway Type	Required for all gateway types. From a pull-down menu, select the type of gateway you are configuring. This menu contains a list of all the available gateway types for the selected service.

Table 6 (Page 2 of 2). Descriptions of the fields appearing in the DB Gateways - Gateway Details window

Field	Description
Pool	Displayed for all gateway types. If the service is participating in a load-balancing pool, enter the name of the pool. Each gateway can belong to only one pool.
Macro Folder	Required for all gateway types. Enter the name of the folder containing the macros for this gateway type, such as DBS-REDBRICK or DBS-SYBASE. If this entry field is left blank, the SA Tool provides a default name based on the gateway type. If you are configuring a DB2 for OS/2 DRDA gateway, provide the name of the folder for the DRDA server type, such as DBS-DB2, DBS-OS400, or DBS-SQLDS.
Maximum Number of Sessions	Required for all gateway types. Specify the maximum number of concurrently active sessions this gateway supports.
Download Commit Count	Required for all gateway types. Enter a number indicating how many rows of data are to be downloaded to the database before the data is actually recorded. For instance, if you enter 60 as the Download Commit Count, the database updates will be committed after every sixtieth row of data is downloaded. The number you specify depends upon the type of database you are using. For instance, you might download more records before a save to a DB2 database than to another type of database. This field does not apply to an MVS CAS database gateway service. The value of 0 defers the commit until all of the data has been transferred.
ORACLE Home Directory	Required only for ORACLE gateways. Enter the root (home) directory of the ORACLE server directory hierarchy. The home directory contains executable programs and data files. The directory you enter for this field is set in the IBM user's profile file.
Interfaces File Directory	Required for a SYBASE or Redbrick gateway, enter the directory containing the interfaces file so the Sybase Open Client interface can locate the directory.
Target Server	Required for SYBASE and Redbrick gateways. Enter the name of a specific SYBASE SQL or Redbrick server to which you want to connect. The server name you enter for this field is set in the interfaces file.
Default SID	Required only for an ORACLE gateway. Enter a specific ORACLE server system identifier (SID) to be used as a default database. The SID you enter for this field is set in the IBM user's profile file.
LU Alias	Required for DB2 and MVS CAS gateways. Enter the gateway's LU alias. This is the same value supplied earlier in the Communications Manager/2 configuration.
Gateway ID	Required for DB2 and MVS CAS gateways. Enter the three-character identifier for the gateway. If you are using the IBM default values, the identifier will be something like GWA or GWB.
Mode Name	Required for DB2 and MVS CAS gateways. Enter the mode name defined earlier for this service. The mode name must match that specified in the Communications Manager/2 configuration.
Pre-Start	Required for DB2 and MVS CAS gateways. Pre-Start choices **On** and **Off** are used to indicate whether database access sessions are to be automatically started when the database gateway service is initialized. **On** indicates sessions are prestarted. **Off** indicates sessions start in response to a connect issued from a data access tool. The default for this field is **Off**. It is generally more efficient to prestart APPC connections.

Other Database Tasks

After a database gateway service and its gateways are configured, you must perform several other tasks to setting up database access. This section provides a brief overview of the tasks. For more information on these tasks, see *Administering Databases with IDS* .

Configuring Data Access Tools for Database Access

For IDS users to run queries against databases and create reports through data access tools, the icons for the IDS data access tools must be configured to access specific databases. The data access tools include:

Query

Reporter

DBA

SQL Entry

Forms Design

SQL Input

Browser

The process for configuring the data access tools is consistent for all tools. The procedure is described in the respective tool publications. Also see *Administering Databases with IDS* .

The data access tools must refer to the requested database gateway service by the gateway name, not the service name.

Creating Gateway Aliases

The process of over-booking sessions enables you to create gateway aliases. For example, suppose you have a gateway named Pubs that has eight sessions allocated to it. You can create another gateway named Docs using the same parameters and specifying the same number of sessions that were assigned to the Pubs gateway. Thus, Docs is an alias gateway for Pubs.

You cannot create gateway aliases for any of the APPC gateways, because each gateway has its own unique set of APPC conversations. However, you can construct an alias by providing a pool name with only one gateway in the pool.

Locating the Database Folders

IDS provides several database folders, which pertain to a gateway type. In some cases, there is more than one folder per gateway because different RDBMS versions can be accessed by a gateway. Each of the database folders contain many macros that are called from the SA Tool to create the:

Desktop Tools Data Dictionary (WTDD) and data tables

Customized macros to define a database to be used by IDS

User IDs for the database

These folders also contain the Install macro (used during installation) and the DBA Tool Queries file, which contains enhanced SQL functions used by the DBA tool to perform database-specific operations.

To access the database gateway folders:

1. From the system desktop, select the System disk icon.
2. Select the File Drawers container.
3. Select the DBA file drawer. A list of database gateway folders opens.

You will find the following macro folders in the DBA file drawer.

DBS-DB2 DBS-ORACLE7 DBS-OS2 DBS-REDBRICK
DBS-SQLDSDBS-SYBASE DBS-Teradata

Administering Databases with IDS describes the macros contained within each of these folders.

Appendix A. Planning an IDS Network

This chapter addresses some basic issues that affect workstation network design and planning of network and internetwork connections. It provides guidelines to help you understand how connective devices (specifically bridges and routers) can be used in IBM Intelligent Decision Server (IDS) local area network (LAN) topologies and how they can connect IDS LANs to wide area networks (WANs).

What Is a Network?

For IDS users to communicate and share information and computing resources, a *network* must first connect the computers and other devices. A workstation network is a group of devices, or several groups of devices, connected to let users exchange and share information electronically. The groups of devices within a network are related in some way, such as serving a particular work group or supporting a certain application or business function, and work together according to software and hardware specifications.

Networks confined to a small geographic area are called local area networks, or LANs. Typically, a LAN is created to serve a particular work group or building. Users within an IDS LAN usually have a need to share resources, such as file services and databases.

For access to LANs outside the geographical area covered by the local LAN, connection to a wide area network, or WAN, is required. Access to the LANs located remotely is over a communications carrier that provides long-distance connectivity, such as a leased telephone line.

Further discussions of connectivity in IDS LANs concentrate on networks and internetworks and how they are formed.

What Skills Are Required for Planning IDS LANs?

Some participants of the network planning process will have more experience and possess a broader technical knowledge base than others. Unless you have a very small network, it is not likely that any one person can provide all the answers needed to develop a comprehensive IDS network design. Skills required for planning IDS LAN-to-LAN connectivity include:

IDS system administration: installation, maintenance, and administration of IDS. This normally includes the planning of IDS LAN expansion, but does not require knowledge of overall network topology (see “Network Topology” on page 74).

LAN administration: monitoring the performance of LAN components and overseeing all products (not limited to IDS) installed on the LAN. For IDS installation, working knowledge of Communications Manager/2 is required.

Network troubleshooting: fault isolation and problem determination. This requires the ability to run network traces of several different protocols, read hexadecimal

© Copyright IBM Corp. 1996

network traces, and includes knowledge of local network functions and, in some cases, LANs, WANs, and large-network topology.

Technical knowledge of personal computers and OS/2: familiarity with their operation, including technical requirements for running IDS, ability to isolate problems with configurations, and ability to troubleshoot malfunctioning units.

Monitoring network performance and tuning the network. This function also often includes overseeing the entire site installation, ensuring its uninterrupted operation, and planning and implementing its expansion.

Because job descriptions and responsibilities vary, the skills necessary for planning networks might be distributed in different ways.

If your network plan involves host-to-LAN connectivity, it also involves Communications Manager/2 and advanced program-to-program communications (APPC) connections, so these additional skills are required:

IDS host administration on the host workstation: usually performed by an MVS or VM system programmer. It involves monitoring and managing IDS resources and is usually a specialized function, but is sometimes combined with management and programming of DATABASE 2 (DB2) or other resources. IDS host administrators might also work with Oracle, Red Brick, and SYBASE data sources.

Security administration: management of security issues for the overall host environment and setting standards for or controlling access to stored data.

Data-center planning: short and long-range planning of hardware and software installation and expansion. It is often combined with overseeing the overall operation and day-to-day activities of the data center.

Communications management: controlling Virtual Telecommunications Access Method (VTAM), Network Control Program (NCP), and Remote Spooling Communications System (RSCS) or job entry subsystem (JES).

Systems programming: controlling host operating systems, which might include Multiple Virtual Storage (MVS) or Virtual Machine (VM). It involves keeping the host system up and managing resources, as well as tuning and monitoring performance.

Database management: controlling DB2 or other relational database management systems. It includes managing resources associated with data access and monitoring database performance.

Planning VM Host-to-LAN Connectivity and *Planning MVS Host-to-LAN Connectivity* contain more details about the host-related skills listed here.

Basic Network Design

Workstation networks comprise a variety of software and hardware components, all of which must function together for communications to take place. Similar components, such as printers, personal computers, and mainframe computers, exist in all networks. Elements to consider when planning for connectivity include:

Physical medium

Networks

Network segments

Internetworks

Connective devices

Physical Medium

The *physical medium* is the network cabling or wiring that connects communications devices and transports the electrical signal between them. Computers, printers, and other devices are attached to the network cable by drop cables.

Associated with each type of medium are standards, such as those for Ethernet and token-ring networks. Standards dictate characteristics of the environment, such as how long segments of wiring can be, how many nodes (communications devices) can be placed on each wire, the minimum distance required between nodes, and the speed at which data can be transmitted.

Network Topology

The primary focus of the IDS network-planning process is to define the overall network topology. The topology encompasses the physical layout of the network, as well as the network medium and the compatibility of software and connected devices. In making decisions about your network topology, you must ensure that the topology:

Is manageable

Adequately meets the communications needs of your users

Allows room for anticipated growth

Yields expected network performance

Provides efficient communications paths between nodes

Obeys the standards for its network type

Networks and Network Segments

You can create networks on a single cable or by connecting two or more network segments through a connective device. Depending upon the type of connective device used to join segments, you can create one large network or a series of smaller networks. Each separate network has a unique number to identify it.

An IDS network can be very small, with only a few computers and other devices attached. Figure 15 on page 75 shows a small, stand-alone IDS network supporting a printer, a print service, a file service, a database server, and three desktops.

