MetaFrame Solutions Guide

Citrix® MetaFrame Application Server for Windows NT 4.0, Terminal Server Edition

Version 1.8

Citrix Systems, Inc.

Document No. mf.solg.sp1.adm

Contents

Welcome

The *Citrix MetaFrame Solutions Guide* is designed to:

- Show you some of the many ways MetaFrame Application Server for Windows can be used to meet common requirements
- List some of the products that have been found to be compatible with MetaFrame
- Help you select the proper hardware and software components to build a system running MetaFrame with Windows NT Server, Terminal Server Edition

Who Should Use this Guide

This guide is designed to help administrators and resellers with the installation, setup, and operation of MetaFrame.

How to Use this Guide

The chapters of the *MetaFrame Solutions Guide* roughly reflect the phases you go through when you deploy a MetaFrame solution:

Chapter	Contents
Chapter 1, “What Is MetaFrame?”	Introduces you to the components of Citrix’ server-based computing solution and provides ideas for planning your deployment.
Chapter 2, “Deploying the MetaFrame Servers and ICA Clients”	Provides installation tips, system configuration guidelines, and information about popular third-party hardware devices.
Chapter 3, “Installing Applications”	Describes the special requirements for multi-user applications and the installation of many popular third-party software applications.
Chapter 4, “Securing the Enterprise”	Describes techniques and third-party applications that you can use to secure your systems.
Chapter 5, “Connecting to the Web”	Introduces Citrix Web Computing and details supported Web browser and server software.
Chapter 6, “Maintaining MetaFrame”	Contains tips about fine tuning MetaFrame systems and instructions for applying service packs and hotfixes.
Chapter 7, “Troubleshooting the System”	Gives step-by-step instructions for diagnosing problems on MetaFrame servers.

Note The products listed in this guide have been tested and found to be compatible with MetaFrame. Many other products work well with MetaFrame but Citrix cannot guarantee the compatibility of untested products.

Because MetaFrame runs on Windows NT Server, Terminal Server Edition, most Windows NT-compatible applications can be expected to work. Review the application notes in Chapter 3 for detailed application integration tips and techniques.

Some application notes in this guide were supplied by third parties and are noted as such.

Disclaimer

This guide is not intended to be a comprehensive listing of all the third-party components that can be used with Citrix MetaFrame. MetaFrame supports industry-standard hardware and software; therefore, many options exist far beyond those contained in this guide.

Citrix makes no claim as to the suitability of products mentioned in this guide to fit your needs. All third-party products may be available through multiple suppliers. The products and suppliers listed are for reference purposes only and are subject to change without notice.

Not all combinations of hardware and software listed in this guide have been tested. When you encounter a compatibility problem, you should first contact the software vendor for technical support and then contact your reseller if the vendor is not able to help you.

Conventions

The following conventional terms, text formats, and symbols are used throughout the printed documentation.

Convention	Meaning
Bold	Indicates boxes and buttons, column headings, command-line commands and options, icons, dialog box titles, lists, menu names, tabs, user input, and menu commands.
Italic	Indicates a placeholder for information or parameters that you must provide. For example, if the procedure asks you to type *filename*, you must type the actual name of a file. Italic also indicates new terms and the titles of other books.
ALL UPPERCASE	Represents keyboard keys; for example, CTRL, ENTER, F2.
`Monospace`	Represents text displayed at the command prompt and text file contents.

Convention	Meaning
▶	Indicates a procedure.
▪	Indicates a list of related information, not procedural steps.
WTSRV or %SystemRoot%	Refers to the Terminal Server system tree. This can be \WTSRV, \WINNT, \WINDOWS, or whatever other directory name you specify when you install Terminal Server.
{braces}	Enclose required items in syntax statements. For example, **{ yes | no }** indicates that you must specify **yes** or **no** when using the command. Type only the information within the braces, not the braces themselves.
[brackets]	Enclose optional items in syntax statements. For example, [*password*] indicates that you can choose to type a *password* with the command. Type only the information within the brackets, not the brackets themselves.
| (vertical bar)	Stands for "or" and separates items within braces or brackets. For example, **{ /hold | /release | /delete }** indicates that you must type **/hold** or **/release** or **/delete**.
… (ellipsis)	Indicates that you can repeat the previous item(s) in syntax statements. For example, **/route:***devicename*[,…] indicates that you can specify more than one device, putting commas between the device names.

Finding More Information About MetaFrame

Your MetaFrame package includes the following printed documentation:

- The CD liner notes includes an overview of the product, Citrix support information, and instructions for activating your Citrix software licenses.
- The *MetaFrame Administrator's Guide* tells administrators how to install, configure, and maintain MetaFrame servers.
- The *Citrix ICA Client Quick Reference Cards* give users step-by-step instructions for using the Citrix ICA Clients to connect to Citrix servers and run published applications.

Your MetaFrame software includes the following online documentation in WinHelp format in the MetaFrame Books Online:

- The *MetaFrame Solutions Guide* gives administrators detailed information about planning, deploying, and configuring server-based computing solutions using MetaFrame, the Citrix ICA Clients, and a wide variety of third-party hardware and software.
- The *Citrix ICA Client Administrator's Guides* tell administrators how to install, configure, and deploy the various ICA Clients to end-users.
- The online version of the *MetaFrame Administrator's Guide.*

▶ **To access *MetaFrame Books Online***

Click **Start**, point to **Programs**, then **MetaFrame Tools**, and click **MetaFrame Books Online**.

All of the documentation for MetaFrame is also available in Adobe PDF format in the documentation directory of your MetaFrame CD-ROM. Using the Adobe Acrobat Reader, you can view and search the documentation electronically or print it for easy reference. To download the Adobe Acrobat Reader for free, please go to Adobe's Web site at http:\\www.adobe.com.

Important Please consult the Readme.txt file in the root directory of your MetaFrame CD-ROM, for any last-minute updates, installation instructions, and corrections to the documentation.

Finding Information About Windows NT Server, Terminal Server Edition

Most Terminal Server compatibility guidelines can be applied to Citrix MetaFrame because MetaFrame is designed to run with Terminal Server. For example, MetaFrame supports the deployment of Win32, Win16, DOS, OS/2 1.x (text only), and POSIX applications. The MultiWin and ICA technologies included in MetaFrame extend the capabilities of Windows NT and, in some cases, require additional setup and configuration for best results with applications.

For Terminal Server compatibility information, see the following Microsoft resources:

- The Microsoft Web site, http://www.microsoft.com
- Microsoft Technet

Citrix on the World Wide Web

Citrix offers online Technical Support Services at http://www.citrix.com that include the following:

- Downloadable Citrix ICA Clients, available at http://download.citrix.com
- A Frequently Asked Questions page with answers to the most common technical issues
- An FTP server containing the latest service packs and hotfixes for download
- An Online Knowledge Base containing an extensive collection of technical articles, troubleshooting tips, and white papers

- Interactive online support forums
- The Citrix Developer Network (CDN) available at http://www.citrix.com/cdn

  This new, open enrollment membership program provides access to developer tool kits, technical information, and test programs for software and hardware vendors, system integrators, ICA licensees, and corporate IT developers who incorporate Citrix server-based computing solutions into their products.

Citrix Technical Support Bulletin Board Service

The Citrix Technical Support Bulletin Board Service is fully integrated with Citrix Online Technical Support Services. Customers without Web or e-mail access can dial in to the Citrix BBS at (954) 267-2590. Communication parameters are: no parity, 8 data bits, 1 stop bit, up to 28,800 baud.

Year 2000 Readiness

For a detailed description of the Year 2000 Readiness of Citrix products, see our Web site at http://www.citrix.com/misc/y2000.htm.

Citrix Sales Offices

Australia
Citrix Systems Australia Pty Ltd.
State Forest Building, Level 7
423 Pennant Hills Road
Pennant Hills, NSW 2120
Australia
Telephone: +61 2 9980-0800
Fax: +61-2-9980-6763
Internet URL: www.citrix.com.au

France
Citrix Systems SARL
7, Place de la Defense
92974 Paris, La Defense 4 Cedex
France
Telephone: +33-149-00-33-00
Fax: +33-149-00-33-01
Internet URL: www.eu.citrix.com

Germany
Citrix Systems GmbH
Am Soeldnermoos 17
85399 Hallbergmoos
Germany
Telephone: +49-811-8300-00
Fax: +49-811-8300-11
Internet URL: www.eu.citrix.com

Italy
Citrix Systems Italia
Via Giovanni da Udine, 34
20156 Milano
Italy
Telephone: +39-(0)2-38093613
Fax: +39-(0)2-38093305
Internet URL: www.eu.citrix.com

Japan
Citrix Systems Japan KK
Arco tower 16F, 1-8-1, Shimo-Meguro
Meguro, Tokyo, Japan153-0064
Telephone: +81-3-5434-0992
Fax: +81-3-5434-0986
Internet URL: www.citrix.com

UK
Citrix Systems UK Ltd.
Buckingham Court, Kingsmead Business Park
London Road, High Wycombe
Buckinghamshire, HP11 1JU
United Kingdom
Telephone: +44(0) 1494 6849-00
Fax: +44(0) 1494 6849-98
Internet URL: www.eu.citrix.com

United States
Citrix Systems, Inc.
6400 Northwest Sixth Way
Fort Lauderdale, FL 33309
Phone: (954) 267-3000
Fax: (954) 267-9319
BBS: (954) 267-2590
Internet URL: www.citrix.com

Readers Comments

We strive to provide you with accurate, clear, complete, and usable documentation for Citrix products. If you have any comments, corrections, or suggestions for improving our documentation, we would be happy to hear from you. You can email the authors at:

documentation@citrix.com

Please include the name and version number of the product and the title of the document in your email.

CHAPTER 1

What is MetaFrame?

This chapter gives you an executive summary of MetaFrame and describes:

- The challenges of deploying applications across the enterprise
- What server-based computing is
- The components of Citrix' server-based computing solution
- MetaFrame's features and benefits
- Citrix partnerships and compatibility
- Planning considerations for a MetaFrame solution

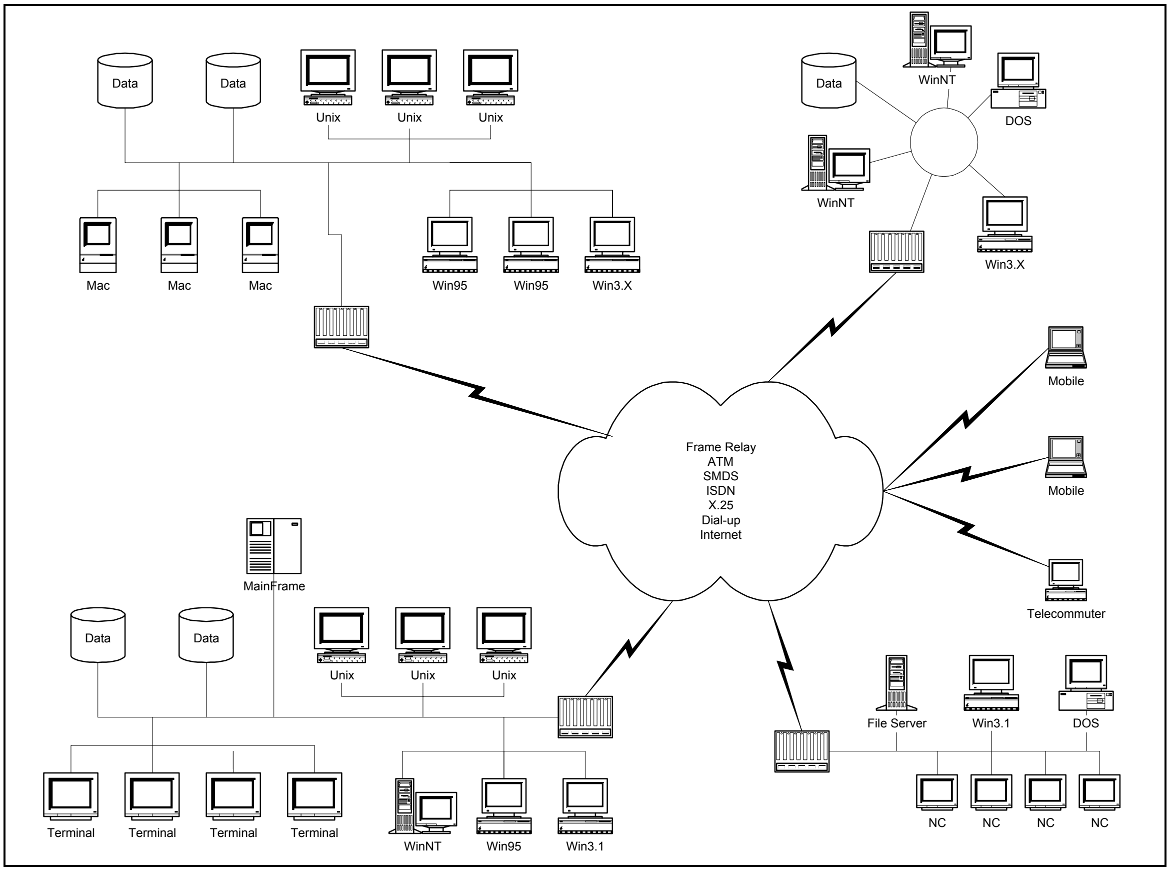
Enterprise Application Challenges

MIS managers face the daunting task of deploying client/server Windows applications across enterprise networks that can easily grow to regional, national, or global proportions. Unfortunately, traditional client/server technologies rarely rise to the enterprise-wide challenges faced by MIS. In fact, the established approaches usually hinder strategic application deployments by inflating costs, complicating management, and performing poorly.

Traditional client/server application architectures and the accompanying deployment models established by distributed PC-based LANs, remote control, and remote node technologies all fail to deliver fast, inexpensive, efficient application deployments. The problem is inherent to traditional client/server architecture, which emphasizes client-side computational power. In today's widely distributed enterprises, the client/server model breaks down as the client moves farther away from the server, yet is required to perform the same tasks as a local machine.

Organizations seeking to broadly deploy line-of-business applications across the enterprise face a diverse set of challenges associated with cost, management, and performance.

- **LAN-Locked Applications**. Most business applications, such as two-tier client/server, are designed for the LAN and are not optimized to run over high-latency phone or WAN connections that run 100 to 1000 times slower than a local segment.
- **New Users**. Today's corporate computing infrastructure is built for employees, not a company's prospects, customers, and suppliers.
- **Heterogeneous Clients**. Not everyone uses or needs a PC on the desktop. Some use non-Windows systems such as OS/2, UNIX, or Macintosh. Some need low-cost, fixed function devices, such as terminals. Others need new devices such as wireless tablets and personal digital assistants (PDAs).
- **Management**. Managing access (security), version control (maintenance), system configuration (moves, adds, deletes), and support (help desk) are very costly, particularly for distant users.



MIS rarely has the luxury of deploying mission-critical applications in a homogeneous environment, let alone from a centralized location. Instead, the enterprise network usually includes a widely-dispersed variety of servers, client workstations, and operating systems. A variety of wide area connections joins remote office LANs throughout the nation or the world. The user base can include from dozens to thousands of local, remote, mobile, and telecommuting users.

What is Server-Based Computing?

Server-based computing is a logical, efficient evolution of today's networking environments that gives organizations a way to extend resources, simplify application deployment and administration, and lower the total cost of application ownership.

With server-based computing, applications are deployed, managed, supported, and executed completely on a server. Client devices, whether "fat" or "thin," have instant access to business-critical applications on the server - without application rewrites or downloads. Because server-based computing works within the current computing infrastructure and standards, it is rapidly becoming the most reliable way to reduce the complexity and total cost of enterprise computing.

Server-based computing relies on three critical components:

- A **multiuser operating system** that allows multiple concurrent users to log on and run applications in separate, protected sessions on a single server.
- A **remote presentation services architecture** capable of separating the application's logic from its user interface, so that only keystrokes, mouse clicks, and screen updates travel the network.

  MetaFrame uses Citrix' ICA, which enables virtually any client device to access virtually any application over any type of network connection. Unlike the Network Computing (NC) architecture, server-based computing does not require applications to be downloaded to client devices. As a result, application performance is neither bandwidth- nor device-dependent.
- **Centralized application and client management**, which enables enterprises to overcome the critical application deployment challenges of management, access, performance, and security.

Citrix Server-Based Computing

Citrix' server-based computing solution consists of:

- MetaFrame Application Server for Windows
- The Citrix ICA Clients
- Citrix Services

MetaFrame Application Server for Windows

MetaFrame Application Server for Windows incorporates Citrix' Independent Computing Architecture (ICA) protocol and provides a high-performance, cost-effective, and secure way to deploy, manage, and access business-critical applications throughout an enterprise - regardless of client device or network connection. With this innovative software, enterprises can:

- Bring server-based computing to heterogeneous computing environments and provide access to the most powerful 32-bit Windows-based applications, regardless of client hardware, operating platform, network connection, or protocol
- Offer enterprise-caliber server and client management that allows IS professionals to scale, deploy, and support applications from a single location
- Provide a seamless user experience at the desktop, delivering a wide variety of applications with exceptional performance that is independent of bandwidth

Citrix MetaFrame brings server-based computing to the entire enterprise - including headquarters, branch offices, and remote users - and extends the capabilities of Windows Terminal Server for departmental and workgroup environments. It offers IS professionals a cost-effective way to deploy, manage, and support applications from a single point. It provides universal application access from virtually any type of client device. It ensures bandwidth-independent performance with any type of network protocol or connection, and offers unique features for enhanced application management and security.