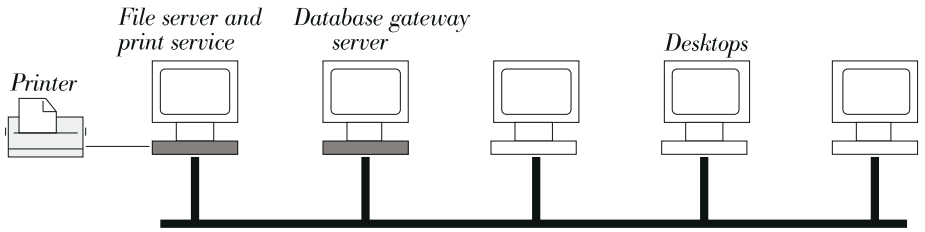


Figure 15. an IDS network providing connectivity for a small group of users

You can attach certain additional equipment to this network to connect it through a communications link to another, remote network. Its users could then exchange mail with users on the remote network and have access to remote services and other resources.

IDS network designs vary from one site to the next. One company, for example, might join many separate segments to form one large IDS network. Another company with a similar layout of physical wiring might create several smaller IDS networks and join them to form an internetwork (see "Internetworks" on page 76) because the configuration better suits its needs. In Figure 16, a bridge (a type of connective device) joins two LAN segments to form a larger network.

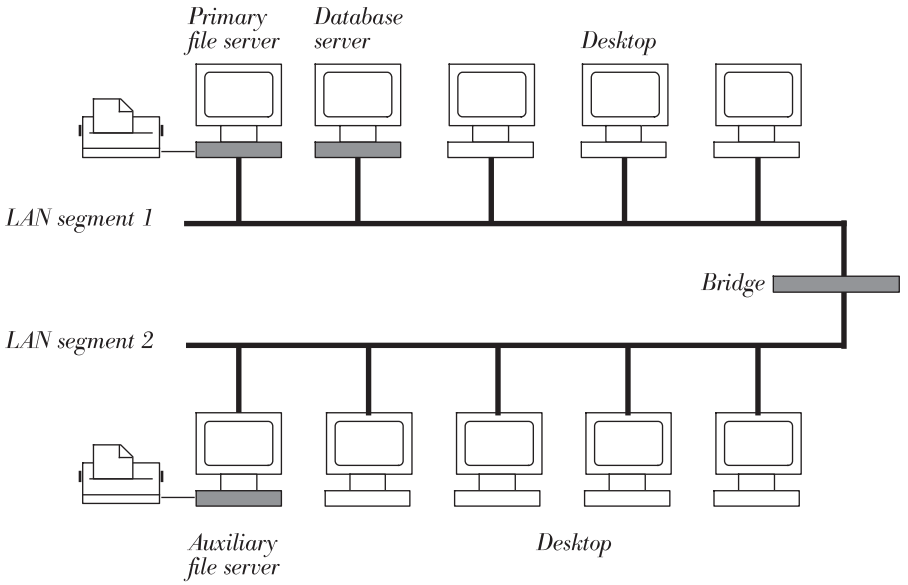


Figure 16. An IDS network comprising two LAN segments joined by a bridge

The bridge provides a physical connection between the two individual segments, making them appear and function as a single network. Users on the two segments are unaware of the bridge and share the same primary file service, database server, and printers. More information on bridges follows in "Connective Devices" on page 77.

In token-ring networks, the maximum number of cards that can be installed on a single ring segment is 255. If you need to install more than 255 token-ring cards on a LAN, you must bridge the LAN at least once.

Internetworks

Internetworks are formed when groups of independent IDS networks are joined together to allow users on the separate networks to exchange mail and to share resources such as database gateway services, mail gateway services, and mainframe resources. Routers are devices that connect independent IDS networks with one another, as shown in Figure 17.

Notice that each of the networks contains its own primary file service. Users on both networks have access to services that can be shared, such as mail and database gateway services.

Additionally, IDS provides the capability for routable workstations (sometimes referred to as RWS). The routable workstation can be physically connected to one network, yet have its primary file service, print services and other services reside on a different network with the appearance of being local. See "Using Routable Desktops in IDS Networks" on page 88 for more information.

The router connects two separate, independently functioning networks to create an internetwork.

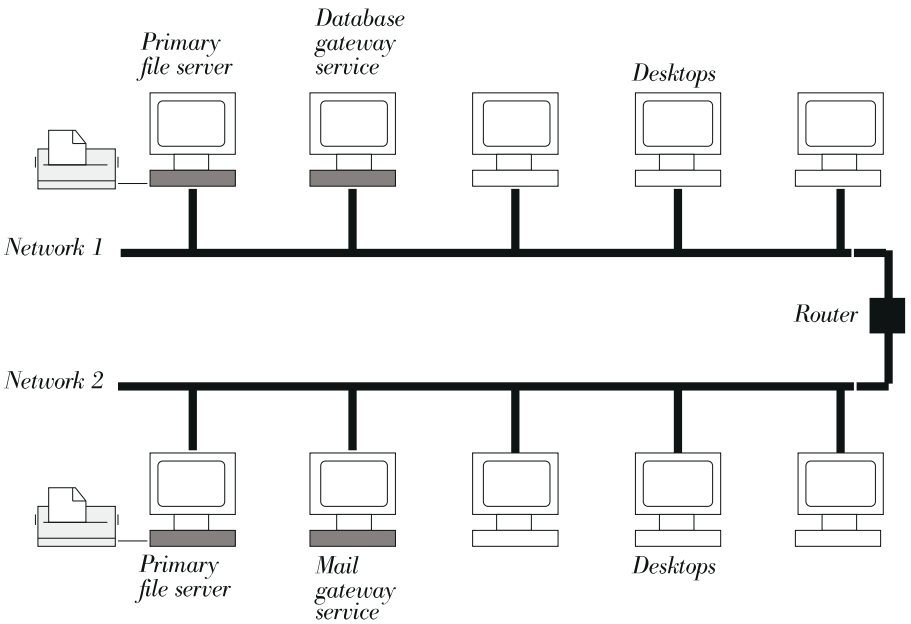


Figure 17. Router connecting two independently functioning networks

Connective Devices

When it is necessary to join two physical media, you use some kind of connective device. In a computing network, connective devices perform a variety of functions, including extending and boosting electrical signals, segmenting LANs, extending geographical boundaries by connecting physically remote LANs, and connecting separate groups of users who need to exchange mail and share resources. Depending upon the function needed, you can use one of five types of connective devices to join the physical media:

Repeaters

Bridges

Routers

Brouters

Gateways

This appendix does not cover all of these connective devices in depth, but it is important to understand how they are used and where they might appear in IDS LANs.

Repeaters

Repeaters are hardware devices that extend the transmission limitations of a carrier by re-sending the electrical signal over the wire and by retiming the signal so that it remains clear as it traverses the network. As the electrical signal travels over the physical medium, it loses strength and becomes distorted. The distance over which it remains effective can vary with different types of physical media. When the distance between devices is beyond the carrier limitation of their physical medium, you can use a repeater to connect two segments, such as two lengths of the same type of Ethernet cable. Users are unaware of the presence of repeaters in a network.

Bridges

Bridges are devices that join two or more LAN segments of the same type of medium, such as two token-ring segments or two Ethernet segments, to form a larger network. They work with *data protocols* (rules that define data formats for communications) rather than with electrical signals on the physical medium. Figure 18 shows two physically separate cables connected by a bridge.

The bridge connects two separate physical segments to create a single, larger LAN.

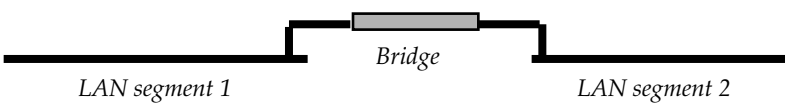


Figure 18. Bridge connecting multiple LAN segments

The bridge in this configuration extends the geographical coverage of the physical medium by connecting the separate LAN segments to create a larger network; the connected LAN segments function together as a single network. Bridges make all the devices on the connected segments appear to be on the same LAN.

A bridge cannot boost the signal; that function requires a repeater.

Segmenting LANs with Bridges: Bridges can be configured to *forward*, or pass, some information and to filter, or block, other information. Information passes through the network in the form of *packets* (binary units of data and control information).

Some bridges can learn and adjust to changes in the networks to which they are attached. Bridges listen to all traffic on each of their connected LAN segments. From addressing information contained in each *packet header* (control information, including source and destination address), bridges learn the source address of each packet. They also look at destination addresses and forward only packets bound for a segment other than the one to which the packet's source address belongs. If the packet's destination address is not one of the bridge's learned addresses, the bridge forwards the packet. The assumption in this case is that the packet is destined for a remote network.

If a network becomes too large and contains many bridges, then fault isolation, or problem determination, can become difficult. Hardware failures and traffic-congestion problems can be difficult to locate and can potentially cause network-wide problems. Some bridges do not function well if a network contains *redundant paths*, or multiple paths, between two end points. When a network has redundant paths, *loops* are created, allowing more than one copy of a packet to be propagated through the network. As networks grow in size, the overall topology can become very complex. It is not always possible, nor is it necessarily desirable, to avoid creating redundant paths in a network.

Redundant paths actually help to prevent communication interruptions caused by hardware failure or by the interruption of a path within the network. When bridges join network segments, one large network is really created from several small physical network segments.

Managing Redundant Paths with the Spanning Tree Algorithm: To prevent packets from being caught in loops, most bridges contain a mechanism called the *spanning tree algorithm* (STA). Bridges use this algorithm to collect source and destination information and use that information to detect redundant paths in the network and determine the most efficient traffic pattern.

IDS requires a valid spanning tree and IBM recommends that you use *dynamic or automatic route determination*, an option included in the configuration of most bridges. When you use the automatic route determination feature, traffic patterns are defined and managed without the need for manual intervention. If the physical medium is a token ring and you are defining your own spanning tree, take extreme care in creating your configurations. Defining the spanning tree manually can result in many errors.

Unless bridges are equipped with advanced features that enable them to detect and properly handle multiple paths, erroneous data packets can be propagated through the network. If all bridges in the network are configured to use the spanning tree algorithm to automatically detect changes in ring topology, the algorithm inherently solves and manages loops.

Understanding Message-Forwarding Protocols: Bridges use one of two protocol types, transparent or source routing, to forward messages.

Bridges that use the transparent routing protocol use only the node address or device address to forward packets. To a bridge, every device appears to reside on the same network. Bridges use the address in each packet to decide whether or not to pass the packet from one connected segment to another. Transparent bridges are usually used on Ethernet LANs only, but can be used in token-ring LANs. If you have an Ethernet LAN and you use transparent bridges, be sure the spanning tree algorithm is enabled in each bridge.

Bridges that use the source-route protocol use the source and destination addresses, contained in the packet header, to pass each packet between network segments. The node sending the data uses a discovery mechanism, in which it sends out a packet to learn the path to the destination. As the discovery packet travels to the destination, each bridge it traverses adds its own segment number as it forwards the packet. When the response to the discovery packet is returned to the source node, it retraces the same path; then, the actual data packet is sent along the learned path. Source-route bridging is usually used on token-ring LANs, although a combination of source-route and transparent bridging can be used.

Source-route transparent (SRT) bridges are capable of using both transparent bridging and source-route bridging methods to forward packets. An SRT bridge examines each packet to see if it uses the source-route protocol. If it does, the bridge uses that protocol to forward the packet. If the packet does not use the source-route protocol, the bridge forwards the packet with the transparent protocol.

Bridges can be either local or remote. Local bridges join LAN segments directly to one another. Remote bridges join a LAN to a communications carrier that provides long-distance connectivity, such as Synchronous Data Link Control (SDLC), X.25, or Frame Relay connections. Remote bridges occur in pairs, with a bridge on each network segment and a long-distance medium in between, to connect remotely located LAN segments.

Bridges are expected to forward network traffic between LANs without impeding performance on either LAN. See Figure 19 on page 80 for an example of local and remote bridges.

Routers

A router connects two or more independent networks into an *internetwork*. Each independent network retains its own identity as a separate network, is identified by a unique network number, and continues to function independently.

Like bridges, routers can be configured to forward or filter packets. Routers use complex network-address information to forward packets. They add or change packet-address information as the packets traverse the network. Because routers use network addresses rather than device addresses and are capable of forwarding more than one packet format, you can mix physical media types in your internetwork. For example, a router can forward traffic between a token-ring LAN and an Ethernet LAN.

A router can process more than one protocol, but it must be configured to route or filter each protocol. The format of each packet is specific to the LAN protocol being used, and each protocol has its own addressing scheme. If you are using NETBIOS or Digital Equipment Corporation's LAT protocol in your network, these protocols cannot be routed. They must be bridged.

Like bridges, routers can be either local or remote. Figure 19 shows a simple IDS internetwork that includes both local and remote bridges and routers.

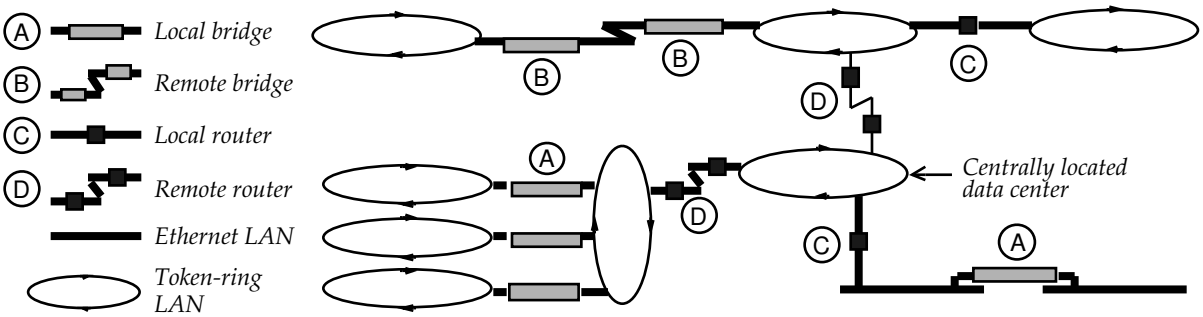


Figure 19. An internetwork that includes local and remote connectivity

In the network topology illustrated in Figure 19, local and remote bridges and routers connect distributed LANs to a centrally located data center. Notice that the internetwork includes both token-ring and Ethernet networks. The bridges connect like physical media while the routers connect like and different physical media.

Routers forward packets based on information stored in a routing table. Each router maintains its own routing table, which associates a specific protocol and a network number with a particular connected LAN. When a router receives a packet, it checks the packet's destination network number against its routing table to determine where to send the packet.

Routing-table information is gathered by either static or dynamic routing. In static routing, a network administrator manually enters the routing information into a routing table.

Some routers are capable of dynamic routing, or learning the routing information by exchanging routing protocol packets with other routers on the network. Several types of dynamic routing protocols exist, such as routing-information protocol (RIP), "open shortest path first" (OSPF), and intermediate system-to-intermediate-system (IS-IS).

Brouters

Another type of device that forwards network traffic is a *brouter*, which combines the capabilities of a bridge and a router into a single device. Brouters are typically used in multiprotocol networks at locations where bridging and routing of different protocols is required over the same part of the network. Each part of the device functions independently, so brouters can be configured to perform bridge functions, router functions, or both. It is not possible to bridge and route a single protocol at the same time, so

brouters must be configured to perform either the bridging function or the routing function for each protocol.

Gateways

Gateways are connective devices in the sense that they perform data or packet-format conversion to enable users of incompatible systems to communicate. The conversion might be for mail exchange between two different mail systems, or it might be for communications between two systems running different protocols. In IDS LANs, gateway technology provides IDS users with the ability to exchange mail with users of external mail systems and to access databases on remote host systems.

Designing IDS Networks

IDS provides a variety of desktop tools for accessing databases and analyzing data. The data access capabilities are based on a client/server architecture. This architecture allows for the distribution of data on a variety of platforms that can be attached directly to IDS networks, or located remotely.

Routers and bridges can play a significant part in the design of your IDS network, especially in complex networks and large LANs. Using bridges enables you to extend the range of a single IDS network allowing the users and services of a single network to be separated over a larger area. Using routers enables you to link separate IDS networks so that users on those networks can exchange mail outside their local network and have access to database gateway services on networks other than their own. Routers can also be used to allow specially configured developer's desktops (called routable desktops) to access a network that is remote to the network of their directly connected LAN. In considering your overall network design, you must plan the connections to be established, and you must determine the means by which you will make those connections. You need to know where in your network routers and bridges are required.

Whether you use a bridge or a router at a particular location in your network depends upon many factors, such as security and resource control, what you need to accomplish at that location, and how that location fits into your overall network design. A simple rule to remember is that bridges are used within network boundaries; routers are used between networks.

You can use bridges to join separate segments into one large LAN. When bridges join physical segments to form a larger network, all the segments are recognized by the same network identifier. In a TCP/IP LAN the network identifier is an 8, 16, or 24 bit field within the IP address corresponding to CLASS A, B, and C, IP addresses. Figure 20 on page 82 shows a bridged and routed TCP/IP environment and the relationship between physical LANs and TCP/IP networks. The actual TCP/IP network numbers are not shown, instead the numbers 1, 2, 3, etc. are used to denote each network. An example of a typical TCP/IP network number is 143.241.0.0, which is a CLASS B address.

The TCP/IP protocol supports a method of subdividing a network into multiple logical networks using subnetwork numbers. IDS supports TCP/IP networks divided into sub-

network identically as it supports networks that do not use subnetworks. IDS itself, provides a method of subdividing TCP/IP networks using the concept of IDS realms.

When routers join separate networks into an internetwork, each of the networks is recognized by its own network number. In Figure 20, notice that each of the connected LANs is identified by a unique network number.

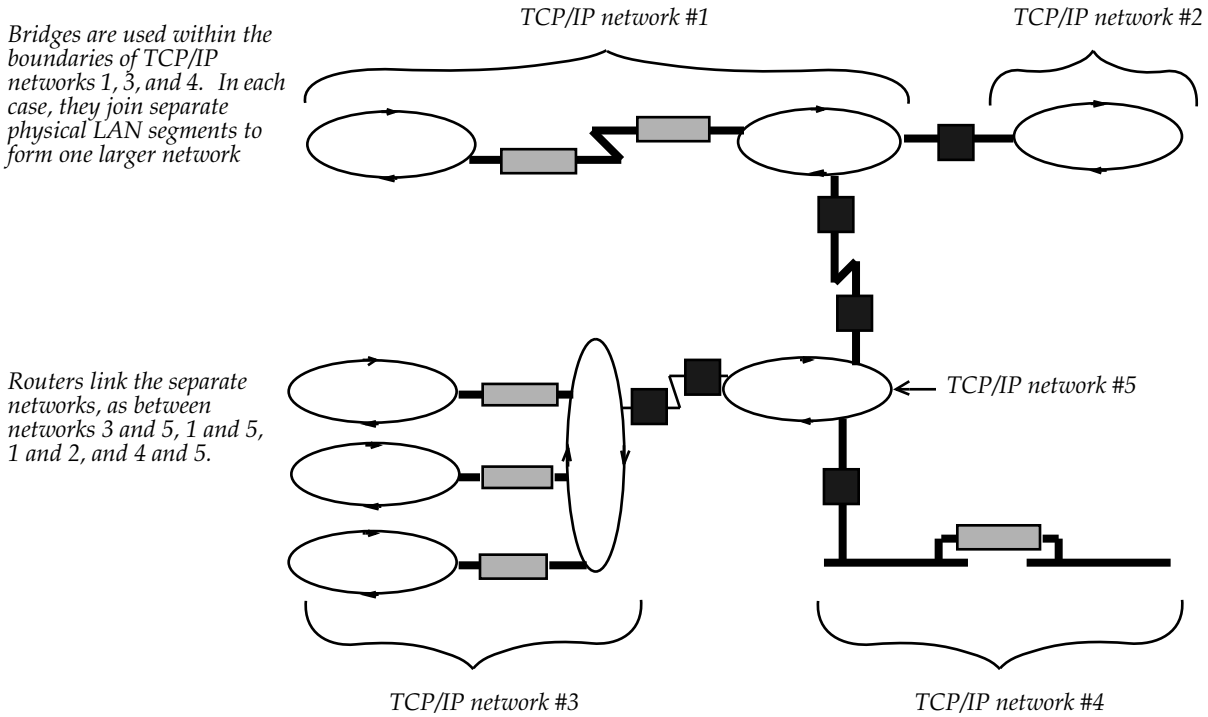


Figure 20. Network numbers in an IDS environment

Selecting the Physical Medium and the LAN Protocol for Your IDS Network

IDS services and desktops run under IBM OS/2. The physical medium for IDS LANs can be either token ring or Ethernet.

IDS is fully compliant with TCP/IP protocol conventions. This protocol compliance lets you remain flexible in selecting vendors of bridging and routing devices. In network locations where bridging or routing of network traffic is advisable, you can use standard bridges or standard routers.

For use in IDS networks, bridges must:

- Be able to bridge the source-route protocol in a token-ring environment
- Provide a minimum of 56-KB line speed for remote connections, although higher speeds are recommended for better performance

Support use of the spanning tree algorithm

IDS Networking Protocols

In addition to the standard protocols implemented in the TCP/IP protocol suites, IDS uses proprietary protocols. All IDS proprietary protocols are encapsulated within TCP/IP standard protocols and are transparent to routers which support TCP/IP.