MetaFrame provides:

- **Support for heterogeneous computing environments**
  While Terminal Server supports Windows-based devices and IP-based connections, MetaFrame goes further, providing universal access to Windows-based applications regardless of client hardware, operating platform, network connection, or LAN protocol. As a result, organizations can keep their existing infrastructures while still deploying the most advanced 32-bit Windows-based applications across the enterprise.
- **Enterprise-scale management**
  Organizations building enterprise computing solutions around Terminal Server will benefit from the robust enterprise management tools of MetaFrame, including increased system scalability and simplified support of multiple applications for thousands of users enterprise-wide. Servers can be added easily and transparently without touching user desktops. Applications can be deployed and administered across multiple servers from a single location.

Not only does MetaFrame provide the ability to train users of heterogeneous clients on the latest Windows-based applications, it also allows administrators to control user access to client resources, thereby maintaining system integrity and network performance. To secure corporate information, MetaFrame keeps all vital data and applications on the server, allowing it to be accessed without downloading.

- **Seamless desktop integration**
  MetaFrame goes beyond Terminal Server by offering increased functionality and enhanced user experience, including complete access to all local system resources, such as full 16-bit stereo audio, local drives, COM ports, and local printers. Applications running remotely from the server look, feel, and perform as though they are running locally. With MetaFrame, users enjoy a comfort level that eliminates the need for training and increases user productivity.

The Citrix ICA Clients

Citrix is continually expanding its offering of ICA Clients to support the growing need for access to Citrix servers from almost any type of device. Among the supported ICA Client platforms are:

32-bit Windows The Citrix ICA Client for Win32 supports Windows 95, Windows 98, and Windows NT, and offers features that take advantage of the robust capabilities of the client machine. The Program Neighborhood provides users customized views of applications published throughout the enterprise that they are authorized to access.

16-bit Windows The Citrix ICA Client for Win16 supports Windows 3.1 and Windows for Workgroups 3.11, leveraging older, less powerful Windows PCs and providing their users access to 32-bit applications.

DOS The Citrix ICA Client for DOS includes versions for both 16- and 32-bit extended DOS machines. The 32-bit version provides more features than the 16-bit version, while requiring less conventional memory.

Web plug-ins The Citrix ICA Windows Web Clients are available as ActiveX and Netscape plug-ins that Web masters can incorporate into Web pages for Internet or Intranet access to applications running on Citrix servers.

Java The Citrix ICA Client for Java can run in both applet and application mode. As an applet, the Java client can be embedded in a Web page, like the Web plug-in clients. As an application the Java client supports client platforms that include a resident Java virtual machine (JVM).

Macintosh The Citrix ICA Client for Macintosh supports Macintosh PCs running System 7.1 or later and extends remote application access to Macintosh users.

UNIX The Citrix ICA Client for UNIX includes versions for Linux, SCO, Digital UNIX, HP-UX, IBM AIX, SGI IRIX, and Sun Solaris.

Windows CE The Citrix ICA Client for Windows CE is integrated into products manufactured by our OEM partners, including manufacturers of windows-based terminals, hand-held devices, and Windows CE Professional devices.

For more information on the types of products available, see our Web site at http://www.citrix.com.

For specific details on the features, installation, and administration of the clients, see the *Citrix ICA Client Administration Guides* for the clients you plan to deploy.

Citrix Services

Citrix offers a variety of server add-ons that enhance the scalability, manageability, and reach of MetaFrame and the Citrix ICA Clients:

- Load Balancing Services
- SecureICA Services
- DirectICA Services
- Resource Management Services
- License Packs

Load Balancing Services

Citrix Load Balancing Services gives you the ability to scale a single MetaFrame server into a multi-server farm. With Load Balancing, you can publish an application to be run on any subset of servers in a Citrix server farm. When an ICA Client user starts a remote session on the Citrix server and launches a load balanced application, that user is automatically connected to the least busy server in the farm. With Load Balancing Services, you can:

- Balance application load among both MetaFrame and *WINFRAME* servers
- Adjust the criteria used to determine server load

SecureICA Services

SecureICA Services contains features to enhance the security of data communication across any type of connection supported by MetaFrame. SecureICA Services uses the RC5 encryption algorithm from RSA Data Security, Inc. The MetaFrame server and the Citrix ICA Client use the Diffie-Hellman key-agreement algorithm with a 1024-bit key to generate RC5 keys.

DirectICA Services

Citrix DirectICA for MetaFrame adds support for multi-VGA adapters to Citrix MetaFrame Application Server for Windows. A *multi-VGA adapter* (also called a *multiconsole adapter*) is a hardware device that contains several VGA video adapters with additional support hardware. Each multi-VGA adapter appears to the server as several VGA video adapters, each with an accompanying keyboard, mouse, and optional serial and parallel ports, depending on the manufacturer and model. The only limit to the number of multi-VGA adapters that you can install is your license count.

The combination of a keyboard, mouse, and monitor attached to a port on the multi-VGA adapter is referred to as a *DirectICA station*. MetaFrame treats connections associated with DirectICA stations much like the system console; the devices (serial and parallel ports) associated with the DirectICA station are on the server computer itself. Any serial or parallel ports associated with a DirectICA station are given unique device names and are treated as ports on the server computer. Because the ports are on the server, DirectICA stations do not support drive mapping, COM port mapping, or printer mapping.

For more information on DirectICA, see the *MetaFrame Administrator's Guide*.

Resource Management Services

Citrix Resource Management Services is the only application and systems management product designed specifically for Citrix servers. RMS provides full-feature management tools for analyzing and tuning MetaFrame, *WINFRAME*, and Terminal Server systems.

License Packs

When you first purchase MetaFrame, you get one or more base licenses for an initial user count. MetaFrame uses server-based concurrent licensing, which determines the number of users that can log onto your server at any given time.

As your user base grows, you can purchase license packs from Citrix to expand your user count.

Citrix MetaFrame License Packs come in 5-, 10-, 20-, and 50-user versions.

For more information about Citrix licensing, including how to pool user counts from multiple servers, see the *MetaFrame Administrator's Guide*.

MetaFrame's Features and Benefits

MetaFrame offers benefits to both IS management and end-users. Version 1.8 provides a range of new features to further simplify application deployment and access.

IS Management Benefits

MetaFrame provides a number of features that ease the burden on MIS:

- **Economy**. MetaFrame supports multiple concurrent users on a single processor and offers free, unlimited client software licensing, making it a cost-effective solution for enterprise-wide application delivery.
- **Enterprise Scalability**. Symmetrical multiprocessing (SMP) hardware compatibility enables MetaFrame to support hundreds of concurrent users.
- **Extensive Connectivity**. MetaFrame connects users to the network through standard telephone lines, WAN links (T1, T3, 56Kb, X.25), broadband connections (ISDN, Frame Relay, ATM), or the Internet.
- **Single-Point Application Management**. With MetaFrame, all application upgrades and additions are made only once at the server and are instantly available to all remote users.
- **End-to-End Management**. Using MetaFrame, administrators can set up applications, view active sessions, monitor system performance and events, troubleshoot problems, and create reports from the server. MetaFrame also allows administrators to use popular network management tools, such as Microsoft Systems Management Server and SNMP managers.
- **Remote Administration**. System administrators can dial-up to the Citrix server for remote administration and management.
- **Remote Support and Training**. Administrators can connect to a remote user's session to visually see what is on the screen and interact with the user, making MetaFrame a valuable remote support and training tool.
- **Seamless Network Integration**. MetaFrame integrates into NetWare, Windows NT, Novell, and other PC networks, allowing administrators to quickly set up users from existing domain or bindery information.
- **Security**. The MetaFrame security tools enhance the standard Windows Terminal Server security features by providing additional methods for securing file systems.

End-User Benefits

MetaFrame also improves the end-user's experience through:

- **Fast Application Access**. The Citrix ICA Clients give remote users fast access to any type of application, including DOS and 16- and 32-bit Windows programs, whether productivity applications, traditional client/server applications, or in-house mission-critical applications.
- **Local/Remote Transparency**. MetaFrame provides all the familiarity of a local LAN desktop. Remote users have complete access to all local system resources such as notebook drives, remote printers, and clipboards. Users can also cut and paste between local and remote applications and drag-and-drop to copy files in the background while they continue to work.
- **Integrated Desktops**. From a single desktop, remote users can run applications locally from the notebook PC or remotely from the Citrix server for best performance.
- **Easy Setup**. With its Windows 95-like installation and setup wizard, ICA Clients are easy to install for Windows 3.1, Windows for Workgroups, Windows 95, and Windows NT. The wizard guides users through all the necessary installation steps and automatically detects the PC's available modem.
- **32-Bit Windows Application Availability**. Remote users gain immediate access to Windows 95 and Windows NT applications, regardless of their client hardware. MetaFrame enables even DOS-based 286 systems to run Windows 95 applications at near-LAN speeds over low-bandwidth connections.

Features Included in 1.8

- **Program Neighborhood**. Program Neighborhood introduces a new metaphor for user application access that replaces Remote Application Manager for the Citrix ICA Win32 Client and delivers access to centrally deployed applications. With the introduction of Program Neighborhood, server-based applications can now be pushed to the Program Neighborhood client, integrated into the local 32-bit Windows desktop, or pushed directly to the client's Start menu.

  Similar in concept to Windows Network Neighborhood, Program Neighborhood provides total administrative control of applications by providing users with dynamic access to published applications. Not only do users have an enhanced server-based application experience, but also no client configuration is required. Program Neighborhood provides complete administrative control over application access and local desktop integration.

- **SpeedScreen**. SpeedScreen builds on the intelligent agent technology, introduced in MetaFrame 1.0, that reduces the transmission of frequently repainted screens. In comparison with MetaFrame 1.0, bandwidth consumption is reduced, on average, by 25-30% and total packets transmitted is cut by up to 60%, resulting in significant improvements in measured speed on restricted bandwidth connections.

  SpeedScreen furthers the user experience with consistent performance regardless of network connection by reducing latency and improving the feel of the server-based application.

- **Installation Management Services (IMS) Ready**. The Installation Management Services option gives Citrix administrators the ability to centrally manage software replication across Citrix server farms. You can run an application's installation routine just once per platform, then deploy the application to each server in the farm automatically.

  This innovative system services option for MetaFrame offers administrators an excellent alternative to manually installing and configuring the same application on multiple Citrix servers. Administrators can now more easily and cost-effectively deploy applications to thousands of users across the enterprise.

- **Video Ready**. VideoFrame in conjunction with MetaFrame 1.8 enables the production and deployment of custom video applications to 32-bit Windows ICA Clients using an innovative intelligent compression and a streaming extension to the ICA protocol.

  By integrating VideoFrame into a Citrix server farm, administrators can now deploy custom video applications to any 32-bit Windows desktop, on demand, while maintaining consistent performance across any network connection, regardless of available bandwidth.

- **ICA Browser Management**. With ICA Browser management, part of the enhancements to Citrix Server Administration, administrators now have the ability to control browser parameters such as backup ICA Browsers, ICA Gateways, and update and refresh intervals. Administrators can also configure which servers always attempt to become the master ICA Browser.

  ICA Browser management simplifies browser administration through an intuitive user interface for better system scaling and management.

- **License Pool Recovery**. Citrix has introduced a new backup licensing feature to better manage pooled licenses across the server farm. With this feature, you can define the number of backup servers to which user licensing data is replicated.

  This new addition to Citrix license pooling provides a greater level of fault tolerance across multiple Citrix servers.

- **Client Device Licensing**. This new feature allows a user to establish multiple sessions to multiple servers while consuming only a single pooled license for each session.

  Client device licensing reduces IT organizations' total cost of ownership (TCO) by providing seamless access to multiple applications across multiple servers, without incurring additional licensing costs.

Partnerships and Compatibility

Citrix has an ongoing program of application compatibility testing; however, we recommend that you contact the application vendors for information about MetaFrame compatibility. The Citrix-Compatible program and the Citrix Business Alliance program supply much of the information found in this guide.

The Citrix-Compatible Program

The Citrix-Compatible program enables software and hardware manufacturers to showcase their products or services as compatible with Citrix products.

Citrix-compatible products are listed in this guide. This guide is available for download on the Citrix World Wide Web site (http://www.citrix.com). Some members of the Citrix-Compatible program also include product brochures and special offers in the Citrix Solutions Provider handbook distributed in every Citrix Solutions Network (CSN) training class.

Citrix Business Alliance Partners

Members of the Citrix Business Alliance program provide the technology building blocks for solutions that include high-performance servers, flexible communications infrastructures, robust client-server development tools, and turnkey corporate applications. This program is composed of leading industry vendors who work with Citrix to develop innovative new products and markets for server-based computing.

Planning Considerations for a MetaFrame Solution

Before you begin the rest of the book, here are some sample questions to help you analyze your system requirements, along with some possible answers:

- What business problem are you trying to solve?
  - Remote e-mail access while traveling
  - Branch office access to large client/server applications (for example, human resources)
  - Streamline order entry process
  - Improve customer service
- What computing platform and applications are you using?
  - NetWare
  - Oracle database
  - PowerBuilder application on Windows desktops
- How many users need access? How many concurrent users? How long will a typical connection last?
  - 100 users total, 25 concurrent connections, 30 minutes
- What application server(s) are you planning to use?
- How will you connect to the application server?
  - Async Dial-In
  - Remote node (Microsoft RAS or third-party remote node software)
  - LAN
  - WAN (leased line, Frame Relay, ISDN, ATM)
  - Internet
- What client hardware/software will you be using?
  - 486DX/2 Windows notebook, 12MB RAM, Shiva PPP dialer supporting IP and IPX
- What are the functional requirements for a remote user?
  - Interactively access Microsoft Office, client/server applications, 3270 connectivity to mainframe applications
  - Print e-mail, documents, reports to client printer
  - File transfer between clients and servers
  - Security issues like dial-back, firewalls, third-party security hardware, etc.
- What are the performance requirements?
  - Ten seconds to look up a record
  - Type ahead limited to 2–3 characters for 50 WPM typist

- What is the time frame for initial pilot and full deployment?
  - Thirty day pilot, full deployment in the following 60 days
- Have the resources been allocated for this project?
  - Budget approved
  - Project manager and internal resources assigned
  - Professional systems integrator/Citrix authorized reseller engaged
- Who are the decision makers?
  - Director of MIS: budget approval, overall responsibility
  - Vice President of Finance: signoff on success criteria and final OK
  - Project Manager: “owns” the project
- How will we support the system once it is in place?
  - Disaster and recovery plans
  - Maintenance plans
  - Capacity planning and evaluating future needs

CHAPTER 2

Deploying the MetaFrame Servers and ICA Clients

The first phase of putting a MetaFrame solution into production is to deploy your servers and clients. To do so, you need to go through these steps:

1. Decide on your server hardware and peripheral devices
2. Decide how your MetaFrame servers should fit into your NT Domains
3. Install Windows NT Server, Terminal Server Edition
4. Install MetaFrame
5. Create a server farm and add your MetaFrame servers to it
6. Preconfigure modem support for your end-users
7. Install the clients and any custom configuration files

This chapter includes information to assist you with these steps.

For help with:	**See these sections:**
Step 1	"Sample Server Configurations" and "Server Hardware Device Notes"
Step 2	"MetaFrame Servers and NT Domains"
Step 3	"Installing Terminal Server"
Step 4	"Installing MetaFrame"
Step 5	"Creating Server Farms"
Step 6	"Client Modem Support"

For step-by-step instructions on installing the ICA Clients, see the*Citrix ICA Client Administrator's Guides* for the clients you plan to deploy.

Sample Server Configurations

Hardware compatible with Terminal Server and MetaFrame is listed in the *Microsoft Windows NT Hardware Compatibility List (HCL)*. The following table shows several sample hardware configurations suitable for deploying MetaFrame servers in an enterprise environment.

Note This is not a comprehensive list of compatible platforms and is presented solely to provide examples of known good configurations. No endorsement of any particular manufacturer is implied.