IDS uses different protocols for communications between components within an IDS LAN and for communications between IDS LANs. Within a single network, IDS makes certain assumptions about the availability of resources, such as access to a primary file service, asset manager, or directory service. These access issues must be considered when you design IDS LANs. TCP/IP and proprietary protocols used within IDS LANs are:

Disk-service protocol (DSP): Used between desktops and file services; it can be bridged or routed.

The use of DSP in a routed environment is limited to routable desktops only.

S411 protocol: Used between services to gather information about service locations; it can be bridged or routed.

Figure 21 shows where each of these protocols is used within an IDS network and the routing or forwarding method that you can use with each.

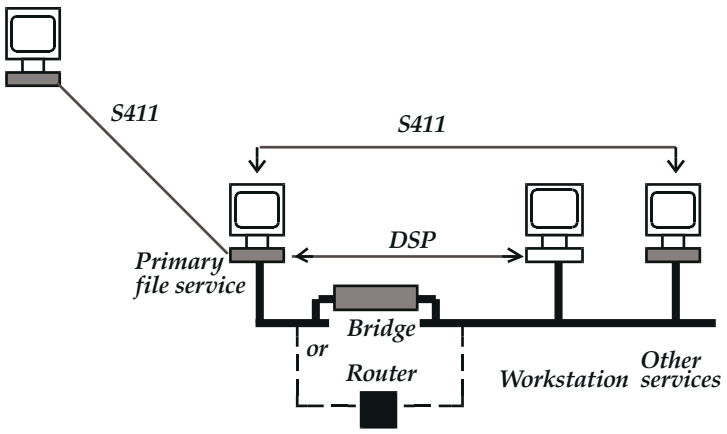


Figure 21. IDS network and proprietary protocols

Disk Service Protocol:

Within IDS LANs, workstations and file services communicate through the proprietary DSP, which makes two assumptions:

Operations occur at network speed, which, depending on the physical medium, is 4, 10, or 16 megabits per second.

Workstations submit requests to file services, then wait in an idle state for the file service to respond.

DSP takes advantage of the ability of file services to read disk files directly to the network; it does not provide a flow-control mechanism. DSP is encapsulated within the User Datagram Protocol (UDP) of the TCP/IP protocol suite. DSP typically performs functions such as loading program overlays from file services, loading user data from file services, and saving user data to file services. The DSP protocol is very sensitive to timing. In IDS, the routable desktop utilizes a special modifications to DSP (and S411) to permit a desktop to communicate with a file server that is on a different network or different subnetwork. For more information, see “Expanding Your Network with Realms” on page 89.

Workstations and file services communicate through DSP; it can be bridged or routed.

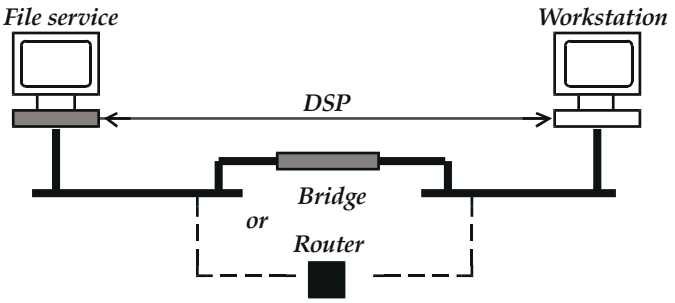


Figure 22. DSP path in an IDS network

Sequenced Packet Protocol and S411 Protocol: Connections between networks are often much slower and the medium is more error prone than within a network, such as on an Ethernet or token-ring segment. Communications between IDS networks depends on:

TCP/IP Transport Control Protocol (TCP)

IBM private S411 protocol

The TCP protocol was designed to provide flow control, data transmission retries, and error-free communications. TCP is used for communications between IDS nodes. IDS services use TCP to communicate with each other and to send mail. Figure 23 on page 85 illustrates the use of TCP between IDS services.

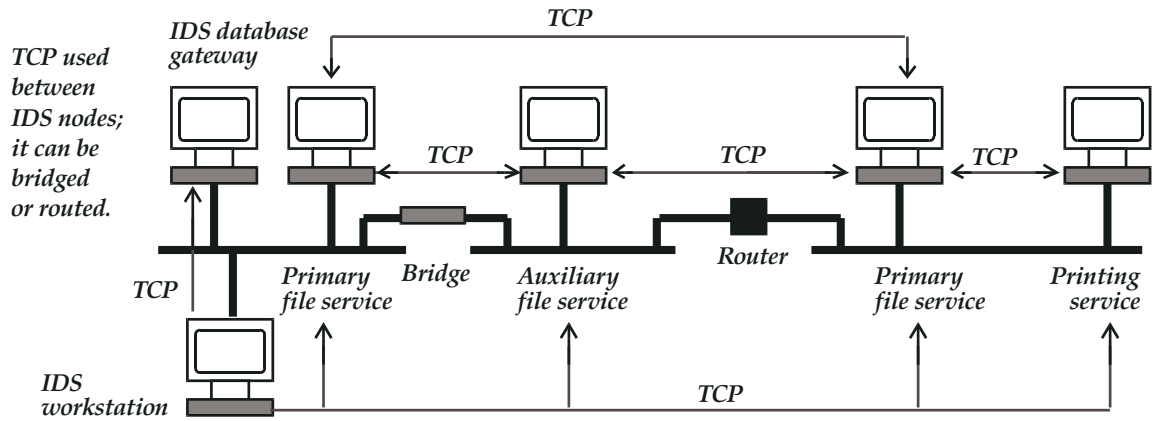


Figure 23. TCP and SPP paths in IDS networks

Almost all IDS services use S411, the IDS directory service's protocol, to gather information about other services and where they are located. Both S411 can be routed, which means that you can have internetwork routers between separate IDS LANs to provide for mail exchange and access to remote resources. Figure 24 illustrates the use of the S411 protocol between IDS services.

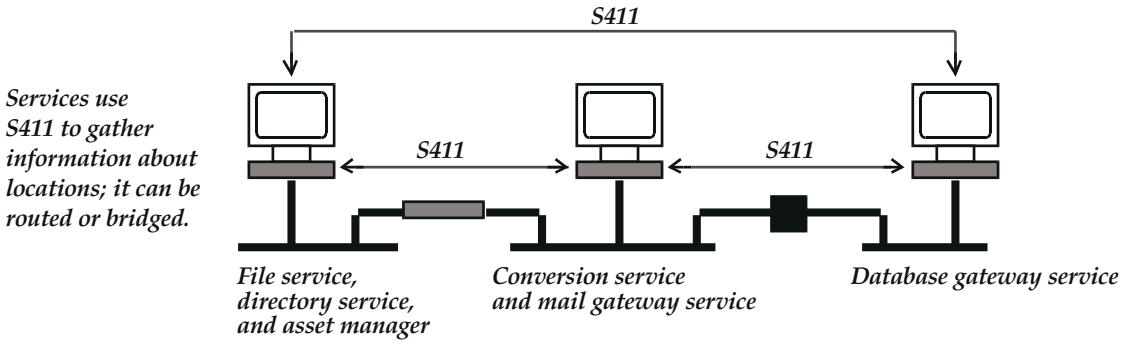


Figure 24. S411 path in IDS networks

Routing Protocols: Routers use routing protocols to build routing tables that list all of the accessible networks and the first router to be used in the path to each. No IDS products implement routing functionality. All routing is handled by third-party industry-standard routers. Therefore, IDS can be installed without concern to the routing protocol chosen for a TCP/IP network.

Using Bridges in IDS Networks

Within a company network, bridges often become necessary to connect LANs that were created at different times by different departments for different reasons. When those LANs were originally created, no need existed for users on the separate LANs to share resources, such as database gateway services; but, due to changing needs, those same users now require use of common hardware and software resources.

Likewise, consider the case where a company occupies several floors of a building or is geographically located throughout several buildings in a campus-like environment. Here, it might be more cost-effective to maintain separate segments on each floor or in each building and connect them as needed through bridges, rather than to duplicate entire IDS facilities in each location. In a network configuration such as the one shown in Figure 25, all users are part of a single large network.

The backbone ring (or main token ring for the building) shown in Figure 25 provides connectivity among the LANs through bridges, to let users located on each of the three floors have access to shared resources such as file services. Although these segments are connected through bridges, they could each contain multiple IDS realms. The backbone ring is connected over a long-distance medium to a central data center. Users on each of the connected segments have access to IDS and other resources maintained at the central data center.

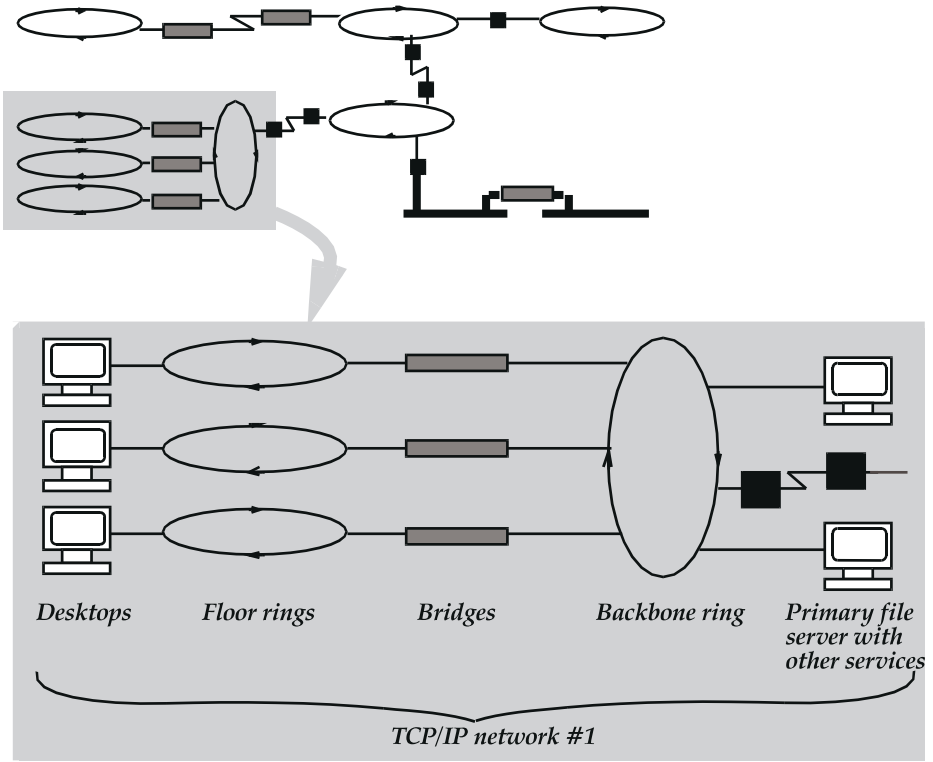


Figure 25. Using bridges to connect LAN segments

To summarize, bridges are useful in networks with:

- Smaller, simpler network topologies
- Only one medium
- Desire for simplified administration

Concern for costs of initial hardware, installation, and maintenance

Only one IDS network required

Using Routers in IDS Networks

Typically, an IDS environment uses routers when the databases are centrally located, thereby aiding administration and resources management. Routers link remote IDS LANs with the central LAN to give remote users access to the databases and other resources. By letting the LANs function independently, you maintain more control over the traffic flow on the network. Figure 26 shows this type of configuration.

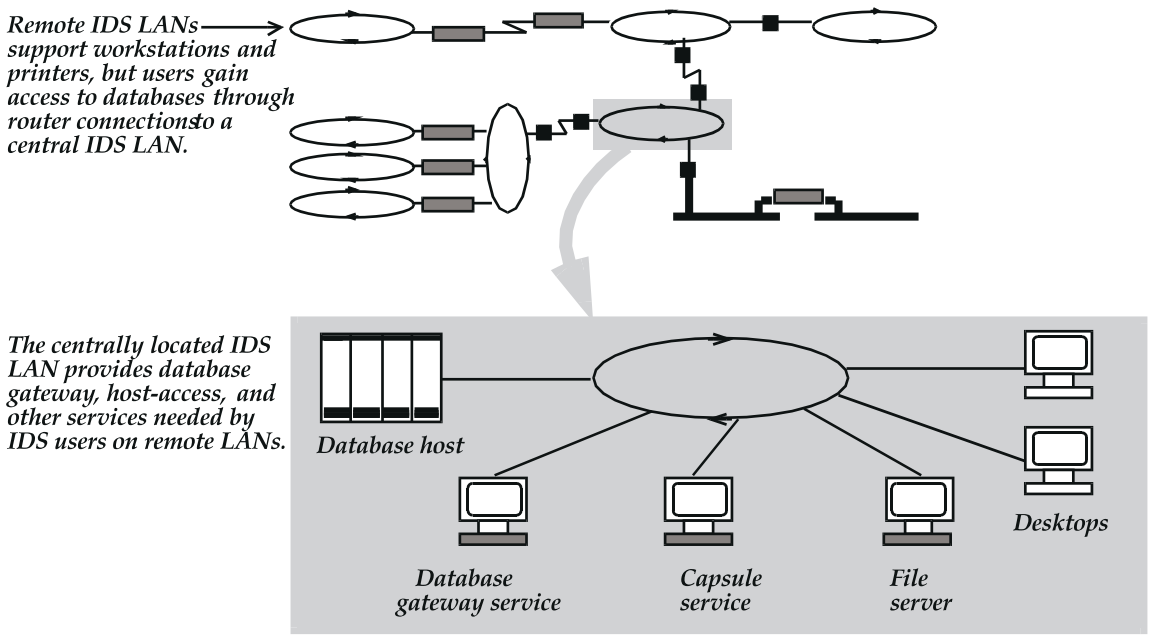


Figure 26. Routers providing access to a centrally located LAN

In Figure 26, some of the routers providing access to the central data center are remote routers, because each connects a LAN to a long-distance medium. Standard routers can connect to a variety of long-distance media; consult each device's reference publications for details.

Routers can link separate IDS LANs for mail exchange, remote database access, and some remote administration support for IDS services. If you have a situation where two or three developer's desktop users are physically located at some distance from the other users and services on the LAN, consider long-term growth before you decide how to incorporate those users into the network. If you anticipate a fair amount of growth and the possibility of adding more users and services to the remote segment, you should consider establishing a full IDS LAN and, therefore, should connect the remote LAN by a router rather than setting up a simple LAN segment connected by a bridge. Developer's desktops can be connected to the main IDS LAN through a router when

using the TCP/IP protocol stack. See “Using Routable Desktops in IDS Networks” on page 88.

To summarize, routers make sense in:

- Larger, more complex environments where multiple networks must be connected
- Networks that are remotely linked (routers make efficient use of remote WAN connections)
- Topologies where unlike media must be linked (such as linking an Ethernet LAN to a token-ring LAN)
- Networks in which security is a critical issue
- Networks where fault isolation is critical and must be addressed in a timely manner so as to minimize any impact on overall network performance
- Situations where developer's desktops require access to IDS services on a different network.

TCP/IP Restrictions: There are no special restrictions imposed by IDS on TCP/IP routers.

Using Routable Desktops in IDS Networks

IDS supports routable desktops, which can be useful in designing and implementing IDS networks. A routable workstation is a specially configured IDS workstation that can be a member of a remote IDS network reached via one or more hops across routers. IDS servers do not have to be present on the local network to which the routable workstation is connected. However, all of the servers of a given IDS network must be located on the same network.

The routable workstation does provide an alternative solution for those sites in which bridging is not possible, and separate IDS networks are not required or desirable. When IDS is incorporated into an existing network, especially a TCP/IP network, it can not be possible to use bridges to allow remote users to access an IDS network. Figure 27 on page 89 shows an example of a building with three floors, each wired with Ethernet and all bridged together using a central backbone FDDI ring with the TCP/IP class B network number, 143.241.0.0. In another building is an Ethernet, with a different network number (143.242.0.0). The first building will house all of the IDS servers and the majority of IDS users. However, the second building also has a need to access IDS services, but will have only a limited number of workstations. In this case, routable workstations can be configured for the second building, allowing these users to "join" the IDS network even though they must use a router to reach it.

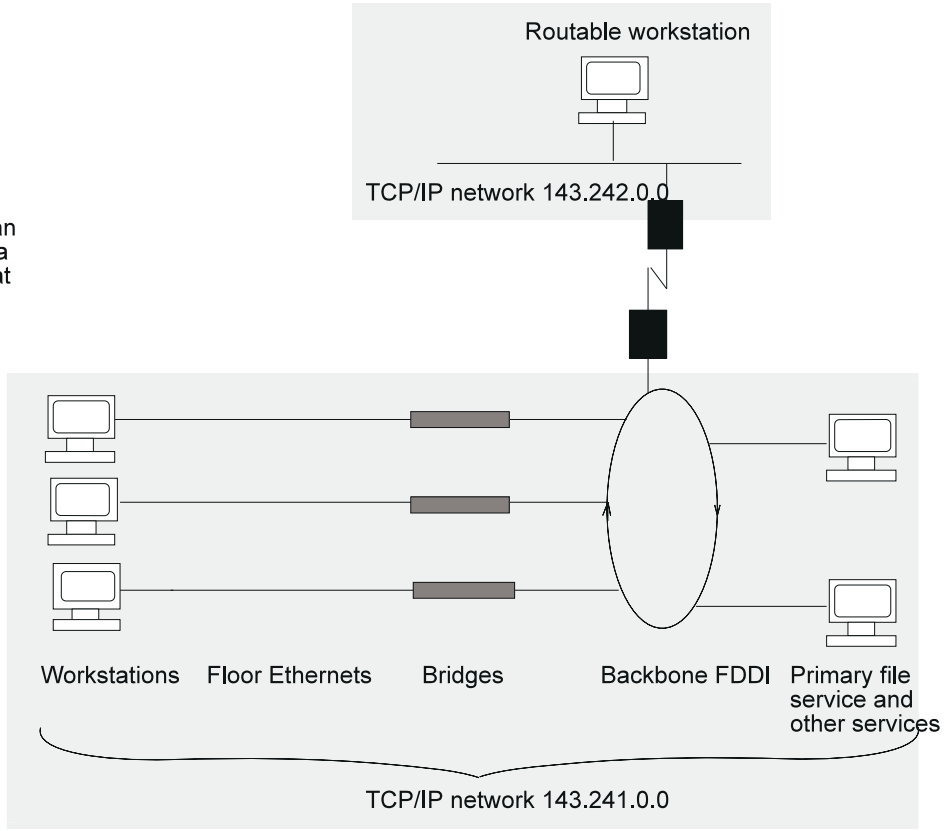


Figure 27. A routable workstation connected via a router to an IDS network.

It is not recommended, however, that the majority of IDS users be configured as routable workstations. The IDS protocols used by file servers and workstations (namely DSP and certain S411 operations) have been optimized for use on a LAN that offers highly reliable delivery of datagrams. The performance of a routable workstation will suffer if it is used across slow or error-prone routers, or if the IDS servers are burdened with too many routable workstations.

Expanding Your Network with Realms

Realms let you expand your IDS network to have almost unlimited numbers of IDS file services and their associated components coexisting simultaneously on the same network.

IDS resources for each realm are maintained as a logical group and must include at least a primary file service, a directory service, and an asset manager. Other services and workstations contribute functionality to the realm.

Multiple realms can exist within a single IDS network. An internal component, the inter-realm monitor, unifies separate realms into a distributed IDS system. The inter-realm

monitor keeps track of the realms through the IDS routing table. The realm information is transmitted periodically to other realms, both local and remote.

Realm Behavior

The existence of realms in an IDS internetwork is transparent to IDS users, who need have no knowledge of the underlying physical network or IDS infrastructure. Instead of a network name being assigned to the entire IDS network, each realm has its own name. Realms behave exactly like separate networks, which means that, to users, they look just like a remote network. The addressing scheme for sending mail is the same as that used between networks. For example, John, a user on the *Marketing* realm, would have the electronic mail address john:marketing. Figure 28 shows the address portion of an IDS envelope.

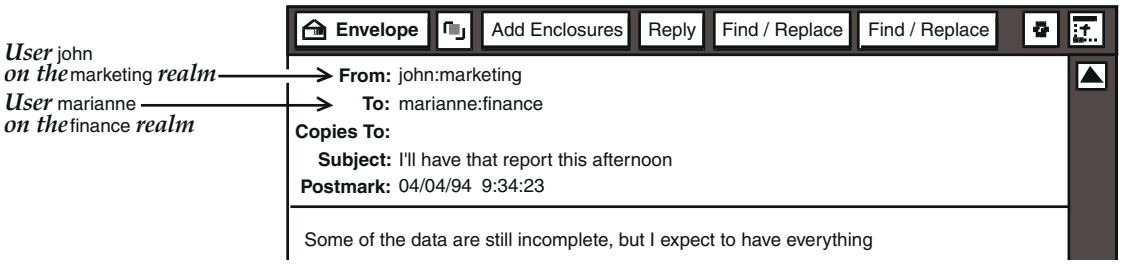


Figure 28. IDS envelope with user addresses

Realms and Connective Devices: You cannot have a router within the boundary of a single IDS network or realm. By placing a router between two nodes, you create two networks, each of which must have its own primary file service. Figure 29 on page 91 shows a router connecting two realms that reside on different networks.