Server Make/Model	System BIOS	CPUs	Disk Controller	Network Adapter
Acer Altos 12000 *		(2) Pentium III 500MHz Xeon	Adaptec AIC-7896 Ultra2 SCSI	Intel 82558 FastEthernet
Acer Altos 21000 *		(4) Pentium III 500Mhz Xeon	Adaptec 7896 U2	Intel 82557-based 10/100
ALR Revolution *	Phoenix 4.0 Release 5.10.8	(6) Pentium Pro 200MHz	Adaptec AHA-7880 Version 1.32	3Com 3C905
Amdahl Envista Series	AMI V.1.00.05.CD0	(2) Pentium 166MHz	(2) AIC 7870 v.1.26s emb_PCI	Intel EtherExpress Pro 100B
Compaq Lightning MAC B2 *		(8) PII Xeon 500MHz	Compaq Integrated Smart Array/42xx	Compaq NC3131 Dual Port UTP Fast Ethernet
Compaq Proliant 800	P02 11/22/96	(2) Pentium Pro 200MHz	SimBios SCSI-3	Embedded Netflex-3 PCI
Compaq Proliant 1500	E12 1/16/96	(1) Pentium 133MHz	SimBios SCSI-3	Netflex-3
Compaq Proliant 2500		(2) Pentium Pro 200MHz	SimBios SCSI-3	Netflex-3
Compaq Proliant 3000 *	P09 11/25/98	(1) Pentium II 450MHz	Compaq Wide-Ultra SCSI	Compaq Netelligent 10/100 TX PCI UTP Controller 2.3
Compaq Proliant 4500 Server		(4) Pentium 166MHz		Netflex-3
Compaq Proliant 5000 Server *	Compaq System BIOS E-16	(4) Pentium Pro 200MHz	PCI Smart Array	Netflex-3
Compaq Proliant 6000 Server *	E20 5/16/97	(4) Pentium 200MHz	Western Digital WDE4360S	PCI Netelligent 10/100 TX
Data General Avion	Phoenix 4.05.9	(4) Pentium Pro 200MHz	Adaptec PCI 7870	Intel Pro 100B

Server Make/Model	System BIOS	CPUs	Disk Controller	Network Adapter
Dell Power Edge 4100/200 *		(2) Pentium Pro 200MHz	Adaptec 7880, 7860, PE RAID 2	Intel EtherExpress Pro 100B
Dell Optiplex Gxpro	Phoenix v1.0 5/29/96	(2) Pentium Pro 200MHz	Adaptec PCI 2939	3Com 3C590 Extended
Hewlett Packard NetServer E/40	Phoenix Release 4.05.8	(1) Pentium 200MHz	Adaptec AHA-2910 AIC 7850	No pre-configured card
Hewlett Packard NetServer LS	AMI 1.00.04.CD0L	(2) Pentium Pro 200MHz	(2) AIC 7870 v.1.2s8 emb_PCI	3Com 3C595
IBM AS/400 *	Surepath 6/30/94	(1) Pentium II 350MHz		AMD PCNET and AS/400 Virtual Token Ring
IBM Netfinity 3000 *	IBM PC BIOS 3/8/98	(1) Pentium II 350MHz	Adaptec AIC-78xx	IBM Etherjet 10/100
IBM Netfinity 3500 *	IBM PC BIOS 3/20/98	(2) Pentium II 333MHz	Adaptec AIC-78xx	IBM Etherjet 10/100
IBM ServeRAID Netfinity 5500 *	Surepath 9/3/97	(2) Pentium II 350MHz	Adaptec AIC-78xx	AMD PCNET
IBM Netfinity 5600 *		(2) Pentium III Xeon 600MHz	Adaptec 7896 U2	Netfinity Fault Tolerant
IBM Netfinity 7000 Server *	Surepath 10/20/97	(4) Pentium Pro 200MHz	Adaptec AIC-78xx	3Com 3C905b-TX
IBM Netfinity 7000 M10 *	IBM Netfinity BIOS	(1) Pentium II Xeon 400MHz	Adaptec AIC-7895 v1.34	Intel 82557-based PCI Ethernet
IBM Netfinity 7000 M10 (86802R) *	Surepath 9/19/98	(4) Pentium II Xeon 400MHz	Adaptec AIC-78xx	Intel-82557 (EtherExpress Pro) Embedded
IBM PC Server 330 *	SurePath 1/21/97	(2) Pentium Pro 200MHz	Adaptec 7880 v.1.25	AMD PCNET
IBM PC Server 704 *	AMI 1.00.08	(1) Pentium Pro 200MHz	Adaptec 7880 v.1.256	3Com 3C905XL
NetFrame NF9000 *		(4) Pentium Pro 200MHz	Qlogic PCI	3Com 3C905XL
NetPower Sparta Series	AMI 1.00.06.CD0	(1) Pentium Pro 200MHz	Adaptec PCI 7880 V1.25	Intel Pro 100B 82557**
Sequent NTS-2000 *	AMI 1.00.07.CD0	(4) Pentium Pro 200MHz	DAC 960 v1.29. 4MB	SMC 9332/9334 BDT 10/100
Unisys Aquanta ES (ES204131) *	BIOS v2.0	(2) Pentium Pro 200MHz	Adaptec 7880 v.1.25	3Com 3C905XL

* Additional information about these systems is included below.

** Requires a supplied driver, Part Number 2569.

Server Hardware Device Notes

This section contains notes for popular servers.

Acer Altos 12000

This section describes how to install Microsoft Windows NT Server 4.0, Terminal Server Edition, and Citrix MetaFrame on an Acer Altos 12000 server.

The Altos 12000 supports up to two Intel Pentium III Xeon 550MHz processors, each with 512KB, 1MB, or 2MB of L2 cache, and a memory capacity of up to 2GB of ECC SDRAM. The Altos 12000 chassis can hold eight hot-swappable Ultra2 SCSI hard drives. It is easily accessible for upgrade or service behind removable side panels. The motherboard can hold five PCI cards and one ISA card and has an integrated Intel 10/100 PCI network interface controller on-board. The Altos 12000 features AGP graphics.

Requirements

Hardware Requirements/Tested System Configuration

- Two Pentium III Xeon 500MHz processors each with 512KB of L2 cache
- 128MB of SDRAM
- Onboard Adaptec AIC-7896 Ultra2 SCSI controller
- Onboard Intel 82558 FastEthernet NIC
- One 9GB Ultra2 SCSI drive
- One IDE CD-ROM drive
- ATI Rage IIc AGP display card

Software Requirements

- Microsoft Windows NT 4.0, Terminal Server Edition, and Service Pack 4
- Citrix MetaFrame Version 1.8

Installing Terminal Server

This section describes how to install the SCSI controller driver and the network adapter during Terminal Server installation.

1. Insert the Terminal Server Setup boot disk in the server's diskette drive A.
2. When prompted, insert Setup Disk 2 and press ENTER. Setup loads the drivers for Terminal Server installation to boot and the Windows NT name, version, and build number are displayed. Also displayed are the Terminal Server build number, the number of processors, and the amount of memory detected in the system.

3. Press ENTER to continue the installation.
4. Setup allows you to manually select SCSI adapters, CD-ROM drives, and special disk controllers for installation. Press **S** to configure additional SCSI controllers.
5. Select **Other** (located at the end of the list), and press ENTER. You are prompted for a driver diskette.
6. Insert the Adaptec 7800 Family Set Manager diskette and click **OK**. The device drivers on the diskette are displayed. Select the Adaptec AHA-294xU2/295xU2/395xU2/AIC-789x PCI SCSI controller (NT 4.0) driver and press ENTER to continue.
7. If the IDE CD-ROM drive is installed in the Altos 12000, repeat Steps 4 through 7 and install the IDE CD-ROM driver.
8. Insert Setup Disk 3 in drive A and press ENTER when prompted. Setup lists all the recognized mass storage devices. Press ENTER to continue.
9. After completing the mass storage device setup, Setup prompts for the Terminal Server compact disk.

   The End-User License Agreement (EULA) is displayed. Read the EULA and press **F8** if you accept the terms and conditions in the agreement.

   Setup performs a search to detect any previous installations of Terminal Server. If you are installing a fresh copy of Terminal Server, press **N** for new install.
10. Setup lists your computer type, video display, mouse, keyboard, and keyboard layout. Acer recommends that you leave these settings unchanged. Press ENTER when done.
11. Setup asks you for a target location to install Terminal Server. You also have a choice of creating or deleting partitions at this point.
12. Select the newly created partition or an existing partition as the target and press ENTER.
13. Setup prompts for the type of file system to be formatted. Acer recommends formatting the partition as NTFS.
14. Specify the directory to install Terminal Server. By default, Terminal Server is installed in the \\WTSRV directory.
15. You are asked if you want to perform an examination of all existing partitions. Press **ESC** to skip this.
16. When the examination is complete, files are copied to the server. Remove any disks and CDs from their drives and press ENTER to restart the computer.
17. After converting the file system into NTFS, the server starts the GUI setup.
18. During the network configuration portion of Setup, select **Other** for the network interface card type and use the Intel PRO/100 Server Adapter driver

diskette to install the appropriate network interface card driver for your configuration.

19. Complete Terminal Server installation and reboot. Acer provides video device drivers on a separate diskette. The video driver cannot be changed during Setup. You can install it after Service Pack 4 is installed.

Installing Citrix MetaFrame

This section describes how to install MetaFrame on an Altos 12000. Before you install MetaFrame, you must install Windows NT Server 4.0, Terminal Server Edition, and Service Pack 4.0.

1. Log on to the Terminal Server console as an administrator.
2. Insert the MetaFrame CD into the CD-ROM drive.
3. Install MetaFrame following the directions in the Citrix MetaFrame documentation.

Acer Altos 21000

This section describes how to install Citrix MetaFrame and Microsoft Windows NT 4.0, Terminal Server Edition, on an Acer Altos 21000 server.

Software Requirements

- Microsoft Windows NT 4.0, Terminal Server Edition, Version 4.0 or later
- MetaFrame Version 1.0 or higher
- Adaptec 7800 Family Manager for Microsoft Windows NT, Version 3.2
- Intel EtherExpress Pro100+ driver for Microsoft Windows NT
- ATI IIc Microsoft Windows NT 4.0 video drivers V5.1

Before Installation

1. Obtain the required device drivers by contacting Acer Support or visiting the Web site at http://www.acer.com.tw/service/index.htm.
2. Create Windows Terminal Server boot disks. From the console of a Windows NT 4.0 workstation or server, start a DOS prompt and type **winnt32 /ox** from the \I386 directory on the Windows Terminal Server CD-ROM. Follow the on-screen instructions.

Installing Terminal Server and MetaFrame

1. Insert Terminal Server Edition boot disk #1 in the appropriate drive, turn on the machine, and follow the on-screen instructions.
2. When prompted to autodetect mass storage controllers, press ENTER to detect.
3. Press **S** to configure additional mass storage controllers.
4. Expand the list of additional SCSI adapters, select **Other** (located at the end of the list), and press ENTER.
5. When prompted for a driver diskette, insert the Adaptec 7800 Family Manager for Microsoft WindowsNT Version 3.2 device driver diskette into drive A (or other appropriate drive) and press ENTER. Select the Adaptec 78xx U2 Adapter for Windows NT 4.0 and press ENTER to continue.
6. See the *Microsoft Windows Terminal Server Installation Guide* to continue the installation.
7. From the **Network Adapters** dialog box, click **Select from list…** to display the **Select Network Adapter** dialog box.
8. Click **Have Disk…** and insert the Intel EtherExpress Pro100 + driver for Microsoft Windows NT device driver diskette. Click **OK** to continue.
9. Select the Intel 82558-based 10/100 adapter and click **OK** to continue.

10. Insert the MetaFrame CD-ROM and choose **MetaFrame Setup** from the list of on-screen options.
11. See the *MetaFrame Administrator's Guide* to complete installation and setup.

Installing the Video Card Adapter

Note During system installation, the standard video driver supplied with Terminal Server is automatically installed. To obtain larger screen sizes and video color depth, you must install the manufacturer-supplied video driver. This procedure describes how to install the correct video driver.

1. Click **Start**, select **Settings**, then click **Control Panel**.
2. On the Control Panel, double click **Display**.
3. On the **Settings** dialog box, click the **Display Type...** button.
4. From the **Display Type** dialog box, in the **Adapter Type** section, click the **Change...** button.
5. In the **Change Display** dialog box, click the **Have Disk...** button.
6. Insert the new display driver diskette into drive A and click **OK**.
7. From the list of displayed ATI devices, select the ATI Rage IIc Graphics Adapter device.
8. From **Third-party Drivers**, click **Yes** to proceed. If the message: "The driver is already installed on the system" appears and you are asked if you want to use the current or new drivers, click **New**.
9. If prompted for the driver diskette a second time, click **Continue**.
10. When the message "The drivers were successfully installed" appears, remove the display driver diskette and click **OK**.
11. From the **Display Type** dialog box, click **Close**.
12. From the **Display Properties** dialog box, click **Close**.
13. At the **System Settings Change** dialog box, click **Yes** to reboot the server.

ALR Revolution

ALR manufactures high-end computer systems. Their Revolution series system provides scalability in the processing, memory, and disk subsystems that allow significant growth. Other available features, such as error correcting memory, hot swappable RAID configurations, and compact rack mounted systems provide a powerful computing environment for running the MetaFrame server.

Software Requirements

- MetaFrame Version 1.0 or higher
- Microsoft Windows NT Server, Terminal Server Edition
- ADAC RAID adapter driver, if using the ADAC RAID controller

Before Installing MetaFrame

If the ADAC RAID controller is not used, proceed to the next section.

If the ADAC RAID controller is being used:

1. During the Power On Self Test (POST), make sure that the on-board Adaptec AHA-7880 recognizes the CD-ROM and that the ADAC RAID controller is also detected.
2. During the POST, press CTRL+M to enter and configure the RAID environment.

Note For performance reasons, it is not recommended that you install the MetaFrame server on hard drives that are in the RAID configuration. Use the RAID configured hard drives to store data.

Installing MetaFrame

If the ADAC RAID controller is not used, install Terminal Server following the directions in “Installing Terminal Server” later in this chapter.

If the ADAC RAID controller is used:

1. During the installation, after Terminal Server detects the Adaptec AHA-7880 controller, press **S** to specify another device. Select Other and insert the ALR-supplied disk with the ADAC RAID controller driver.
2. Continue installing Terminal Server, following the directions in “Installing Terminal Server” later in this chapter.

Compaq Lightning MAC B2

This section describes how to install Citrix MetaFrame and Microsoft Windows NT Server, Terminal Server Edition on a Compaq Lightning MAC B2 server.

Software Requirements

- MetaFrame Version 1.0 or later
- Microsoft Windows NT Server, Terminal Server Edition
- Compaq Softpaq for NT 4.0 (v4.21 or later)

Before Installation

1. Obtain the Compaq Softpaq for Microsoft Windows NT from the Compaq Web site at http://www.compaq.com/support/files/server/softpaqs/WINNT/NTSSD400.html or by contacting Compaq Support.
2. Create the four Softpaq support diskettes by following the online instructions.
3. Create Windows Terminal Server boot disks. From the system console, start a DOS prompt, change to the \i386 directory on the Windows Terminal Server CD-ROM, type **winnt32 /ox**, and follow the on-screen instructions.

Installing Windows Terminal Server and MetaFrame

1. Install Terminal Server following the directions in “Installing Terminal Server” later in this chapter.
2. When prompted to autodetect mass storage controllers, press **S** to skip mass storage detection.
3. Press **S** to configure additional mass storage controllers.
4. Expand the list of additional SCSI adapters, select **Other** (located at the end of the list), and press ENTER.
5. When prompted for a driver diskette, insert the Compaq Softpaq Disk #2 and press ENTER. Select the Compaq Integrated Smart Array/42xx Controllers and press ENTER to continue.
6. Press **S** to configure additional mass storage controllers. Expand the list and select the IDE CD-ROM (ATAPI 1.2)/PCI IDE Controller and press ENTER to continue.
7. From the Network Adapters screen, click **Select from list…** to display the **Select Network Adapter** screen.
8. Click **Have Disk…** and insert the Compaq Softpaq Disk #4 into the disk drive and click **OK** to continue.
9. Select the **Compaq NC3131 Dual Port UTP Fast Ethernet controller** and click **OK** to continue.

10. Refer to the *Microsoft Windows Terminal Server Installation Guide* to complete the installation.
11. After installation is complete and the system reboots, log on to the console as an administrator.
12. Insert the MetaFrame CD into the CD-ROM drive.
13. Install MetaFrame following the directions in the Citrix MetaFrame documentation.

Compaq Proliant 3000

This section describes how to install MetaFrame on the Compaq Proliant 3000 systems.

Software Requirements

- Microsoft Windows NT Server 4.0, Terminal Server Edition
- MetaFrame Version 1.0 or higher
- Compaq Softpaq for Windows NT 4.0 (v4.21 or later)

Pre-installation Steps

1. Obtain the Compaq Softpaq for Microsoft Windows NT 4.0 from the Compaq website at http://www.compaq.com/support/files/server/softpaqs/WINNT/NTSSD400.html.
2. Create the four Softpaq support diskettes by following the online instructions.
3. Create Windows Terminal Server Boot Disks. From the console of an NT 4.0 workstation or sever start a DOS prompt and type winnt32 /ox from the \i386 directory on the Windows Terminal Server CD-ROM and follow the on screen instructions.

Terminal Server Edition and MetaFrame Installation

1. Insert Terminal Server Edition Boot disk #1, turn on the machine, and follow the on-screen instructions.
2. When prompted to autodetect mass storage controllers, press ENTER to detect mass storage controllers.
3. Refer to the Microsoft Windows Terminal Server Installation Guide to continue the installation.
4. From the Network Adapters screen, click “Select from list…” to display the “Select Network Adapter” screen.
5. Click “Have Disk…” and insert the Compaq Softpaq diskette #4 into drive “A:\” and type in the path “a:\net\intelnic\”. Click “OK” to continue.
6. Select the Compaq Fast Ethernet NC3120 (NT 4.0) and click “OK” to continue.
7. Refer to the *Microsoft Windows Terminal Server Installation Guide* to complete the installation.
8. Insert the MetaFrame CD into the CD-ROM Drive and choose MetaFrame Setup from the list of on screen options.
9. Refer to the MetaFrame *Installation Guide* and to complete the installation and setup.

Compaq Proliant 5000 Server

This section describes how to install MetaFrame on the Compaq Proliant 5000 systems. Two procedures are documented:

- Installing on an upgrade of *WINFRAME*
- Installing on Terminal Server

Upgrading from *WINFRAME* Version 1.7 to MetaFrame

1. Insert the Terminal Server CD into the CD-ROM drive on the *WINFRAME* Version 1.7 server.
2. Upgrade *WINFRAME* following the directions in “Installing Terminal Server” later in this chapter. During the text-based portion of the install, Setup asks if you want to upgrade an existing operating system or do a new install. Select upgrade an existing operating system. Setup lists the operating system(s) present on the computer. Select *WINFRAME* as the operating system to upgrade.

Note The following six files cannot be copied because of conflicting Oemsetup.inf files:

NetFlx3.sys

NetFlx3.dll

OemSetup.inf

NetFlx3.exe

NetFlx.hlp

NetFlx.cpl

These files, which pertain to the network card, are not critical and can be ignored during installation. Terminal Server uses the existing *WINFRAME* Version 1.7 network drivers.

3. Complete Terminal Server installation.
4. After the system reboots, log on to the Terminal Server console as an administrator.
5. Insert the MetaFrame compact disk into the CD-ROM drive.
6. Install MetaFrame following the directions in the Citrix MetaFrame documentation.

MetaFrame detects the existing *WINFRAME* ICA sessions (*WINFRAME* Upgrade Detection) and gives you the option of either keeping the current ICA sessions or creating new ones.

Remarks

Network connectivity is maintained after the upgrade; however, the updated network drivers can be installed once Terminal Server Setup is complete. This can be done manually through the **Network** applet under Control Panel. Remove the network card under the **Adapters** tab and reinstall it from the Terminal Server compact disk.

MetaFrame Installation on Terminal Server

1. Install Terminal Server following the directions in "Installing Terminal Server" later in this chapter.
2. After installation is complete and the system reboots, log on to the console as an administrator.
3. Insert the MetaFrame compact disk into the CD-ROM drive.
4. Install MetaFrame following the directions in the Citrix MetaFrame documentation.

Compaq Proliant 6000 Server

This section describes how to install MetaFrame on a Compaq Proliant 6000 system. The Compaq Proliant 6000 server incorporates a symmetrical multiprocessor (SMP) architecture that supports the installation of up to four system processors.

Hardware Tested

- Compaq Proliant 6000
- Four Pentium Pro 200MHz processors
- Two Compaq Ultra Wide SCSI controllers (embedded)
- Netflex-3 network adapter
- Four 4GB SCSI drives

Software Requirements

- MetaFrame Version 1.0 or later
- Microsoft Windows NT Server, Terminal Server Edition

Installing MetaFrame

1. Install Terminal Server following the directions in “Installing Terminal Server” later in this chapter.
2. When prompted to autodetect mass storage controllers, press ENTER.
3. Complete Terminal Server installation.
4. After the system reboots, log on to the Terminal Server console as an administrator.
5. Insert the MetaFrame CD-ROM in the CD drive and choose **MetaFrame Setup** from the list of on-screen options.
6. Install MetaFrame following the instructions in the Citrix MetaFrame documentation.

Dell PowerEdge 4100/200

This section describes how to install MetaFrame on a Dell PowerEdge 4100 system.

The Dell PowerEdge series systems are high-speed, upgradeable PC servers designed around the Intel Pentium Pro family of microprocessors. The PowerEdge 4100 systems provide both Extended Industry-Standard Architecture (EISA) and high-performance Peripheral Component Interconnect (PCI) expansion slots. The PowerEdge 4100 series comes in two models: the 4100/180 equipped with one or two 180MHz Pentium Pro processors (each with 256KB of Level 1 cache) and the 4100/200 equipped with one or two 200MHz Pentium Pro processors (each with 512KB of Level 1 cache). The 4100 series has an upper limit of 1GB of RAM. Optionally, the 4100 can be equipped with the Dell PowerEdge RAID II controller.

Software Requirements

- MetaFrame Version 1.0 or higher
- Microsoft Windows NT Server, Terminal Server Edition
- Dell Server Assistant CD-ROM Version 1.30 or later

Installing MetaFrame

1. Insert the Dell Server Assistant CD-ROM into the CD-ROM drive of the PowerEdge 4100 and power on the Dell machine. The Dell Server Assistant software boots from the CD-ROM. From the Dell Server Assistant CD-ROM menu, select **Create Diskettes**. Follow the instructions on-screen to create the Dell support diskettes.
2. Install Terminal Server following the directions in “Installing Terminal Server” later in this chapter. When Terminal Server Setup displays all recognized SCSI controllers, if the PowerEdge RAID II Controller is installed in the PowerEdge 4100, press **S** to install the Dell PowerEdge RAID II Controller drive
3. Insert the Dell PowerEdge Terminal Server Drivers diskette that was created in Step 1 and click **OK**.
4. Complete Terminal Server installation.
5. After the system reboots, log on to the Terminal Server console as an administrator.
6. Insert the MetaFrame compact disk into the CD-ROM drive and begin installing MetaFrame following the instructions in the Citrix MetaFrame documentation.

Installing the Dell PowerEdge RAID II Controller Console

1. Install the PowerEdge RAID II Console after Terminal Server installation is complete.
2. From the console, log on as an administrator.
3. Insert the Dell PowerEdge Terminal Server RAID II Controller Driver diskette into drive A.
4. Type **a:\setup** in the text box of the **Run** menu and press ENTER to begin installation. Follow the displayed instructions.
5. When installation is complete, the PowerEdge RAID II Console is added to the Programs folder in the administrator's **Start** menu.

IBM AS/400

This section describes how to install Citrix MetaFrame and Microsoft Windows NT Server, Terminal Server Edition on an IBM AS/400 system.

Today, many companies use AS/400s to run their commercial and business applications. In addition, it is not unusual for companies to install PC-based servers alongside the AS/400s to provide PC file and print services to their users. Companies deploying Windows NT Server, Terminal Server Edition and MetaFrame as their network operating system also have the option of running this software configuration on an AS/400.

The AS/400 focuses on the value of integration for database, networking, security and application services. AS/400 integration value reduces complexity in customers' installations, lowering their total cost of ownership (TCO). Customers using the AS/400 can extend the same integration value to include their PC servers. The Integrated PC Server extends the AS/400's integration to combine a PC server inside the AS/400, sharing many of its resources: disk, tape, and CD-ROM.

Requirements

Hardware Requirements

- AS/400 server
- Twinax cable
- ASCII (PC connection) cable
- AS/400 Integrated Netfinity Server

Software Requirements

- Microsoft Windows NT Server, Terminal Server Edition
- MetaFrame Version 1.0 or later

Installation Overview

The steps required for installing Terminal Server/MetaFrame on the AS/400 Integrated Netfinity Server are separated into the following sections.

- AS/400 configuration verification
- Terminal Server and MetaFrame installation
  - Installing Terminal Server on the AS/400 Integrated Netfinity Server (AS/400 – side tasks)
  - Installing Terminal Server on the AS/400 Integrated Netfinity Server (Terminal Server Edition – side tasks)
  - Installing MetaFrame on the AS/400

After Terminal Server and MetaFrame are installed on the AS/400, any software administration such as user accounts, security, and application deployment are the same as for a standard PC-based system. See the AS/400 documentation for additional system hardware maintenance and configuration.

AS/400 Configuration Verification

1. Before installing Terminal Server on an AS/400, verify that the Integrated Netfinity Server is installed. The software requirements for Terminal Server IPCS are as follows:
   - OS/400 V4R2
   - AS/400 Integration with Terminal Server

   To obtain more information, visit the IBM Web site at http://www.pc.ibm.com/server.
2. Use the work sheets below as a guideline to ensure that the AS/400 Integrated Netfinity Server is configured correctly before installing Terminal Server and MetaFrame on an AS/400.

Table 1 - Installation Work Sheet for AS/400 Parameters

Field	Description and Instructions	Value
Network server description	Defines the operating characteristics and communications connections of the network server that controls the Terminal Server. Use a name that is easy to remember. The name can have up to eight characters. Use only the characters A-Z and 0-9 in the name and use a letter for the first character. The network server description name is also the computer name and TCP/IP host name of the Terminal Server.	
Resource name	Identifies the Terminal Server hardware. To determine the name, enter DSPHDWRSC *CMN at the AS/400 command line. If you have a 2850 model Integrated PC Server, look for a name in the format LINxx, in which xx is a number. The text associated with this name should indicate that the resource is a file server IOP.	

Field	Description and Instructions	Value
Domain role	Specifies the role performed by this network server: *DMNCTL. This network server is a primary domain controller, managing user access between servers and clients. *BKUCTL. This network server is a backup domain controller. *SERVER. This network server is a stand-alone or member server that provides services such as printing or e-mail to client computers but does not control access. To change the domain role to or from *SERVER, you must reinstall Terminal Server. Consider your options carefully before choosing a role. See the Terminal Server documentation for more information about deciding the role of the Terminal Server.	
Install option	Specifies the Terminal Server installation method. *INSTALL. Install a new Terminal Server and the AS/400 integration with Windows NT Server code. This option creates a new network server description, storage spaces, message queue, line descriptions, and TCP interfaces on the AS/400. *REINSTALL. Reinstall or upgrade an existing Terminal Server and the AS/400 integration with Terminal Server code. This option uses an existing network server description, storage spaces, message queue, line descriptions, and TCP interfaces on the AS/400. See the *Windows NT Start Here: Basics and Installation Guide* and Setup.txt files for more information prior to reinstalling or upgrading Terminal Server.	
TCP/IP local domain name	Specifies the TCP/IP local domain name associated with the Terminal Server. You can specify *SYS to use the same value the AS/400 system uses.	
TCP/IP name	Specifies the Internet address of the name server used by the Terminal Server.	

Field	Description and Instructions	Value
server system	You can specify up to three Internet addresses or you can specify *SYS to use the same value the AS/400 system uses.	
Server domain name	Applies to domain controllers and backup domain controllers only. Specifies the Terminal Server domain on which the server will be a domain controller.	
To workgroup	Used when the server's domain role is *SERVER. Specifies the name of the Terminal Server workgroup in which the server will participate.	
To domain	Used when the server's domain role is *SERVER. Specifies the name of the Terminal Server domain in which the server will participate.	
Server message queue and library	Specifies the name of the message queue and the library in which it will be located. If the message queue does not already exist, the INSWNTSVR command creates it. The message queue is where all event logs and errors associated with this server are sent. Specify a MSGQ name and library. You can also specify *JOBLOG to send non-severe errors to the job log of the user administration monitor and severe errors to QSYSOPR. If you specify *NONE, non-severe errors are not sent to the AS/400 and severe errors are sent to QSYSOPR.	Queue: Library:

Field	Description and Instructions	Value
Event log monitor	Specifies whether or not the AS/400 receives event log messages from the Terminal Server. The choices are all, system, security, application, or none: *ALL. The AS/400 receives all event log messages. *NONE. No event log messages are received. *SYS. The AS/400 receives system event log messages. *SEC. The AS/400 receives security event log messages. *APP. The AS/400 receives application event log messages. **Note**: If you propagate the security log (by specifying *ALL or *SEC), be sure to set up the message queue with the proper security.	
Server storage space sizes	Specifies the size of the server storage spaces for drives D and E. Drive D must be large enough to hold the contents of the I386 Terminal Server installation CD-ROM and the AS/400 integration with Terminal Server code. It can be from 200 to 1007MB. Drive E must be large enough to hold the Terminal Server operating system. It can be from 500 to 1007MB. **Note**: When deciding each drive's size, allow room for future needs such as new applications or upgrades to the Terminal Server product.	Drive D size: Drive E size:

Field	Description and Instructions	Value
Restricted device resources	Restricts tape devices from being used as backup media for the network server data. *NONE. Restricts no tape devices from being used as the backup media for the network server. *ALL. Restricts all tape devices from being used as the backup media for the network server. Restricted device. Specifies up to ten tape drives that cannot be used as the backup media for the network server.	
Time zone	Records AS/400 offset from Greenwich Mean Time for use in the Terminal Server phase of installation.	

Table 2 - Windows Terminal Server Networking Information

Note Fill in this work sheet only if you plan to share the LAN adapters installed in your Integrated PC Server with the AS/400. LAN adapters are referred to as *ports* on the AS/400.

Item	Description and Instructions	Value
Line type	Identifies the type of network adapter that is installed in the Integrated PC Server that will be shared by the AC/400 and Terminal Server. This value can be one of four types: *ETH10M (10Mbps Ethernet), *ETH100M (100Mbps Ethernet), *TRN4M (4Mbps token ring), or *TRN16M (16Mbps token ring).	Port 1: Port 2:
Local adapter address	Identifies the network adapter address on the AS/400. The values you can specify depend on the line type. Ethernet lines use values between 020000000000 and 7EFFFFFFFFFF. The second character must be 2, 6, A, or E. Token ring lines use values between 400000000000 and 7EFFFFFFFFFF. Your network administrator can assign your local adapter address. Every network adapter on the LAN must have a unique local adapter address.	Port 1: Port 2:

Item	Description and Instructions	Value
Maximum transmission unit	Specifies the maximum size (in bytes) of IP datagrams that are transmitted. Either taken the default of 1492 or specify MTU to take the optimized value of your interface type. A larger size increases the efficiency of sending and receiving data. However, problems can arise if your network has bridges or routers that cannot accommodate larger sizes.	Port 1: Port 2:
AS/400 Internet address	Specifies the AS/400 Internet address for each shared LAN adapter. (An Internet address consists of four numbers, each between 0 and 255, separated by periods.) All Internet addresses must be unique on the network. Your network administrator can give you the Internet addresses.	AS/400 Port 1 AS/400 Port 2
AS/400 subnet mask	Used in TCP/IP communications. A subnet mask consists of four numbers, each between 0 and 255, separated by periods. Your network administrator can give you the subnet mask.	AS/400 Port 1 AS/400 Port 2
Windows NT Internet address	Specifies the NT Internet address for each shared LAN adapter. (An Internet address consists of four numbers, each between 0 and 255, separated by periods.) All Internet addresses must be unique on the network. Your network administrator can give you the Internet addresses.	NT Port 1 NT Port 2
Windows NT subnet mask	Used in TCP/IP communications. A subnet mask consists of four numbers, each between 0 and 255, separated by periods. Your network administrator can give you the subnet mask.	Windows NT Port 1 Windows NT Port 2

Item	Description and Instructions	Value
Internet LAN	An internal LAN (also called the virtual LAN) exists between the AS/400 and the Terminal Server. Both the AS/400 side and the Terminal Server side of this LAN have IP addresses and subnet masks. **Note**: These Internet addresses are set up automatically by the INSWNTSVR command. You record the Terminal Server side address during the Terminal Server phase of the installation when it appears on the AS/400 screen. From that information, you can infer the AS/400 side information. The fourth octet of the AS/400 side internal IP address is always one less than the fourth octet of the Terminal Server internal IP address. The subnet mask is always 255.255.255.0.	AS/400-side IP address: Terminal Server-side IP address:

Terminal Server and MetaFrame Installation

Installing Terminal Server on an AS/400 (AS/400-side Tasks)

1. Insert the Terminal Server installation CD in the CD-ROM drive.

   Note If you are using an upgrade version of the Terminal Server CD-ROM to do the installation, you are prompted for a non-upgrade version during the text mode of the installation. At that time, insert the non-upgrade Terminal Server CD and press ENTER to continue the installation.