Each of the realms on these two networks is equally accessible by other realms on the same two networks. The router is providing connectivity at the network level.

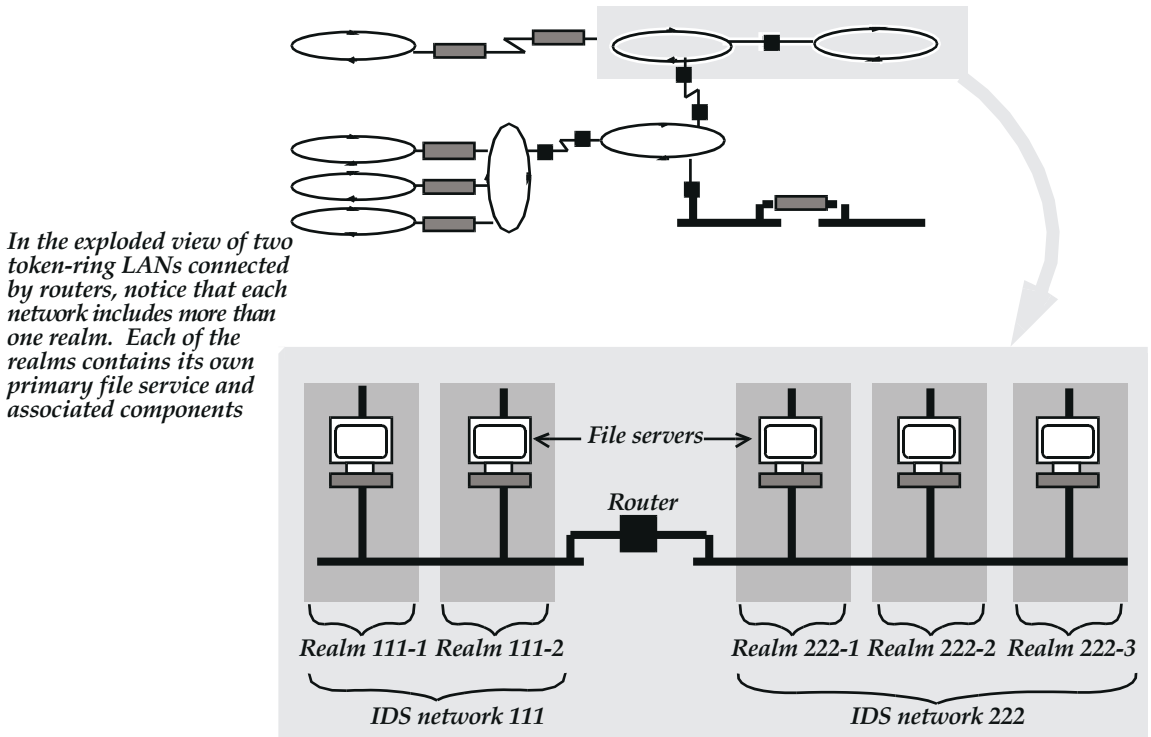


Figure 29. Internetwork router providing connectivity between realms

Realms separate large IDS networks into collections of smaller, more manageable groups of resources, all of which can reside on the same large, bridged network and use the same network number. A realm must reside on one network; it cannot cross a network boundary.

It is possible that workstations on one LAN segment might actually belong to a realm whose file service is on another LAN segment. This can be implemented either by using routable workstations or by requiring the use of a bridge within the realm boundary. For example, you might find that you have many IDS users on a LAN segment other than the one to which the rest of the work group is connected, thereby making a bridge desirable. If the number of remote users is small and bridging is not feasible, configuring these IDS users as remote workstation might be preferable.

Through the bridge, the remote user has access to the work group's primary file service. In such a configuration, the bridge is between the workstation and the primary file service; the bridge can be either local or remote.

When planning for bridges in your IDS network topology, consider that bridges used for remote connections must be able to support a line speed of at least 56 KB. Line speeds of fractional-T1, T1, or faster might be required. IBM recommends using the highest line speed you can afford.

When remote bridges are used in your IDS network topology, the remote line speed can be a limiting factor in bridge performance. The line speed limits the throughput of the bridge to a fixed maximum value. Any data in excess of that value must be buffered by the bridge to wait for processing.

If the network environment is token-ring, the bridges must be source routing bridges or source routing transparent bridges.

If the network environment is Ethernet, the bridge must support transparent routing with STA enabled.

Integrating IDS into Existing Networks

IDS can be (and often is) easily integrated into a variety of existing network environments, many of which run multiple protocols. IDS can run or coexist with other applications on the same workstation. Regardless of whether you run a single-protocol or a multiprotocol environment, the key to understanding how to integrate IDS into your network is to know the:

Type of network adapter cards connecting your systems to the network

Driver that enables the system to access the network interface card (NIC)

Software and protocols used on your network

Protocol standard compliance of the network software and interface card (also called a network adapter card)

The most basic requirement is that you must know the mechanism your systems use to access the network. To illustrate network access, Figure 30 shows a stack of network-access (or transport) components, as required in every system connected to a network.

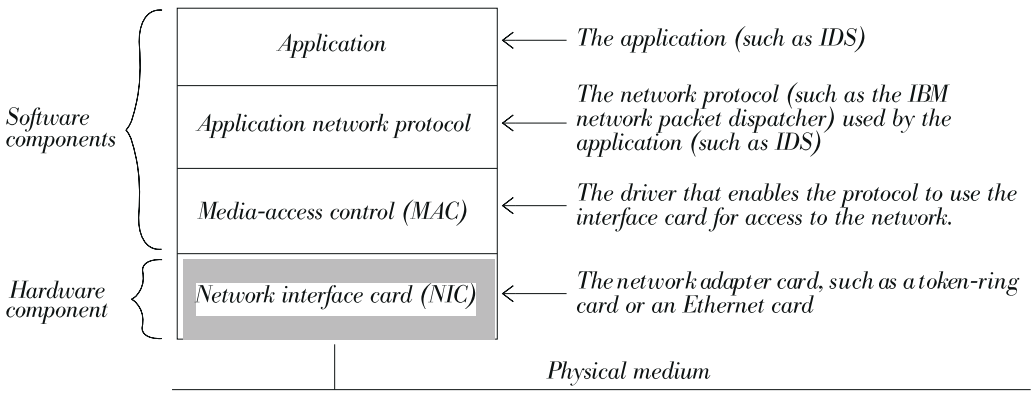


Figure 30. Network-access components

The components that enable network access typically comply with one of two standards:

Network Driver Interface Specification (NDIS), developed by 3Com and Microsoft

Open Data-Link Interface (ODI), developed by Novell

Network adapter cards normally are distributed with a diskette, which contains a number of drivers that allow the cards to be used in a variety of network environments. The standard with which your network-access components comply determines how you incorporate IDS into your network. IBM and Novell supply the drivers to vendors of network adapter cards so that you can enable coexistence between the two standards within the same network.

Adding IDS to a Multiprotocol Environment

IDS runs quite successfully in multiprotocol environments with such protocols as IPX/SPX, TCP/IP, NETBIOS, DECnet, and LocalTalk. If you are already running multiple protocols, then you have previously configured routers and bridges to deal with each of the protocols.

For example, if you have applications that are maintained on separate networks in different cities, their networks would be organized in different ways, but they would all make use of the same long-distance connections. Some traffic could be bridged, some traffic could be routed, and some traffic could be routed over the same connections.

Adding IDS to this network should not pose a problem. As with adding any other application to an existing environment, you should examine your connections and make certain you are using them as efficiently as possible.

For example, if you plan to bridge IDS over a 56-KB line between Seattle and San Francisco, you might want to reconsider your network design and increase the line speed over that particular long-distance connection; bridged traffic could cause network congestion at that location.

The presence of a bridge would imply that routable workstations could access a file service over the 56-KB connection. Because bridge traffic can add extra traffic to the connection, it would appear to remote users that IDS functions were slow, when, in fact, heavy use of the 56-KB connection would cause slow responses.

Evaluating Your Environment

Before making final decisions about the topology of your network, do some long-range planning and evaluation of the growth potential of your network and user needs. Here are a few points to consider during your planning process.

What type of workstation hardware are you currently using?

IDS provides support for workstations that are similar to IBM Personal System/2 (PS/2) 486 computers. IBM recommends that personal computers used for IDS

services be equivalent to a 486 workstation or better and compatible with the PS/2 486 workstation. When planning your installation, ensure that you have sufficient memory and disk space in all of your machines.

What is the operating system installed on the workstations?

IDS requires OS/2 Warp for workstation on which the developer's desktop has been installed. If you have workstations that run other operating systems, you must install OS/2.

Do you have a LAN already installed?

If you have a LAN already installed, you probably want to maintain your existing configuration when adding IDS to your LAN. IDS works equally well on Ethernet and token-ring LANs and can coexist with network operating systems such as Novell's NetWare, IBM's LAN Server, Banyan System's Banyan VINES, and Microsoft's LAN Manager.

How much traffic does your network currently support?

If your network is already heavily loaded, any additional application, including IDS, will increase your network activity. You might find it beneficial to segment your network with bridges or break your single network into one or more independently functioning networks.

As you add new IDS users, you might want to break your single IDS network into two or more IDS realms to maintain the best performance. Adding a second realm requires additional hardware for the IDS primary file service and other services, but can substantially improve response time.

How much growth do you anticipate?

If you expect your IDS network to grow, either due to an increase in the number of users or due to increased activity, it might be more cost-effective to plan for that growth now, while you are making decisions about machines' processor type and speed, memory and disk capacity, and network topology. A key decision is whether to install a single LAN or multiple LANs. If you decide to develop a single LAN, realize that at some point in the future you will probably need to add additional, separate realms to accommodate growth.

What physical medium do you plan to use?

While IDS supports both Ethernet and token-ring networks, mixing segments with different media types on a single IDS network is not supported. If you need to support both types of media within your IDS installation, the media must be maintained as separate networks, each with its own primary file service. Connectivity between the networks can then be provided by routers.

What type of long-distance media do you plan to use and what are the transmission speeds?

If, for example, you are using X.25 and have a bridged network, you need to consider the potential amount of broadcast traffic inherent in bridged environments. Most vendors charge by the packet (or kilopacket). A leased line might be more economical.

You will not find one correct solution for any situation. Try to avoid making decisions based only on current needs. Planning now for later growth in the network will make expansions and upgrades easier and less costly.