2. At the AS/400 command line, type **inswntsvr** and press F4. The **Install Windows NT Server** dialog box appears.
3. In **Network Server Description**, **Resource Name**, and **Domain Role**, type the information from Table 1.
4. Choose the Terminal Server version you want to install.
5. For the **Install** option, use the default *INSTALL.
6. If you have LAN cards installed on the Integrated PC Server, the AS/400 can use one or both of those LAN adapters. Use the information from Table 2 to fill in the following information for each port:
   - Line type
   - Local adapter address
   - Maximum transmission unit
   - AS/400 Internet address

- AS/400 subnet mask
- Windows NT Internet address
- Windows NT subnet mask

Note If you have LAN cards but do not specify any port information, Terminal Server still detects the cards during installation and installs them. However, the AS/400 cannot access the LAN through these cards.

```
Install Windows NT Server (INSWNTSVR)
Type choices, press ENTER.
Network server description       NTSVR1 Name
Resource name                    LIN05 Name
Domain role                      *DMNCTL *DMNCTL, *BKUCTL,
                                 *SERVER
Windows NT version               *NT40 *NT40
Install option                   *INSTALL *INSTALL, *REINSTALL
Port 1:
Line type                        *TRN16M *NONE, *ETH10M,
                                 *ETH100M…
Local adapter address            654F927AD011 020000000000-
                                 7FFFFFFFFFFF
Maximum transmission unit        1492 Number
AS/400 Internet address          *NONE
AS/400 subnet mask               *NONE
NT Internet address              150.1.1.1
NT subnet mask                   255.255.0.0
More…
F3=Exit F4=Prompt F5-Refresh F10=Additional parameters F12=Cancel
F13=How to use this display F24=More keys
```

Figure 1 - Installing Terminal Server (OS/400 Display 1)

```
Install Windows NT Server (INSWNTSVR)
Type choices, press ENTER.
Port 2:
Line type                        *NONE *NONE, *ETH10M, *ETH100M
Local adapter address            020000000000-7FFFFFFFFFFF
Maximum transmission unit        1492 Number
AS/400 Internet address          *NONE
```

```
AS/400 subnet mask                 *NONE
NT Internet address
NT subnet mask
TCP/IP local domain name           *SYS
TCP/IP name server system          *SYS
+ for more values
Server message queue               *JOBLOG Name, *JOBLOG, *NONE
Library                            Name, *LIBL, *CURLIB
More…
F3=Exit F4=Prompt F5=Refresh F10-Additional parameters F12=Cancel
F13=How to use this display F24=More keys
```

Figure 2 - Installing Terminal Server (OS/400 Display 2)

7. Type the values from Table 2 in the following fields:
   - TCP/IP local domain name
   - TCP/IP name server system
   - Server message queue
   - Library

```
Install Windows NT Server (INSWNTSVR)
Type choices, press ENTER.
Event Log                          *ALL *ALL, *NONE, *SYS, *SEC,
                                   *APP
+ for more values
Server storage space sizes:
Drive D size                       200 200-1007
Drive E size                       500 500-1007
Convert to NTFS                    *NO *NO, *YES
Server domain name                 NTDMN1
To workgroup
To domain
Full Name
Organization
Language version                   *PRIMARY *PRIMARY, 2911, 2922,
                                   2923
Synchronize date and time          *YES *YES, *NO
Windows NT license key
```

```
License Mode:
License type                          *PERSEAT *PERSEAT, *PERSERVER
Client licenses                       number
More…
F3=Exit F4=Prompt F5=Refresh F10-Additional parameters F12=Cancel
F13=How to use this display F24=More keys

Install Windows NT Server (INSWNTSVR)
Restricted device resources           *NONE Name, *NONE, *ALL
+ for more values
Text ‘description’                    *BLANK
Additional parameters
Keyboard layout                       *DEFAULT *DEFAULT,…
Bottom
```

Figure 3 - Installing Terminal Server (OS/400 Displays 3 and 4)

8. In **Event Log** box, specify which event log messages you want the AS/400 to receive from the server.
9. In the boxes for Server storage space sizes, type the values from Table 1.
10. In the **Convert to NTFS** box, specify *NO to leave the Terminal Server system drive formatted with the file allocation table (FAT) file system. If you want drive E converted to the New Technology File System (NTFS) during the install, specify *YES.
11. In the **Server Domain Name**, **To Workgroup**, and **To Domain** boxes, type the values from Table 2.
12. In the **Full Name** box, specify the name of the user who holds the Terminal Server license you are installing.
13. In the **Organization** box, specify the name of the organization that holds the Terminal Server license you are installing.
14. In the **Language Version** box, specify *PRIMARY to have the AS/400 Integration with Terminal Server use your primary language. To prevent problems with predefined names that cannot be enrolled, choose the language that matches the language of the Terminal Server that you are installing.
15. In the **Synchronize Date and Time** box, specify *YES to have the AS/400 synchronize the date and time with Terminal Server every 30 minutes. If you want the AS/400 to synchronize the date and time with Terminal Server only when you vary the network description for Terminal Server, type *NO.
16. In the **Windows NT License Key** box, specify the CD key that Microsoft provides. In most cases, this CD key is printed on the back of the Terminal Server CD-ROM jewel case.

17. In the **License Type** box, specify the type of Terminal Server license that you purchased.
18. If you specified *PERSERVER in the **License Type** box, in the **Client Licenses** box, specify the number of client licenses that you purchased.
19. In the **Restricted Device Resources** box, type the value from Table 2.
20. If you want to install a keyboard type other than the default on the Terminal Server, press F10=Additional parameters. Specify the keyboard layout identifier in the **Keyboard Layout** box. Prompting for this parameter shows the keyboard layout identifiers that are available on the Terminal Server installation CD-ROM.
21. Provide any other information on the screen that seems relevant for your needs and press ENTER.

Terminal Server starts to install. The install process takes between 15 and 45 minutes to finish, depending on what hardware you have and how you have configured it. When this stage completes, the AS/400 displays the message "NTA100F - First phase of install completed for server in the job log." At that time, the console attached to the Integrated PC Server starts.

Installing Terminal Server on an AS/400 (Terminal Server-side Tasks)

When the AS/400 phase of the Terminal Server installation completes, the Integrated Netfinity Server starts. The Terminal Server phase of the installation begins. The Terminal Server phase of the installation has four parts (known as *modes*). You do not need to take any action during the first three modes. The Terminal Server console restarts after each mode. Information provided with the INSTWNTSVR command makes this phase of the installation easy. However, Terminal Server installation does require you to enter some information.

To complete the installation of Windows NT Server, perform these tasks:

1. If the installation program prompts you for a non-upgrade version of the Terminal Server CD-ROM, insert the non-upgrade version. Then press ENTER to continue with the installation.

Note If the installation program prompts you again for the non-upgrade CD, just press ENTER again.

2. After the first three modes complete, the console screen that is attached to the Integrated PC Server displays the Microsoft License. In the background, a title reads "AS/400 Integration with Windows NT Server." At the beginning of this mode, the INSWNTSVR command displays Internet address information for the internal LAN. Record this information in Table 2. You will need it later.
3. In the **Administration Account** dialog box, type and confirm the password.
4. In the **Windows NT Server Setup** dialog box, click **Next**.

5. The installation program prompts you for TCP/IP information with the following error message:

   ```
   Error (Unattended Setup)
   The IP Address key in the TCP/IP section of the database must be set
   to a value. Please correct the problem after the property sheet is
   displayed.
   ```

   Click **OK** and provide the Internet address from Table 2.
6. The installation program prompts you for the subnet mask with the following error message:

   ```
   Error (Unattended Setup)
   The subnet mask that you have entered for the IP address is not set
   to  a value. Please correct the problem after the property sheet is
   displayed.
   ```

   Click **OK**.
7. In the **Adapter** box, select **(1) AS/400 Virtual Token Ring Adapter**.
8. In the **IP Address** and **Subnet Mask** boxes for the internal LAN, enter the values that you recorded in Table 2 from the INSWNTSVR command display.
9. Enter the Internet address information for the remaining LAN adapters for Terminal Server:
10. In the **Adapter** box, select an adapter card.
11. Fill in the **IP Address** and **Subnet Mask** fields with the values from Table 2.
12. Fill in the correct value in the **Default Gateway** field.
13. Configure any additional TCP/IP properties required for the installation that you did not configure on the INSWNTSVR command. You can configure Properties for Domain Name System (DNS), Domain name, and Windows Internet Name Services (WINS) now.
14. If you get other error messages, click **OK**. At this time, you can correct the situation or provide the necessary information.
15. On the **Date/Time Properties** screen:
    - Select the time zone that matches your offset from Greenwich Mean Time (recorded in Table 1).
    - Uncheck **Automatically adjust clock** option. This ensures that the time is synchronized.
16. Configure the display adapter. Select the display color palette, resolution, and refresh frequency for the SVGA monitor that is connected to the Integrated PC Server.
17. When installation is complete, the sign-on screen appears.

Installing MetaFrame on an AS/400

1. After the sign-on screen appears (Step 17 above), log on to Terminal Server.
2. Insert the MetaFrame CD in to the CD-ROM drive.
3. In the **MetaFrame Auto-Run** dialog box, choose **MetaFrame Setup** from the list of on-screen options.
4. See the *MetaFrame Installation Guide* to complete the installation and set up.

IBM Netfinity 3000

This section describes how to install MetaFrame on an IBM Netfinity 3000 system. The IBM Netfinity 3000 offers solutions for your file-and-print and application computing needs.

Software Requirements

- MetaFrame Version 1.0 or later
- Microsoft Windows NT Server, Terminal Server Edition

Installing MetaFrame

1. Install Terminal Server following the directions in “Installing Terminal Server” later in this chapter.
2. When prompted to autodetect mass storage controllers, press ENTER to detect the Atapi Version 1.2 IDE CD-ROM controller and the Adaptec AIC-78xx driver for Microsoft Windows NT.
3. Complete Terminal Server installation.
4. After the system reboots, log on to the Terminal Server console as an administrator.
5. Insert the MetaFrame compact disk into the CD-ROM drive and begin installing MetaFrame following the instructions in the Citrix MetaFrame documentation.

IBM Netfinity 3500

This section describes how to install MetaFrame on an IBM Netfinity 3500 system. IBM Netfinity 3500 servers are the new generation foundations foryour networked computing and e-business needs today and into the future.

Software Requirements

- MetaFrame Version 1.0 or later
- Microsoft Windows NT Server, Terminal Server Edition
- SCSI-7800 Device Drivers, Version 2.11 or later

Installing MetaFrame

1. Obtain the SCSI-7800 Device Driver and Utilities Version 2.11 by contacting IBM Support or visiting the IBM Web site at http://www.pc.ibm.com/servers
2. Install Terminal Server following the directions in “Installing Terminal Server” later in this chapter.
3. When prompted to autodetect mass storage controllers, press ENTER to detect the Atapi Version 1.2 IDE CD-ROM controller.
4. Press **S** to configure additional SCSI controllers.
5. Expand the list of SCSI controllers, select **Other** (located at the end of the list), and press ENTER.
6. Insert the SCSI-7800 Device Driver/Utilities Diskette and click **OK**. The device drivers on the diskette are displayed. Select the Adaptec AIC-78xx driver for Microsoft Windows NT 4.0 and press ENTER to continue.
7. Complete Terminal Server installation.
8. After the system reboots, log on to the Terminal Server console as an administrator.
9. Insert the MetaFrame compact disk in the CD-ROM drive and choose **MetaFrame Setup** from the list of on-screen options.
10. Install MetaFrame following the instructions in the Citrix MetaFrame documentation.

IBM ServeRAID Netfinity 5500

This section describes how to install MetaFrame on an IBM ServeRAID Netfinity 5500 system. The IBM Netfinity 5500 server has the power, scalability, and manageability for today's complex network systems demands. There is support for two-way SMP integral tape drives and the ultra-fast 10,000-rpm hard disk drives. Fully in step with Intel's processor technology, Netfinity 5500 is the powerful and reliable foundation upon which you can run your business-critical applications.

Software Requirements

- MetaFrame Version 1.0 or higher
- Microsoft Windows NT Server, Terminal Server Edition
- IBM PC ServeRAID Device Driver and Utilities (Version 2.0 or later)

Installing MetaFrame

1. Obtain the IBM PC ServeRAID Device Driver and Utilities Version 2.00 by contacting IBM Support.
2. Install Terminal Server following the directions in "Installing Terminal Server" later in this chapter.
3. When prompted to autodetect mass storage controllers, press **S** to detect the Atapi Version 1.2 IDE CD-ROM controller.
4. Press **S** to configure additional SCSI controllers.
5. Expand the list of additional SCSI controllers, select **Other** (located at the end of the list), and press ENTER.
6. When prompted for a driver diskette, insert the IBM PC ServeRAID Adapter Device Driver/Utilities Diskette and press ENTER. The device drivers on the diskette are displayed. Select the IBM PC ServeRAID Adapter driver and press ENTER to continue.

   The ServeRAID Adapter **must** be installed first or the installation process will hang.
7. Complete Terminal Server installation.
8. After the system reboots, log on to the Terminal Server console as an administrator.
9. Insert the MetaFrame CD into the CD-ROM drive and choose **MetaFrame Setup** from the list of on-screen options.
10. Install MetaFrame following the instructions in the Citrix MetaFrame documentation.

IBM Netfinity 5600

This section describes how to install Citrix MetaFrame and Microsoft Windows NT 4.0, Terminal Server Edition, on an IBM Netfinity 5600 Server.

Software Requirements

- Microsoft Windows NT 4.0, “Terminal Server Edition, Version 4.0 or later
- MetaFrame Version 1.0 or higher
- IBM ServeRAID Device Drivers, Version 3.10 (or higher)
- IBM Netfinity 10/100 Fault Tolerant Adapter Device Drivers, Version 1.01 (or higher)

Before Installation

1. Obtain the required device drivers by contacting IBM Support or visiting their Web site at http://www.pc.ibm.com/support?page=brand&brand=IBM +PC+Server%7CNetfinity+5000.
2. Create Windows Terminal Server boot disks. From the console of a Windows NT 4.0 workstation or server, start a DOS prompt and type **winnt32 /ox** from the \I386 directory on the Windows Terminal Server CD-ROM and follow the on-screen instructions.

Installing Terminal Server and MetaFrame

1. Insert Terminal Server Edition boot disk #1, turn on the machine, and follow the on-screen instructions.
2. When prompted to autodetect mass storage controllers, press **S** to skip mass storage detection.
3. Press **S** to configure additional SCSI adapters.
4. Expand the list of additional SCSI adapters, select **Other** (located at the end of the list), and press ENTER.
5. When prompted for a driver diskette, insert the IBM ServeRAID Device Drivers diskette and press ENTER. Select the IBM ServeRAID Adapter and press ENTER to continue.
6. Press **S** to configure additional SCSI adapters. Expand the list of additional SCSI adapters, select the select IDE CD-ROM (ATAPI 1.2) / Dual-channel PCI IDE controller, and press ENTER to continue.
7. See the *Microsoft Windows Terminal Server Installation Guide* to continue the installation.
8. From the **Network Adapters** dialog box, click **Select from list…** to display the **Select Network Adapter** dialog box.

9. Click **Have Disk…** and insert the IBM Netfinity 10/100 Fault Tolerant Device Drivers diskette. Click **OK** to continue.
10. Select the AMD PCNET adapter and click **OK** to continue.
11. See the *Microsoft Windows Terminal Server Installation Guide* to complete the installation.
12. Insert the MetaFrame CD-ROM and choose **MetaFrame Setup** from the list of on screen options.
13. See the *MetaFrame Administrator's Guide* to complete installation and setup.

IBM Netfinity 7000 Server

This section describes how to install Terminal Server and MetaFrame on an IBM Netfinity 7000 system.

The IBM Netfinity 7000 is a high-performance, symmetric multiprocessing (SMP) server that is ideally suited for networking environments requiring superior microprocessor performance, efficient memory management, flexibility, and large amounts of data storage, utilizing hot-swap drive bays for added reliability. The IBM Netfinity 7000 provides both Extended Industry-Standard Architecture (EISA) and high-performance Peripheral Component Interconnect (PCI) expansion slots.

Software Requirements

- MetaFrame Version 1.0 or later
- Microsoft Windows NT Server, Terminal Server Edition
- IBM PC ServeRAID Device Driver and Utilities (Version 2.82 or later)

Installing MetaFrame

1. Obtain the IBM PC ServeRAID Device Driver and Utilities Version 2.82 by contacting IBM Support or visiting the IBM Web site at http://www.pc.ibm.com/servers
2. Install Terminal Server following the directions in “Installing Terminal Server” later in this chapter.
3. During Setup, press **S** to manually configure SCSI controllers.
4. Expand the list of SCSI controllers, select **Other** (located at the end of the list), and press ENTER.
5. When prompted for a driver diskette, insert the IBM PC ServeRAID Adapter Device Driver /Utilities Diskette and press ENTER. The device drivers on the diskette are displayed. Select the IBM PC ServeRAID Adapter driver and press ENTER to continue.

   The ServeRAID Adapter **must** be installed first or the installation process will hang.
6. Press **S** to configure additional SCSI controllers. Select Adaptec AHA294x/AIC78xx and IDE CD-ROM (ATAPI v1.2 PCI).
7. Complete Terminal Server installation.
8. After the system reboots, log on to the Terminal Server console as an administrator.
9. Insert the MetaFrame compact disk in the CD-ROM drive and choose **MetaFrame Setup** from the list of on-screen options.

10. Install MetaFrame following the directions in the Citrix MetaFrame documentation.

IBM Netfinity 7000 M10

This section describes how to install Terminal Server and MetaFrame on an IBM Netfinity 7000 M10 system.

The IBM Netfinity 7000 M10 is a high-performance, symmetric multiprocessing (SMP) server that is ideally suited for networking environments requiring superior microprocessor performance, efficient memory management, flexibility, and large amounts of data storage, utilizing hot-swap drive bays for added reliability. The IBM Netfinity 7000 M10 provides both Extended Industry-Standard Architecture (EISA) and high-performance Peripheral Component Interconnect (PCI) expansion slots. The M10 adds the processing power of up to four Intel Pentium II Xeons.

Software Requirements

- MetaFrame Version 1.0 or later
- Microsoft Windows NT Server, Terminal Server Edition
- Adaptec AIC-7895 SCSI Drivers Version 1.34 (or higher)

Installing MetaFrame

1. Obtain the Adaptec AIC-7895 SCSI Drivers Version 1.34 by contacting IBM Support or visiting the IBM Web site at http://www.pc.ibm.com/servers
2. Install Terminal Server following the directions in “Installing Terminal Server” later in this chapter.
3. When prompted to autodetect mass storage controllers, press ENTER to detect the Atapi Version 1.2 IDE/PCI CD-ROM controller.
4. Press **S** to configure additional SCSI controllers.
5. Expand the list of SCSI controllers, select **Other** (located at the end of the list), and press ENTER.
6. When prompted for a driver diskette, insert the Adaptec AIC-7895 SCSI drivers Version 1.34 disk and press ENTER. The device drivers on the diskette are displayed. Select the Windows NT 4.0 SCSI adapter driver and press ENTER to continue.
7. Complete Terminal Server installation.
8. After the system reboots, log on to the Terminal Server console as an administrator.
9. Insert the MetaFrame compact disk in the CD-ROM drive and choose **MetaFrame Setup** from the list of on-screen options.
10. Install MetaFrame following the directions in the Citrix MetaFrame documentation.

IBM Netfinity 7000 M10 (86802RU)

This section describes how to install Citrix MetaFrame and Microsoft Windows NT Server, Terminal Server Edition, on an IBM Netfinity 7000 M10 system.

The IBM Netfinity 7000 M10 is a high-performance, symmetric multiprocessing (SMP) server that is ideally suited for networking environments requiring superior microprocessor performance, efficient memory management, flexibility, and large amounts of data storage, utilizing hot-swap drive bays for added reliability. The IBM Netfinity 7000 M10 provides both Extended Industry-Standard Architecture (EISA) and high-performance Peripheral Component Interconnect (PCI) expansion slots. The M10 adds the processing power of up to four Intel Pentium II Xeons.

Requirements

Software Requirements

- Microsoft Windows NT Server, Terminal Server Edition
- MetaFrame Version 1.0
- Adaptec 7800 Family Manager Set for Windows NT 4.0, Version 3.01 or higher
- IBM ServeRaid Adapter Device Drivers, Version 3.00.18 or higher
- IBM 100/10 EtherJet PCI Adapter Device Drivers, Version 2.5 or higher
- S3 Incorporated Video Adapter Device Drivers, Version 3.24.10 or higher

Hardware Requirements

- External SCSI cable (IBM Part No. 76H3589)
- External half-high SCSI storage enclosure (IBM Part No. 3510020)
- Netfinity 4.51G 10K Wide Ultra SCSI hard disk drive (IBM Part No. 01K8009)

Before Installation

1. Obtain the required device drivers by contacting IBM Support or visiting the IBM Web site at http://www.pc.ibm.com/servers.
2. Create Windows Terminal Server boot diskettes. At a DOS prompt, type **winnt32 /ox** from the \I386 directory on the Windows Terminal Server CD-ROM and follow the on-screen instructions.
3. Install the Netfinity hard disk drive in the external SCSI enclosure and connect it to the Adaptec SCSI controller card's external port using the SCSI cable.

Installing Terminal Server and MetaFrame

1. Insert Terminal Server boot disk #1, turn on the machine, and follow the on-screen instructions.
2. When prompted to autodetect mass storage controllers, press **S** to skip mass storage detection.
3. Press **S** to configure additional SCSI adapters.
4. Expand the list of additional SCSI adapters, select **Other** (located at the end of the list), and press ENTER.
5. When prompted for a driver diskette, insert the IBM ServeRaid Device Drivers diskette and press ENTER. Select the IBM ServeRaid Adapter and press ENTER to continue.
6. Press **S** to configure additional SCSI adapters, select **Other**, and press ENTER.
7. When prompted for a driver diskette, insert the Adaptec 7800 Family Manager Device Drivers diskette and press ENTER. Select the Adaptec AIC-78XX PCI SCSI controller (NT 4.0) and press ENTER to continue.
8. Press **S** to configure additional SCSI adapters. Expand the list of additional SCSI adapters, select the IDE CD-ROM (ATAPI 1.2)/PCI IDE controller, and press ENTER to continue.
9. When prompted to choose where to install Terminal Server, select the external (non-RAID) hard disk drive and press **C** to create a partition.

Note It is recommended that you create a 1000MB partition for the installation of Terminal Server, leaving the bulk of the hard disk to be used for the page file.

10. Refer to the Microsoft Windows Terminal Server *Installation Guide* to continue the installation.
11. From the **Network Adapters** dialog box, click **Select from list…** to display the **Select Network Adapter** dialog box.
12. Click **Have Disk…** and insert the IBM 100/10 EtherJet PCI adapter diskette. Click **OK** to continue.
13. Select the IBM 100/10 EtherJet PCI adapter and click **OK** to continue.
14. Refer to the Microsoft Windows Terminal Server *Installation Guide* to complete the installation.
15. Insert the MetaFrame Version 1.0 CD and choose **MetaFrame Setup** from the list of on-screen options.
16. See the MetaFrame *Administrator's Guide* to complete installation and set up.

Video Card Adapter Installation

During system installation, the standard video driver supplied with Terminal Server is automatically installed. To obtain larger screen sizes and video color depth, you must install the manufacturer's supplied video driver. The following procedure outlines how to install the correct video driver.

1. Click Start, select **Settings**, then click Control Panel.
2. In Control Panel, double click **Display**.
3. Select the **Settings** tab and then click the **Display Type...** button.
4. In the **Adapter Type** field, click the **Change...** button. The **Change Display** dialog box appears.
5. Click the **Have Disk...** button.
6. Insert the new display driver diskette into drive A, then click **OK**.
7. From the list of displayed S3 devices, select your S3 device.
8. From **Third-party Drivers**, click **Yes** to proceed. If you receive the message "The driver is already installed on the system" and are asked to use the current or new drivers, click **New**.
9. If prompted for the driver diskette a second time, click **Continue**.
10. When you receive the message "The drivers were successfully installed," remove the display driver diskette, then click **OK**.
11. Click **Close** twice.
12. Click **Yes** to reboot the server.

IBM PC Server 330

This section describes how to install MetaFrame on an IBM PC Server 330 system.

The IBM PC Server 330 is a high-speed, upgradeable PC server-class system with large data storage capacity and improved system expandability. The PC Server 330 provides both Extended Industry-Standard Architecture (EISA) and high-performance Peripheral Component Interconnect (PCI) expansion slots.

Software Requirements

- MetaFrame Version 1.0
- Microsoft Windows NT Server, Terminal Server Edition
- IBM PC ServeRAID Device Driver and Utilities Version 1.40

Installing MetaFrame

1. Install Terminal Server following the directions in "Installing Terminal Server" later in this chapter.
2. When prompted whether to autodetect mass storage controllers , press **S** to skip mass storage detection and **S** again to specify additional SCSI adapters.
3. Insert the IBM ServeRAID Device Driver and utility diskette, press ENTER until the IBM PC ServeRAID Adaptor is displayed. Press ENTER to accept the driver and then press ENTER to continue.
4. Complete Terminal Server installation.
5. After the system reboots, log on to the Terminal Server console as an administrator.
6. Insert the MetaFrame CD into the CD-ROM drive and begin installing MetaFrame following the instructions in the Citrix MetaFrame documentation.

IBM PC Server 704

This section describes how to install MetaFrame on an IBM PC Server 704 system.

The IBM PC Server 704 is a high-performance, symmetric multiprocessing (SMP) server that is ideally suited for networking environments requiring superior microprocessor performance, efficient memory management, flexibility, and large amounts of reliable data storage. The PC Server 704 provides both Extended Industry-Standard Architecture (EISA) and high-performance Peripheral Component Interconnect (PCI) expansion slots.

Software Requirements

- MetaFrame Version 1.0
- Microsoft Windows NT Server, Terminal Server Edition
- IBM PC ServeRAID Device Driver and Utilities (Version 2.0 or later)

Installing MetaFrame

1. Install Terminal Server following the directions in “Installing Terminal Server” later in this chapter.
2. When prompted whether to autodetect mass storage controllers, press ENTER to detect the IDE CD-ROM (Atapt 1.2)/ PCI IDE and Adaptec AHA-294X/AHA-394X/AIC-78XX SCSI controllers.
3. Press **S** to specify additional SCSI adapters.
4. Insert the IBM ServeRAID Device Driver and utility diskette. Press ENTER until the IBM PC ServeRAID Adapter is displayed. Press ENTER to accept the driver and then press ENTER to continue.
5. Complete Terminal Server installation.
6. After the system reboots, log on to the Terminal Server console as an administrator.
7. Insert the MetaFrame CD into the CD-ROM drive and begin installing MetaFrame following the directions in the Citrix MetaFrame documentation.

NetFrame NF9000

NetFrame Systems Inc. manufactures high-end computer systems. Their 9000 series system provides scalability in the processing, memory, and disk subsystems that allow significant growth. Other available features such as error correcting memory, hot swappable RAID configurations, and compact rack-mounted systems provide a powerful computing environment for running the MetaFrame server.

Software Requirements

- MetaFrame Version 1.0 or higher
- Microsoft Windows NT Server, Terminal Server Edition

Installing MetaFrame

1. Install Terminal Server following the directions in "Installing Terminal Server" later in this chapter.
2. When installation is complete and the computer reboots, log on as an administrator.
3. Insert the MetaFrame CD into the CD-ROM drive and choose **MetaFrame Setup** from the list of on-screen options.
4. Install MetaFrame following the directions in the Citrix MetaFrame documentation.

Sequent NTS-2000

This section describes how to install MetaFrame on a Sequent NTS-2000 system.

Software Requirements

- MetaFrame Version 1.0 or later
- Microsoft Windows NT Server, Terminal Server Edition

Installing MetaFrame

1. Install Terminal Server following the directions in “Installing Terminal Server” later in this chapter.

   Note During installation, Setup might inform you that the system has one or more hard drives that has more than 1024KB. This does not indicate an error condition, but is merely additional information informing you that the hard drive is larger than the size for which it is configured.

2. When prompted to autodetect mass storage controllers, press ENTER.
3. Complete Terminal Server installation.
4. After the system reboots, log on to the Terminal Server console as an administrator.
5. Insert the MetaFrame CD into the CD-ROM drive and choose **MetaFrame Setup** from the list of on-screen options.
5. Set up MetaFrame following the directions in the Citrix MetaFrame documentation.

Unisys Aquanta ES (ES204131)

This section describes how to install Citrix MetaFrame and Microsoft Windows NT 4.0 “Terminal Server Edition” on a Unisys Aquanta ES server.

Software Requirements

- Microsoft Windows NT 4.0 “Terminal Server Edition” Version 4.0 or later
- MetaFrame Version 1.0 or higher
- American Megatrends MegaRAID Device Drivers v2.12 or later
- 3Com Fast Etherlink XL PCI Device Drivers v4.01 or later
- Cirrus Logic GD5480 Video Device Drivers for Windows NT v1.22 or later

Pre-installation Steps

1. Obtain the required Device Drivers by contacting Unisys Support or visiting the web site http://www.service.unisys.com/.
2. Create Windows Terminal Server Boot Disks. From the console of an NT 4.0 workstation or sever start a DOS prompt and type winnt32 /ox from the \i386 directory on the Windows Terminal Server CD-ROM and follow the on screen instructions.

Terminal Server Edition and MetaFrame Installation

1. Insert Terminal Server Edition Boot disk #1, turn on the machine, and follow the on-screen instructions.
2. When prompted to autodetect mass storage controllers, press ENTER to detect.
3. Press S to configure additional mass storage controllers.
4. Expand the list of additional SCSI adapters, select **Other** (located at the end of the list), and press ENTER.
5. When prompted for a driver diskette insert the American Megatrends MegaRAID device driver diskette into A:\ and press ENTER. Select the MEGARAID NT SCSI Driver and press ENTER to continue.
6. Refer to the Microsoft Windows Terminal Server Installation Guide to continue the installation.
7. From the Network Adapters screen, click “Select from list…” to display the “Select Network Adapter” screen.
8. Click “Have Disk…” and insert the 3Com Fast EtherLink XL PCI device drivers diskette. Click “OK” to continue.
9. Select the 3Com Fast EtherLink XL PCI (3C905b-TX) Adapter and click “OK” to continue.
10. Insert the MetaFrame CD and choose MetaFrame Setup from the list of on screen options.
11. Refer to the MetaFrame *Installation Guide* and to complete the installation and setup.

Video Card Adapter Installation

Note During system installation the standard video driver supplied with Terminal Server is automatically installed. To obtain larger screen sizes and video color depth you must install the manufacturer’s supplied video driver. This procedure outlines how to install the correct video driver.

1. From **Start**, select the **Settings** group, then click the **Control Panel** icon.
2. In the Control Panel, double click the **Display** icon.

3. In the Settings dialog box, click the **Display Type...** button.
4. In the **Adapter Type** section of the **Display Type** dialog box, click the **Change...** button.
5. In the **Change Display** dialog box, click the **Have Disk...** button.
6. Insert the new display driver diskette into the A:\ drive, then click the **OK** button.
7. From the list of displayed Cirrus Logic devices, select the Cirrus Logic CL-GD5480 Graphics Adapter device.
8. From **Third-party Drivers**, click the **Yes** button to proceed. If the message "The driver is already installed on the system" appears and asks to use the current or new drivers, click the **New** button.
9. If prompted for the driver diskette a second time, click the **Continue** button.
10. When the message "The drivers were successfully installed" is displayed, remove the display driver diskette, then click the **OK** button.
11. Back at the **Display Type** dialog box, click the **Close** button.
12. Back at the **Display Properties** dialog box, click the **Close** button.
13. At the **System Settings Change** dialog box, click **Yes** to reboot the server.

MetaFrame Servers and NT Domains

MetaFrame can be used in one of two ways: as a stand-alone server or as a server on a network domain. MetaFrame inherits the properties of the Terminal Server on which it is installed. When you install Terminal Server, you can configure it as a server or as a domain controller.

When installed as a server, MetaFrame can be used as a stand-alone system or it can join an existing network domain. If your MetaFrame server is not joining an existing domain and you do not anticipate having more than one MetaFrame server (for example, if you are adding a single MetaFrame server to an existing NetWare network for Dial-In user access), you do not need to establish a domain. If your configuration will eventually expand past a single MetaFrame server, establishing a domain avoids the need to recreate users on each additional server.

If you set up MetaFrame as a domain controller, it becomes the central point for a new network domain. Other servers can join this network domain. Usually the best configuration is to make one MetaFrame server a domain controller and configure all other MetaFrame servers as servers on that network domain. During MetaFrame Setup, you are given the option of joining a network domain. In this case, you select the name of the domain used on the domain controller to join the network domain. Setting up a domain allows your MetaFrame and Terminal Server systems to work together. You can also leave the MetaFrame server in its own network workgroup, which is the default; the system becomes a stand-alone system and is unaware of the domain.

Note If you do not add the server to a network domain when you install Terminal Server, you can join a domain later by using the Network application in Control Panel.

Installing Terminal Server

You must install and configure Terminal Server before you install MetaFrame. Before you install Terminal Server, make sure the following information is available:

- The types of SCSI adapters and devices on your servers
- The types of network adapters you plan to use and any disks that were provided by the vendors

Note Terminal Server cannot be installed on drives altered with a compression utility.

You can install Terminal Server:

- Using the Terminal Server boot diskettes
- Over an existing Windows NT, Terminal Server, *WINFRAME*, or MetaFrame installation using the Winnt32.exe program
- From a DOS prompt using the Winnt.exe program

Tip Citrix recommends using the boot diskettes provided with Terminal Server to perform the installation because you can then partition and format the target hard disk drives as necessary. The other two methods do not support reformatting of the drive containing the installation files.

Use one of the other methods only if you do not have a CD-ROM drive on the server and want to perform the installation across the network. In that case, boot the server in DOS, format the system partition, and then install Terminal Server across the network, converting the drive to NTFS from FAT in the process.