Glossary

access key. A code number, assigned by the system administrator to a user or a group of users, that can be used to restrict access to an IDS icon.

asset. An IDS service or tool. An asset can be for a set of desktop tools; a service, such as a mail service or database gateway service; or a database-access session.

asset management. Identification and distribution of purchased IDS features, services, and tools licensed for use.

auxiliary file service. Any file service other than the primary file service. Each auxiliary file service is associated with a primary file service.

batch. An accumulation of data to be processed.

block. A fixed number of consecutive bytes that are read, written, or transmitted as a group. an IDS disk block is 1024 bytes.

broadcast. Simultaneous transmission of data to more than one destination.

capsule. A tool for building an automated processing sequence using icons that represent IDS tools and PC applications.

capsule service. A tool that allows scheduled batch execution of capsule applications as an alternative to running the application directly on the desktop.

cluster. A set of execution engines. A service such as Capsule Services can have several clusters in different computers, but each cluster is in a single computer.

cluster manager. A process used by certain services, such as Capsule Services, to control one cluster, under direction from a service manager; the service manager can control several cluster managers in different computers.

container. An icon, such as the Folder and File Drawer icons, that can hold other icons.

cross-server backup. A backup from a disk on an IDS file server to a tape drive on another file server.

database administrator (DBA). The person who issues administrative instructions to a database service. The DBA defines the data tables used by data access tools, monitors database performance, and assigns user access.

DBA. Database administrator.

developer's desktop. The IDS interface primary used to develop applications, and is also used to access and run IDS services; administrators use the developer's desktop to manage services and assets for the realm.

DLL. Dynamic link library.

dynamic link library (DLL). Program code that is loaded from the file service to the desktop only when needed. Each DLL is a component of one or several tools or services.

Envelope. A tool used to create messages and to send messages and icons to other users.

Ethernet. A type of local area network used for IDS connections. An Ethernet network uses a bus topology (all devices are connected to a single cable). An Ethernet network can include any of several kinds of physical transmission media.

exception condition. An abnormal situation or illegal action that may arise during program execution and cause a deviation from the normal execution sequence. The 911 error reporting facility documents exception conditions detected by the Intelligent Decision Server and OS/2.

exception handler. A programming language facility that exists to recognize, define, and deal with exception conditions.

execution engine. A process used by certain services, such as Capsule Services, to execute specific actions under the control of a service manager through a cluster manager.

file descriptors.

file drawer. A container, created or renamed by the system administrator, that can be shared among desktops. A file drawer typically contains folders.

file service. In IDS, a software process that manages disk storage of the system software and user data.

© Copyright IBM Corp. 1996

file service volume. A virtual disk drive, similar in function to a hard disk partition, associated with a specific file server.

internetwork. Two or more local area networks (LANs) interconnected for exchange of data.

irrecoverable error. An error that causes further execution to be meaningless, impractical, or possibly damaging to data.

LAN. Local area network.

local area network (LAN). A data communications network, spanning a limited geographical area, in which serial transmission is used for direct communication among computers or other devices.

local network. The network to which a specified user or resource is directly connected.

log. A collection of messages or other information that is stored for data collection or troubleshooting purposes.

mail service. A service that controls the exchange of envelopes within IDS.

Mail Tray. An IDS icon where envelopes are mailed or received by being relayed through the mail service.

message bar. The rectangular area along the bottom of the desktop, where advisory or error messages are displayed.

network. A set of desktops, servers, and other devices connected together for the interchange of information.

Network Diagnostics tool. A tool that allows you to find and diagnose problems on the network.

911. The IDS error reporting facility that documents irrecoverable errors.

911 log file. A file containing error reports generated by the 911 error-reporting facility. The active 911 log file is always the system error log file. An inactive 911 log file is incapable of receiving new error reports.

node. A workstation that has been registered to the asset manager and, therefore, can have assets assigned to it.

primary file server name. The name of the primary file server in a realm. The default name is based on the machine name of the primary file server

primary file service volume. The file service containing the IDS system disk and software.

print formatter. A process within the printing service that translates an icon into a formatted file.

printer host. A computer on the LAN that has a printer attached to it.

printing queue. A request queue for a printer. It is a directory where icons are copied to await the attention of the printing service.

printing service. A service that controls the formatting, queuing, and printing of printable objects.

realm. A logical grouping of IDS services that includes a primary file service. The same network can contain multiple realms, and therefore multiple primary file servers. Realms are identified by the realm number and realm name; the name and number for a ream are specified when the primary file service is installed, and the defaults are based on the TCP/IP address of the primary file server.

realm name. The realm name of the primary file server in the realm. See primary file server name.

realm number. Uniquely identifies the one realm from another in a network, and is set when the primary file server is installed. The default number is the last segment of the server's TCP/IP address.

remote network. A network other than the local network, but which is accessible to the local network by some means.

RIP. Routing-information protocol.

router. In internetwork routing, a device that connects two separate networks. Routers function at the network layer of the OSI model and use network addresses to deliver packets.

routing table. A table maintained by internetwork routers. Each router uses the information in a routing table to forward packets from one connected segment to another.

satellite network. An IDS LAN that does not include a gateway. Such a system must connect to a fully configured LAN and use that LAN's gateways to have access to relational databases and other host services.

secondary file service. Auxiliary file service.

server. The computer in which a service runs.

service. A software process that provides facilities to other parts of IDS, such as a file service, a mail service, a mail gateway service, and a data access service.

service manager. A process used by certain services, such as Capsule Service, to control one or more sets of execution engines through one or more cluster managers.

stack dump. A printed record of the area in memory that stores temporary register information, parameters, and return addresses of subroutines.

subnet. A part of a TCP/IP network that is identified by a portion of the Internet address.

subnet mask. A bit template that identifies the bits of the host address to the TCP/IP protocol code that are used for routing to specific subnets.

system administrator. In IDS, the person who is responsible for maintaining and configuring IDS, including its desktops, servers, and network.

system error log. The central location in the IDS file system for storing 911 error reports.

thread. The smallest unit of execution within a process that is not identifiable outside its parent process.

token-ring network. A network that uses a ring topology, in which tokens are passed in a circuit from node to node. A node that is ready to send can capture the token and insert data for transmission.

tool. A developer's desktop program, such as Text, Reporter, or Query. Every tool is represented by an icon.

tool set. A set of tools that are bundled together as a single asset that can be assigned to a user or a node. The end-user tool sets are named Executive, Explorer Plus, and Expert Plus.

transformer. A tool that can be used to perform various types of data manipulation either interactively or in a Capsule application.

volume. A virtual disk drive, similar in function to a hard disk partition.

IDS Publications

This section lists IDS publications, including order numbers. To order copies of the books listed here, or to get more information about a book, see your IBM representative.

General Publications

Getting Started with the Intelligent Decision Server (SC26-8892)

Working with the Intelligent Decision Server (SC26-8893)

Installation, Configuration, and Administration Publications

Installing IDS LAN Components (GC26-8877)

System Administration Guide and Reference (SC26-8890)

Messages and Codes (GC26-8878)

Database Gateway Services Publications

Installing Database Gateway Services for UNIX Environments (GC26-8884)

Configuring and Administering Database Gateway Services (GC26-8885)

Administering Databases with IDS (SC26-8891)

Host Services Publications

Planning MVS Host-to-LAN Connectivity (GC26-8880)

Installing Host Services and Configuring Host-to-LAN Communications for MVS (GC26-8881)

Administering Host Services for MVS: DB2 and Cooperative Application Services (GC26-8882)

Developing Applications with Cooperative Application Services (GC26-8883)

Configuring and Administering Mail Gateway Services (GC26-8923)

Open Data Access Service Publications

Developing Applications with Open Data Access Service (SC26-8888)

Data Access Tools Publications

Browser User's Guide (SC26-8900)

Data Entry User's Guide (SC26-8897)

DBA Tool User's Guide (SC26-8894)

SQL Entry User's Guide (SC26-8898)

Data Analysis Tools Publications

BASIC Tool User's Guide (SC26-8908)

Query User's Guide (SC26-8901)

Spreadsheet User's Guide (SC26-8904)

Presentation Tools Publications

Layout User's Guide (SC26-8902)

Plot User's Guide (SC26-8905)

Reporter User's Guide (SC26-8903)

Text User's Guide (SC26-8896)

Application Development Tools Publications

© Copyright IBM Corp. 1996

Transformers Guide (SC26-8907)
Capsule User's Guide (SC26-8906)
Forms Design User's Guide (SC26-8899)
Interacting with PC Applications (SC26-8895)
Installing and Configuring IDS Open Clients (GC26-8889)

Index

A

active service status 60
Add Service
  button 60
  menu 59
adding
  capsule service 53
  capsule service execution engine 54
  capsule service manager 53
  conversion service 56
  conversion service execution engine 58
  conversion service manager 56
  gateway 66
  IDS services to a server or node 42
  IDS to multiprotocol environments 93
  mail service 42
  ODAS 29
  OS/2 database gateway service 61
  print service 47
  print service execution engine 49
  print service manager 47
  printer host 51
  remote mail gateway service 59
  services 29
  users and tools 39
addresses, registering for nodes 61
administration
  IDS system 72
  LAN 72
Administrator Icons file drawer 59
Advanced Program-to-Program Communications 66
aliases, creating for gateways 70
anticipating growth in networks 95
APPC connections 65, 66
asset 1, 40
  assignable 4
  management service 2
Asset Configuration window 60
Asset Management window
  Nodes page 37, 60, 61
  User Details page 41
asset manager, opening 42
Asset Mgmt
  Gateway Type Details window 64
  Service Details window 63
assets 40
assigning tool assets to a registered node 40
assigning tools to a user ID 40
Auto Configuration field 65
Auto Restart field 61, 64
Auto Start field 60, 63
automatic route determination 78
auxiliary file server 1
  initializing 19
  installing 17

B

backbone ring 86
bridge
  compared with router 81
  definition 77
  for remote connection 91
  function of 75
  local 79
  remote 79
  segmenting LANs with 78
  source route transparent 79
  source-routing 92
  standard 82
  transparent 79
  when needed 85, 86
bridge router
  router 80
brouter 80
Browser data-access tool 70
buttons
  Add Service 60, 63
  Register Service Information 61, 64

C

capsule service 3
  adding 53
  adding execution engine 54
  adding manager 53
collecting network details 7
command buttons
  Add Service 60
  Register Service Information 61
Communication Manager/2 66