If the installation disks, also called boot diskettes, that are supplied with Terminal Server are lost or misplaced, you can create them on an existing Windows NT, Windows Terminal Server, or *WINFRAME* or MetaFrame server using the Winnt32.exe program as follows:

1. Have three blank, formatted, high-density 3.5-inch floppy disks ready. Label the formatted disks “Setup Boot Disk,” “Setup Disk#2,” and “Setup Disk#3.”
2. Insert the Terminal Server CD in the CD drive.

3. At a command prompt, change to the \I386 directory on the CD-ROM.
4. Once in this directory, type **winnt32 /ox** and press ENTER.
5. When prompted, insert Setup Disk #3 in drive A. After some files are copied to Setup Disk #3, you are prompted to insert Setup Disk #2 and then the Setup Boot Disk in drive A.

To install a fresh copy of Terminal Server using the boot diskettes, perform the following steps:

1. Insert the Terminal Server Setup Boot Disk into the server's drive A and start the server.

   An installation screen appears.
2. Insert disk #2 in drive A. Setup loads the drivers for Terminal Server installation to boot and the Windows NT name, version, and build number are displayed. Also displayed are the Terminal Server build number, the number of processors, and the amount of memory detected in the system.
3. Press ENTER to continue the installation.
4. Setup gives you a choice of autodetecting the mass storage devices or selecting them manually. In the latter case, Setup allows you to manually select SCSI adapters, CD-ROM drives, and special disk controllers for installation. Citrix recommends that you allow Setup to autodetect the devices.
5. Insert Disk #3 in drive A and press ENTER when prompted. Setup lists all the recognized mass storage devices. Type **S** to specify additional SCSI adapters, CD-ROM devices, or special disk controllers for use with Terminal Server; otherwise press ENTER to continue Setup.
6. After completing the mass storage device setup, Setup prompts for the Terminal Server compact disk.

   The End-User License Agreement (EULA) is displayed. Read the EULA and press F8 if you accept the terms and conditions in the agreement.
7. Setup performs a search to detect any previous installations of Terminal Server or *WINFRAME*. If you are installing a fresh copy of Terminal Server, select **N** for new install
8. Setup lists your computer type, video display, mouse, keyboard, and keyboard layout. Citrix recommends that you leave these settings unchanged. Press ENTER when done.
9. You are asked for a target location to install Terminal Server. You also have a choice of creating or deleting partitions at this point.
10. Select the newly created partition or an existing partition as the target and press ENTER.
11. You can choose to format this partition as either FAT or NTFS or leave it unchanged. To restrict and audit user access, Citrix recommends formatting the partition as NTFS.

12. Specify the directory to install Terminal Server. By default, Terminal Server is installed in the \Wtsrv directory.
13. Setup asks if you want to perform an exhaustive secondary examination of all existing partitions. Press ENTER to perform this examination or ESC to skip it.
14. When the examination is complete, files are copied to the server. Setup has completed the text-based portion of the install and is ready to reboot. Remove any disks and CDs from their drives and press ENTER to restart the computer.
15. The server restarts with the GUI setup. Follow the on-screen prompts to install and configure Terminal Server, keeping the following in mind:
    - Install all the protocols for which you will be creating ICA connections. To minimize resource allocations, install **only** the protocols required.
    - Setting up Terminal Server as a domain controller causes greater load on the server because it must authenticate domain logons and maintain the directory database for a domain.
    - Screen savers cause unnecessary load and should not be installed.
    - Install only the Terminal Server services that you need.
    - Create an Emergency Repair Disk for your system. Do not forget to update this disk after making changes to your system configuration; for example, after renaming drives when installing MetaFrame.

Installing MetaFrame

If you are deploying only one or two MetaFrame servers, a typical interactive installation, running Setup.exe on each server, is fine. However, if you have a large number of servers to deploy, you may prefer to use unattended setup.

You can run an unattended setup to perform a new installation or an upgrade of a MetaFrame server without being present. Unattended setup mode uses an optional answer file to provide answers to the questions asked during Setup. If you do not use an answer file, or if you use an answer file but do not specify answers to some questions, default answers are used for those questions.

You can accommodate a variety of server configurations by creating multiple answer files and tailoring them to the specifics of each type of server you are deploying. Similar server configurations require only minor changes in the answer files.

For step-by-step instructions on installing MetaFrame and additional information on unattended installation, see the *MetaFrame Administrator's Guide*.

Creating Server Farms

Published applications:

- Give ICA Client users easy access to applications running on Citrix servers
- Increase your control over application deployment
- Shield users from the mechanics of the Windows NT server environment hosting the ICA session

The Citrix utility Published Application Manager, with its support for server farms and Program Neighborhood, is the main tool for publishing applications.

When you publish applications, user access to those applications is greatly simplified in three areas:

- **Addressing**. Instead of connecting to a Citrix server by its IP address or server name, ICA Client users can connect to a specific application by whatever name you give it. Connecting to applications by name eliminates the need for users to remember which servers contain which applications.
- **Navigation of the server desktop**. Instead of requiring client users to have knowledge of the Windows NT 4.0 and/or 3.51 desktop (Windows NT Explorer or Program Manager) to find and start applications after connecting to Citrix servers, published applications present the ICA Client user with only the desired application in an ICA session.
- **User authentication**. Instead of logging on and logging off multiple Citrix servers to access applications, Program Neighborhood users can authenticate themselves a single time to all servers and obtain immediate access to all applications configured for their user group or specific user name. Also, publishing applications for the special Citrix *anonymous* user group lets you completely eliminate the need for user authentication for those applications you want to provide to all users on your network.

Citrix server farms provide you with a flexible and robust way of deploying applications to ICA Client users. Server farms let you centralize your control over the application deployment process by grouping Citrix servers into a single administrative unit. Citrix servers in a farm function together to make applications easily available to your ICA Client users.

A *server farm* is a group of Citrix servers managed as a single entity and that share some form of physical connection and a common base of user accounts. After you place your servers in a server farm, you can publish applications on servers in the farm for users in the common base of accounts. After starting Program Neighborhood, a user logs in once, then sees an application set containing each application configured for his or her specific user account or user group.

For more information server farms and how to create them, see the*MetaFrame Administrator's Guide* and the online help for Published Application Manager.

Modem Pooling Hardware Device Notes

This section contains notes for popular modem pooling hardware devices.

Digi AccelePort PCI Host Adapter with AccelePort Modem/4em

The Digi AccelePort PCI adapter card together with the AccelePort Modem/4em provides four external modems in one box. When installed and configured on a MetaFrame server, the AccelePort system can be used for incoming remote asynchronous ICA sessions and as an outgoing modem pool. This document describes a tested configuration of Digi AccelePort Modem/4em with MetaFrame.

Requirements

Hardware

- Dell OptiPlex GXi with one Pentium processor
- Digi AccelePort PCI host adapter card
- AccelePort Modem/4em

Software

- MetaFrame Version 1.0
- Digi AccelePort Modem/4em Device Driver Version 2.3.0

Installing Digi AccelePort Adapter Card and Modem/4em

1. Turn the computer off, remove the computer cover, and select a PCI slot to install the controller.
2. Remove the expansion slot cover and insert the AccelePort host adapter card.
3. Replace the covers.
4. Connect the modem cable from the modem to the AccelePort adapter card and the power supply.
5. Restart the system.

Note With the system used for the test, conflicts with other PCI devices caused the system to freeze. The other PCI cards installed on the test configuration were an onboard video card, a SCSI adapter, and a multiport adapter. Information provided with the Digi AccelePort adapter suggested adding `/PCILOCK` to the end of the line in the Boot.ini file to boot to MetaFrame. This stopped the system from freezing but the video adapter no longer functioned. The problem was corrected by switching PCI slots for the AccelePort adapter card and the multiport adapter card.

Installing Digi AccelePort Device Driver

1. In Control Panel, double-click **Network**.
2. Click **Adapters** and then click **Add**.
3. Click **Have Disk**.
4. Insert the driver diskette and enter **A:\I386** for the path. Click **OK**.
5. In **OEM Option**, select **Digi AccelePort Xem-PCI Adapter** and click **OK**.
6. In Adapter Configuration Wizard, select **Modem/4em module**, click **Add**, and then **Next**.
7. Enter the starting COM port (COM3 was used in this test).
8. Click **OK** in Digi Xem (PCI) Adapter Setup.
9. Close the **Network** dialog box.
10. Restart the system.

Setting up Digi AccelePort Modem/4em

1. In Control Panel, double-click **Modems**.
2. Click **Add**.
3. Allow the modem installation procedure to detect the modem.
4. Select the first COM port used for the AccelePort Modem/4em and click **Next**.
5. When the Digi Modem/4em is found, click **Next**.
6. Select all ports in the range assigned to the AccelePort Modem/4em and click **Next**.
7. Enter location information and click **Next**.
8. Click **Finish** to complete the setup.
9. Click **Close**.

Terminal Connection Configuration using Digi AccelePort Modem/4em

1. Click **Start**, select **Programs**, then **Administrative Tools**, and then **Terminal Server Connection Configuration**.
2. From the **Terminal Connection** menu, select **New**.
3. Enter a connection name, select **Citrix ICA 3.0** for type, select A**sync** for transport, select one of the AccelePort Modem/4em COM ports for device, and then click **OK**.
4. In the **Reboot Message** dialog box, click **OK**.
5. Repeat Steps 1– 4 for additional terminal connections.
6. Reboot the server.

Configuring the 32-bit ICA Client to use Digi AccelePort Modem/4em

1. Expand the file Mdmdigi.in_ from the driver's diskette in Mdmdigi.inf.
2. Open the 32-bit ICA Client.
3. From the **Options** menu, select **Modems**.
4. Click **Add**.
5. Check **Don't detect my modem; I will select it from a list** and click **Next**.
6. Click **Have Disk**.
7. Enter the path to the Mdmdigi.inf file created in Step 1.
8. Select **Digi Modem/4em** and click **Next**.
9. Select the COM ports and click **Next**.
10. In the **Reboot Message** dialog box, click **OK**.
11. Reboot the server.

Citrix ICA 32-bit Clients can now access the AccelePort Modem/4em.

Verifying the Installation of Digi AccelePort Modem/4em

Follow the procedure below to verify that the Digi AccelePort Modem/4em is correctly installed and configured:

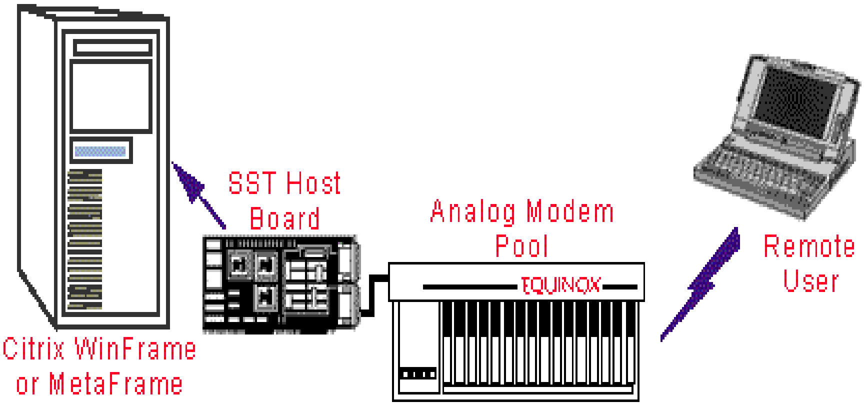
1. Connect the modem ports to phone ports.
2. Click **Start**. Select **Programs**, then **Accessories**, and then **Hyperterminal**.
3. Enter a name in **Connection Description** and click **OK**.
4. In **Connect To**, enter an area code and a phone number that can be used for testing.

5. In the pull-down list to the right of the **Connect** dialog box, select the first AccelePort Modem/4em.
6. In **Connect**, click **Dial**.
7. Verify the connection is made.
8. Repeat Steps 1– 7 for each AccelePort Modem/4em.

Equinox Analog Modem Pool

Note This section was provided by Equinox Systems, One Equinox Way, Sunrise, FL 33351. All trade names referred to are the Servicemark, Trademark, or Registered Trademark of the respective manufacturers.

The information contained in this document is subject to change without notice.



The Equinox Analog Modem Pool connects remote and local users directly to your Citrix MetaFrame server. The compact, integrated chassis is designed to use internal modems in four-unit banks. The Analog Modem Pool connects to the server through an Equinox host board that offloads communications processing from the server CPU, eliminates Ethernet protocol stacks, and reduces network traffic.

The Equinox Analog Modem Pool can be configured in fault-tolerant clustering options for mission-critical applications and high availability and is easily managed using the EquiView Plus management software. The modular design of the Equinox Analog Modem Pool allows expansion.

The Equinox Analog Modem Pool is fully compatible with MetaFrame Version 1.0. This product is a table-top (or rack-mounted) chassis designed to accommodate up to 16 industry standard internal ISA modems. The chassis is externally attached to an Equinox SST Expandable Host Controller and can be daisy-chained to support up to 128 modems from one slot in the server. The server slot containing the SST controller can be ISA, EISA, or PCI.

The Equinox Analog Modem Pool provides remote dial-in connectivity to Citrix ICA Clients. Users can remotely access MetaFrame servers and applications.

Requirements

Hardware Requirements

The server platform is configured with one of the following Equinox Expandable SuperSerial adapters attached to an Equinox Analog Modem Pool:

- SST-64I, P/N: 990268
- SST-128I, P/N: 990269
- SST-64P, P/N: 990303
- SST-128P, P/N: 990305
- SST-64E, P/N: 990270
- SST-128E, P/N: 990271
- Equinox Analog Modem Pool, P/N: 990308

Software Requirements

- Equinox NT/Citrix Device Driver Version 3.40 or higher
- Citrix MetaFrame Version 1.0
- Microsoft Windows NT Server, Terminal Server Edition

Installing and Configuring the Equinox Analog Modem Pool

Note It is assumed that Microsoft Terminal Server and Citrix MetaFrame are already installed on the server.

1. Install the Equinox SuperSerial adapter into any available slot in the MetaFrame server.
2. Connect one end of the expansion bus cable to the adapter card you just installed.
3. Connect the other end of the expansion bus cable to the Analog Modem Pool.
4. Install the ISA analog modems into the Analog Modem Pool.
5. Power on the Analog Modem Pool.
6. Power on the server PC. When the server boots, install the Equinox NT/Citrix device driver provided.

A. Log on to the Terminal Server console as an administrator.

B. From the Task Bar, click Start.

C. Click **Settings** and then **Control Panel**.

D. Double-click **Network**.

E. Select the Adapters tab.

F. Click **Add Adapter**.

G. Click **Have Disk**.

H. In the **Insert Disk** dialog box, type the drive where you installed the Equinox NT/Citrix device driver.

I. Follow the screen prompts and reboot the server for changes to take effect.

Terminal Server Connection Configuration

1. From the Task Bar, click **Start**.
2. Select **Programs**, **Administrative Tools**, and then **Terminal Server Connection Configuration**.
3. On the **Connection** menu, click **New**.
4. Configure each port in the **Connection** dialog box for each of the modems that are installed in the Analog Modem Pool.
5. When configuration is complete, exit **Terminal Server Connection Configuration**.
6. Click **Start**, **Programs**, **MetaFrame Tools**, **MetaFrame Administration**, and then **Sessions**. Make sure all of the entries you just created are listed and in a listen state.

The system is now ready to accept remote dial-in connections.

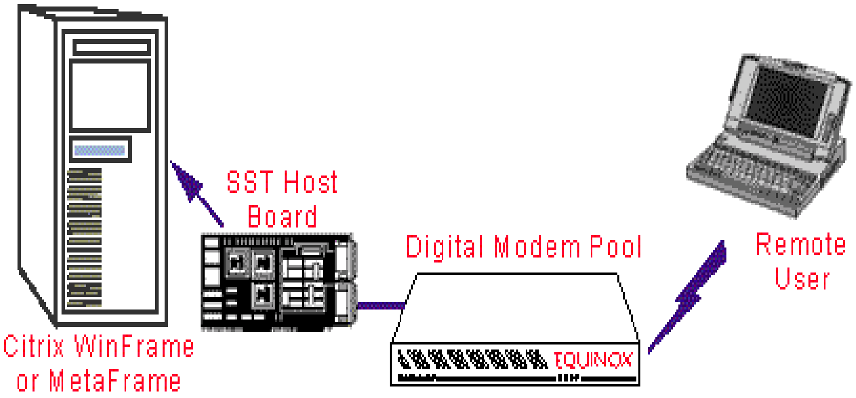
Troubleshooting

See the “Modem Pool Frequently Asked Questions (FAQ)” on the Equinox Web site at http://www.equinox.com/tech/mpoolfaq.html

Equinox Digital Modem Pool

Note This section was provided by Equinox Systems, One Equinox Way, Sunrise, FL 33351. All trade names referred to are the Servicemark, Trademark, or Registered Trademark of the respective manufacturers.