© Copyright IBM Corp. 1996

communications management 73
configuring
  data access tools for database access 70
  database gateway service 65
  gateway 66
  gateway service 65
  mail service 45
  nodes and adding users and tools 36
  ODAS 28
  ODAS components 28
  ODAS server 32
connecting existing LANs 85
connective device
  bridge 75, 77
  brouter 80
  definition of 77
  repeater 77
  router 79
Consoles Available field 65
conversion service 3
  adding 56
  adding execution engine 58
  adding manager 56
  default naming convention used for 37, 61
creating an installation diskette for the developer's desktop 26
creating gateway aliases 70

D

data access tools for database access, configuring 70
data-access tools 70
  Browser 70
  DBA 70
  Forms Design 70
  Query 70
  Reporter 70
  SQL Entry 70
  SQL Input 70
data-center planning 73
database
  gateway service, configuring 65
  locating folders 70
  management 73
  other tasks 70
DB Gateways
  Gateway Details window 66, 68
  Service Info window 65
DB2 for OS/2 DRDA gateway 66
DB2 for OS/2 gateway 66
DB2 gateway 67
DBA data-access tool 70
DBS
  DB macro folder 71
  DB2 macro folder 68
  ORACLE7 macro folder 71
  OS/2 macro folder 71
  OS400 macro folder 68
  SQLDS macro folder 68, 71
  SYBASE macro folder 71
  Teradata macro folder 71
DBS - REDBRICK macro folder 71
DDCS/2 67
Default SID field 68
designing IDS environments 81
developer's desktop 3
  create installation diskette 26
  definition 1
  installing 24
  installing from the IDS CD-ROM 24
  starting 26
directory service 3
disk-service protocol (DSP) 83
disk-space requirements 8
Download Commit Count field 68
DSP 83
dynamic route determination 78
dynamic routing protocols 80

E

enabling coexistence 93
envelope, setting the lifetime 46
environment
  bridged 81
  evaluating 93
  routed 81
Ethernet bridge 92
Ethernet LANs 93
execution engine
  capsule service 54
  conversion service 58
  print service 49

F

fault isolation 78
fields
  Add Service 56

fields *(continued)*
Auto Restart 61, 64
Auto Start 60, 63
Locked Memory 60, 63
Parameter Values 61
Service Name 60
Service Status 60
User Name 67
file drawer, Administrator Icons 59
file service volume
initializing additional 16
initializing auxiliary 19
filtering 79
Forms Design data-access tool 70
forwarding 79
fractional T1 91

G

gateway 81
adding 66
configuring 66
creating aliases 70
DB2 and MVS CAS 67
ID field 68
name field 68
ORACLE 68
OS/2 database 3
SYBASE and Red Brick 68
type field 68
gateway service, OS/2 database 61

H

hardware requirements 7
host administration 73

I

Icon Options window 67
IDS assignable assets 4
IDS network topology 91
IDS realms 89
IDS system administration 72
IDs, registering 39
inactive service status 60
initializing
additional file service volumes 16
auxiliary file server 17
auxiliary file service volumes 19
initializing *(continued)*
primary file server 14
installation
preparing for 7
stopping 14
installing
auxiliary file server 17
developer's desktop 24
CD-ROM 24
from diskette 26
ODAS administration and client test applications on WIN-OS/2 and Windows 3.1 30
ODAS clients 33
ODAS components 28
primary server 11
installing other services 21
capsule 21
conversion 21
mail 21
ODAS 21
OS/2 database gateway 21
print 21
printer host 21
remote mail gateway 21
integrating IDS into existing networks 92
Intelligent Decision Server
introduction 1
understanding the structure 1
interface, mail 45
Interfaces File Directory field 68
intermediate system-to-intermediate-system (IS-IS) 80
internetworks 76
introduction to the Intelligent Decision Server 1
IS-IS 80

L

LAN Manager (Microsoft) 93
LAN Server (IBM) 93
learned addresses 78
learned path 79
learning source addresses 78
lifetime, setting up the envelope 46
linking LAN segments 85
local bridge 79, 80
local user ID 67
locating the database folders 70
Locked Memory field 60, 63
logging on to the ODAS administration application 30

logging onto the primary file server 15
long-distance medium 95
loops, managing 78
LU Alias field 68

M

Macro Folder field 68
macro folders
  DBS - DB2 68
  DBS - OS400 68
  DBS - SQLDS 68
mail
  addressing scheme 90
  interface 45
  realm names 90
  sending 90
mail service 3
  adding 42
  configuring 45
  remote gateway 59
manager
  capsule service 53
  conversion service 56
  print service 47
managing loops 78
Maximum Console Sessions field 65
Maximum Database Sessions field 65
Maximum Number of Sessions field 68
message forwarding 79, 80
Mode Name field 68
multiprotocol environments, adding IDS to 93
MVS CAS gateway 66, 67

N

NETBIOS 79, 93
NetWare (Novell) 93
network 1
  access components 92
  adapter cards 92
  administration 72
  collecting details 7
  database management 73
  definition of 72, 74
  design
    elements of 73
    planning the connections 81
  details 7
  elements of 73, 76
network *(continued)*
  expanding 85
  growth of 95
  IDS sample configuration 2
  interface card 92
  planning
    communications management 73
    data-center management 73
    security administration 73
    skills required 72
    systems programming 73
  remote 75
  routers in 87
  segments 74, 86
  topology of 74
  topology, IDS 91
  traffic on 93
  troubleshooting 72
NIC 92
node 1
  adding services to 42
  assigning tools to 40
  registering workstation as 37
Novell NetWare 93

O

ODAS
  adding 29
  administration and test applications 28
  administration application, resizing columns 32
  administration interface 31
  client platforms 28
  configuring the server 32
  installing administration and client test applications on WIN-OS/2 and Windows 3.1 30
  installing and configuring components 28
  installing clients 33
    on OS/2 33
    on WIN-OS/2 or Windows 3.1 33
    on Windows 95 34
  logging on to the administration application 30
  server configuration 32
  service 3, 28
  starting 30
  testing the connection to Windows 34
open shortest path first (OSPF) 80
opening the asset manager 42
opening the SA tool 36

operating systems 93
ORACLE gateway 68
Oracle Home Directory field 68
OS/2 database gateway service 3
  adding 61
OSPF 80
other database tasks 70
other IDS services 1
  installing 21

P

packets
  filtering 79
  forwarding 79
Parameter Values fields 61
physical medium 74
planning
  configure nodes 36
  nodes, add 36
  users, add 36
Pool field 68
post office, setting the path 46
Pre-Start field 68
preparing for installation 7
previewing IDS services 2
primary file server 1
  initializing 14
  installing 11
print service 4
  adding 47
  adding execution engine 49
  adding manager 47
printer host 4
  adding 51
Program Manager window 30
protocol
  disk-service protocol (DSP) 83
  IPX/SPX 93
  IS-IS 80
  OSPF 80
  RIP 80
  S411 83, 84
  SPP 84
  standard compliance with 92
  TCP/IP 81, 82, 83, 84, 85, 88, 93

Q

Query data-access tool 70

R

RAM requirements 8
RDBMS 66
realm 1
  behavior of 90
  connective device between 90
  connective devices within 90
  definition 89
  in IDS networks 89
  segmenting IDS networks 91
Red Brick gateway 68
redundant paths, managing 78
Register Service Information button 61, 64
registering user IDs 39
registering workstations as nodes 37
remote
  bridge 79, 80
  bridge, line speed 92
  mail gateway service 4
  mail gateway service, adding 59
  network 75
  user ID 67
removing IDS 14
repeater 77
Reporter data-access tool 70
requirements
  disk-space 8
  hardware 7
  RAM 8
  software 10
resizing columns, ODAS 32
resource control 81
RIP 80
routable desktop 81, 83, 84, 88
routable workstation 88
route determination 78
router
  definition 76
  local 80
  remote 80
  use of 79
  when to use 88
  with IDS networks 87
routing
  dynamic 80

routing *(continued)*
source routing 79
source-routing transparent 79
static 80
table, gathering information for 80
routing-information protocol (RIP) 80

S

S411 83, 84
SA tool
opening 36
window 37
sample IDS network 2
security 81
security administration 73
segmenting LANs with bridges 78
segments of networks
creating 74
joining by a bridge 75
server
adding services to 42
auxiliary 1, 3, 17
initializing file service volumes 19
installing 17
primary 1
initializing 14
installing 11
logging onto 15
primary file 3
service
ODAS 3
remote mail gateway 4
status field 60
Service Details window 53, 55
services 1
adding to a server or node 42
asset management 1, 2
auxiliary file 3
capsule 3
conversion 3
developer's desktop 1, 3
directory 1, 3
file service volumes 3
mail 3
OS/2 database gateway 3
other 1
previewing 2
primary file 1, 3
print 4
services *(continued)*
printer host 4
Sessions Available field 65
setting the envelope lifetime 46
setting the post office path 46
skills
IDS host administration 73
network troubleshooting 72
SNA 66
software requirements 10
Software Version field 65
source routing
bridge 92
protocol type 79
source-routing transparent (SRT) 79
spanning tree algorithm (STA) 78, 79, 82
spanning tree, defining your own 78
SQL Entry data-access tool 70
SQL Input data-access tool 70
SRT 79
STA 78, 92
starting ODAS 28, 30
starting the IDS developer's diskette 26
static routing 80
stopping the IDS installation 14
SYBASE gateway 68
system administration 72
Systems Network Architecture 66
systems programming 73

T

T1 91
Target Server field 68
tasks, database 70
TCP/IP 81, 82, 83, 84, 85, 88
testing the connection to ODAS on Windows 34
token ring
backbone 86
bridge 92
token-ring LANs 93
tools 1
assigning to a registered node 40
assigning to a user ID 40
topology 74, 91
Transmission Control Protocol/Internet Protocol 81, 82, 83, 84, 85, 88
transparent bridges 79
transparent routing 79, 92

U

understanding the IDS structure 1
UNIX 64
user ID
  assigning tools to 40
  registering 39
User Name field 67
using the mail interface 45

V

vendor 60
volumes, file service 3

W

when to use bridges 85, 86
windows
  Asset Configuration 60
  Asset Management
    Nodes page 37, 60, 61
    User Details page 41
  Asset Mgmt - Gateway Type Details 64
  Asset Mgmt - Service Details 63
  DB Gateway - Gateway Details 68
  DB Gateways - Gateway Details 66
  DB Gateways - Service Info 65
  Program Manager 30
  Service Details 53, 55
workstation 93
  registering as node 37

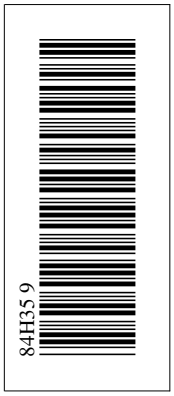
X

X.25 95

IBM®

Part Number: 84H3509

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.



GC26-8877-