The information contained in this document is subject to change without notice.



The Digital Modem Pool is designed for T1 applications (E1 and ISDN PRI support planned for 1999). The Equinox Digital Modem Pool provides V.90/56K central site connections to any Windows NT server including Citrix MetaFrame, and supports off-the-shelf server-based Windows NT communications applications, including RAS, dial-up networking, and HyperTerminal. The Digital Modem Pool connects to the server through an Equinox host board that offloads communications processing from the server CPU.

This server-based remote access solution is scalable from 6 to 384 modems. The Digital Modem Pool is managed using the EquiView Plus management software and can be clustered for high availability.

The Equinox DMP is designed to support three types of WAN connectivity: DS-1, ISDN Primary Rate Interface (PRI), and E1. DS-1 support is currently available. Please contact Equinox Systems Inc. for information regarding availability of PRI and E1. The DMP also supports fractional T1 and is modularized to allow installation of 6 to 24 modems in increments of six modems. Up to four modem pools (four T1 lines and 96 modems) can be attached to one SuperSerial Expandable Host board, ISA or PCI, installed in the server platform. The T1 interface includes integrated CSU/DSU. The DMP is fully managed, locally or remotely, through SNMP-based EquiView Plus software. The DMP can be daisy-chained to DMPs, Equinox Analog Modem Pools, and Equinox Port Modules.

Requirements

Hardware Requirements

The server platform is configured with one of the following Equinox SuperSerial Expandable adapters and an Equinox Digital Modem Pool:

- SST-64I, P/N: 990268
- SST-128I, P/N: 990269
- SST-64P, P/N: 990303
- SST-128P, P/N: 990305
- Equinox Digital Modem Pool, P/N: 990309
- Six Modem Module, P/N: 990310

Software Requirements

- Windows NT Server, Terminal Server Edition
- Citrix MetaFrame, Version 1.0
- Equinox NT/Citrix Device Driver Version 4.00 or higher.
- Equinox EquiView Plus management software

Note It is assumed that Microsoft Terminal Server and Citrix MetaFrame are already installed on the server, and that channelized T1 services are provisioned and installed. (See the “Buying DS-1 Service” white paper on the Equinox Web site at http://www.equinox.com/product/dmp_5.html)

Installing the Digital Modem Pool

1. Install the Equinox SuperSerial adapter into any available slot in the server.
2. Connect one end of the expansion bus cable to the adapter card you just installed.
3. Connect the other end of the expansion bus cable to the Digital Modem Pool.
4. Install the Six Modem Modules into the Digital Modem Pool. See the Hardware Guide included with the Equinox Digital Modem Pool.
5. Plug in the power cord to the Digital Modem Pool.
6. Power on the server. When the server boots up, install the Equinox NT/Citrix device driver provided:

   A. Log on to the Terminal Server console as an administrator.

   B. From the Task Bar, click **Start**.

   C. Click **Settings** and then **Control Panel**.

   D. Double-click the Network icon.

E. Click the **Adapters** tab.

F. Click **Add**.

G. Click **Have Disk**.

H. In the **Insert Disk** dialog box, type the drive where you installed the Equinox NT/Citrix device driver.

I. Follow the screen prompts and reboot the server for changes to take effect.

Configuring the Digital Modem Pool

1. Log on to the Terminal Server as an administrator.
2. From the Task Bar, click **Start**.
3. Click **Settings** and then **Control Panel**.
4. Double-click Equinox Digital Modem Pool.

   A. Select **Digital Modem Pool** and click **Configure**.

   B. Select the appropriate frame type, signaling, line coding, and cable length for the DS-1 services being provided.

   C. Click **Next**.

   D. Click **Finish**.
5. Shut down and reboot the server for the settings to take effect.

Configuring the Terminal Server Connection

1. From the Task Bar, click **Start**.
2. Select **Programs**, **Administrative Tools**, and then **Terminal Server Connection Configuration**.
3. From the **Connection** pull-down menu, select **New**.
4. Configure each port in the **Connection** dialog box for the Six Modem Modules that are installed in the Digital Modem Pool.

   When a modem is identified using the detection routine, it is identified as an “Equinox Central Site V.90/K56 Flex Modem”.
5. When configuration is complete, exit **Terminal Server Connection Configuration**.
6. In **MetaFrame Administration**, make sure all of the entries you just created are listed and in the active state.

The system is now ready to accept remote dial in connections.

Troubleshooting

See the Equinox Web Site Technical Support at www.equinox.com.

Remote Access Server Hardware Device Notes

This section contains notes for popular remote access server hardware devices.

ExtendNet VPN Remote Access Server

Note The information in this section was provided by Extended Systems Inc., 5777 North Meeker Ave., Boise, ID 83713.

This section describes how to install and use the ExtendNet VPN to manage PC-to-LAN Virtual Private Network connections. By simply dialing a local Internet Service Provider (ISP) and using the industry-standard Point-to-Point Tunneling Protocol (PPTP), remote users can access their LAN (and, consequently, Citrix MetaFrame server) as if physically connected. All authentication from the Internet, encryption of packets, decryption of packets, and management of users is processed by the ExtendNet VPN server.

The primary benefits of utilizing the ExtendNet VPN for managing PC-to-LAN (MetaFrame server) connections are:

Security. ExtendNet VPN shields your mission-critical MetaFrame server from direct Internet access. Anyone desiring access to the MetaFrame server MUST authenticate to the ExtendNet VPN first. This keeps the Terminal Server Edition/MetaFrame server safely behind the ExtendNet VPN, further reducing the risk of attack from the Internet. PPTP provides 40-bit (the maximum allowed internationally) or 128-bit (domestic maximum) encryption keys. The ExtendNet VPN is also a dedicated hardware platform with a proprietary “hardened” operating system with a reduced code set instead of a commercially available system, such as Windows NT Server, Terminal Server Edition.

Performance. The ExtendNet VPN offloads the tasks of encryption and decryption from the MetaFrame server. The ExtendNet VPN is hardware optimized to maximize throughput and decrease the utilization levels of the MetaFrame server.

Ease of use. By utilizing a standards-based solution dedicated to remote access, the ExtendNet VPN is easy to set up and configure. Interoperability is achieved using standard PPTP and Simple Network Management Protocol (SNMP) communication specifications.

Requirements

Hardware

- File server

- An available 10Base-T, 10Base-2, or 100Base-TX network connection for the VPN server
- Dedicated Internet connection at the MetaFrame site
- Management console in the form of a PC running Windows 95 or Windows NT 4.0 to run the management software (InterprEYES Manager and Monitor)
- Remote clients with dial out capability (modem, etc.) and access to the Internet through an account with an ISP

Software

- MetaFrame Version 1.8 or higher
- Microsoft Windows NT, Terminal Server Edition
- Remote clients running Windows 95, Windows 98, or Windows NT
- Remote Windows 95 or Windows 98 must have Dial-Up Networking (DUN) Version 1.3 with the Microsoft VPN option enabled
- Remote Windows NT clients must have Service Pack 4 installed
- Network Operating System (NOS) protocol supporting TCP/IP

System Integration

Note Before you proceed, make sure that Microsoft Terminal Server and Citrix MetaFrame are already installed on the server and that the server is configured to accept TCP ICA connections.

- ExtendNet VPN serves as a gateway between the Citrix network and the Internet. Because the ExtendNet VPN functions on the TCP/IP layer (the network and transport layers of the OSI model), remote users can authenticate to the ExtendNet VPN, receive an IP address that is valid for the local subnet, and then authenticate to the Citrix MetaFrame server as if physically connected to the MetaFrame server's network.
- Firewall and/or router configuration. The ExtendNet VPN utilizes Microsoft's PPTP for encapsulating and encrypting the packets during transmission over the Internet. PPTP requires that two packet types are passed to the PPTP server (in this case, the ExtendNet VPN). Data packets are PPP packets encapsulated using an enhanced Internet Generic Routing Encapsulation Protocol Version 2 (GRE V2). GRE is protocol type 47. Control packets (for status inquiry and signaling information) are transmitted and received over a TCP connection. The TCP port used is 1723. Both of these packet types must be able to reach the ExtendNet VPN and may require some configuration of a router and/or firewall (if present and filtering) at the ExtendNet VPN site.

- Client configuration. Because the ExtendNet VPN uses PPTP to enable remote access to a LAN over the Internet, each client must be configured to utilize PPTP. Installing the Microsoft software varies by operating system (either Windows 95, Windows 98, or Windows NT), but is detailed in the *Extended Systems VPN User's Guide – Remote Setup*.

Installation

▶ **To install and configure the ExtendNet VPN server**

1. Connect the ExtendNet VPN to the LAN with 10Base-T, 10Base-2, or 100Base-TX.
2. Install the InterprEYES discovery and management software on a Windows PC.
3. InterprEYES discovers and allows configuration of the ExtendNet VPN. It automatically discovers an ExtendNet VPN on the same local subnet but requires multicast support to discover an unconfigured device that is on a remote network.
4. Configure a remote client to access the ExtendNet VPN.

Note The Independent Computing Architecture (ICA) client must already be installed on the remote client machine in order to log on to the Citrix server.

5. Test the configuration by attempting to connect the remote client to the ExtendNet VPN.
6. After authenticating to the local network successfully, the remote client can log on to the Citrix server by a TCP ICA connection. This type of connection is enabled by default on a MetaFrame 1.8 server.

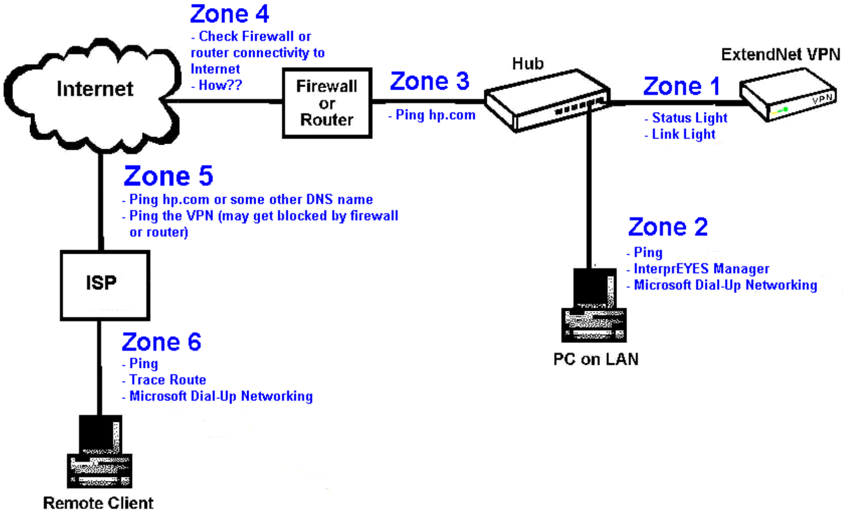
Usage

When utilizing the ExtendNet VPN, a client performs the following steps to initiate a Citrix MetaFrame session.

1. Connect to the Internet. This is typically achieved through a DUN connection but could also be a LAN connection to the Internet.
2. Double-click the DUN icon representing the VPN connection to the ExtendNet VPN.
3. Log on to the Citrix MetaFrame server with the ICA client.
4. You can now access any resources on the MetaFrame server as if you were physically connected.

Troubleshooting

To start troubleshooting a VPN connection, break the issue into zones. Start with the physical connection (Zone 1). Verify that you have a green status and link light. Build up to Zone 2. Verify that local communication exists to the ExtendNet VPN by executing a ping from a local workstation, such as **ping <local IP address>**.


Zone 4
- Check Firewall or router connectivity to Internet
- How??
Internet
Firewall or Router
Zone 3
- Ping hp.com
Hub
ExtendNet VPN
Zone 1
- Status Light
- Link Light
Zone 5
- Ping hp.com or some other DNS name
- Ping the VPN (may get blocked by firewall or router)
Zone 2
- Ping
- InterprEYES Manager
- Microsoft Dial-Up Networking
ISP
PC on LAN
Zone 6
- Ping
- Trace Route
- Microsoft Dial-Up Networking
Remote Client

Ensure that a workstation can communicate with the ExtendNet VPN using the InterprEYES utility to check the ExtendNet VPN's current IP address, subnet mask, and default gateway. Another good test is to see if a client workstation can initiate a VPN session locally utilizing Microsoft's VPN adapter (DUN on Windows 95 or 98 and a RAS connection in Windows NT). In Zone 3, verify that communication exists with the Internet. Ping a domain name by entering the following at a command line: **ping www.extendedsystems.com** or some other domain name.

Zone 4 is the most common cause of issues. A router or firewall is generally configured to deny all traffic from the Internet by default. This means a remote user trying to connect to the ExtendNet VPN will never reach the ExtendNet VPN server (in Zone 1) because the packets will be refused by the firewall/router at Zone 4. Check your forwarding rules for the firewall/router to make sure these packets types are allowed through. If remote clients are getting errors connecting to the ExtendNet VPN (specifically error 650 or 629), but clients in Zone 2 can reach the VPN, it is most likely due to the firewall. In Zone 5, verify the client DUN is configured to the IP address of the ExtendNet VPN server. Also, try to ping hp.com and then try to ping the IP address of the ExtendNet VPN.

For more advanced troubleshooting tips, query our knowledge base at **http://www.extendedsystems.com,** by e-mail at mailto:support@extendsys.com, by phone at 800-235-7576, or contact Extended Systems technical support directly.

Client Modem Support

Although Citrix and Microsoft make every effort to provide support for the latest modems, new modems are released almost daily. This section describes how to add support for a new modem to the MetaFrame server and client systems.

The first step in adding support for new modem types is to obtain the modem INF file from the manufacturer's Web site, bulletin board system (BBS), or FTP site. Once you have the .INF file, follow the procedures in this section to install the INF file on a client PC for use by the Citrix ICA Client. Follow the procedures in the Terminal Server Administrator's Guide to install the INF file for use by Terminal Server Configuration and Microsoft RAS.

▶ **To install a new modem for use by the Citrix ICA Client (DOS, Win16, Win32)**

1. The modem scripts for the ICA Clients are contained in the Modem.ini file. This file is located in the following directory (by client type):
   - DOS client: \WFClient\Modem.ini
   - Win16 client: \WFC16\Modem.ini
   - Win32 client: \Program files\Citrix\Metaframe client\Modem.ini
2. Use a text editor to add the name of the new modem to the [Modems] list at the beginning of the Modem.ini file. Insert the name in the proper position by alphabetical order.
3. Add the initialization strings for the modem that you downloaded from the manufacturer to the file. These strings are located in alphabetical order by manufacturer and modem type at the end of the Modems list. Save the file and exit the editor.
4. Verify that the modem added now appears in the Remote Application Manager modem list.

Support for Pen Input from Client Devices

PenX VC

Note The information in this note was provided by Communication Intelligence Corporation, 275 Shoreline Drive, Suite 500, Redwood Shores, CA 94065.

In the past, pen-based solutions required significant investments in pen hardware. The rapid growth of Windows CE devices has significantly reduced pen hardware costs and has increased the market for thin client/server pen-based solutions. PenX VC uses pen data instead of mouse data with the Citrix virtual channel, thus significantly improving the quality of data collected without having to increase the bandwidth or processing power of the server.

Requirements

Hardware

- Systems with Windows 95, 98, NT, CE

Software

- MetaFrame Version 1.0 or higher

Installation

PenX VC installation consists of two parts, the server installer and the client installer.

Server Installation

1. Log on to the MetaFrame server as an administrator

   - Or -

   Log on through an ICA session as an administrator or as a user with administrator privileges.
2. Open the installer directory (PenX VC Server) and execute the Setup.exe file in the Disk 1 directory.
3. Choose the destination directory (default is Program Files\CIC) for PenX VC).
4. When installation is complete, reboot the system.
5. A new program folder, called CIC PenX VC, is created under Start/Programs.

Note The PenX VC Server will not run in a console session.

Client Installation

1. The server installation installs the installers for PenX VC Client in the directory Program Files\CIC\PenX VC\Client Installations (if you choose the default install directory).
2. Different directories are created under the installation directory for various clients:

   Win32: Client Installer for Windows 95/98/NT using Citrix Remote Application Manager 4.00 or earlier

   Win32_420: Client Installer for Windows 95/98/NT using Citrix Remote Application Manager 4.20 or later (for MetaFrame 1.8)

   WinCE FTP: File transfer installer for a Windows CE device

   WinCE PC: PC installer for a Windows CE device.

Windows 95/98/NT Client Installation

1. Copy the installer Win32 or Win32_420 folder onto the client machine:
   - Over the regular network
   - Through disks
   - Through an ICA session to client drives labeled as C$ on Client D:
2. Exit the ICA session if you are running one.
3. Run the installer on the local machine.

Notes The installer copies files and modifies the Module.ini file. It automatically searches for these files and displays the path found (usually \Program Files\Citrix\ICA Client). The installation completes without further notification. No CIC or PenX directory is created.

The PenX VC Client for Windows 95/98/NT requires an active PenX or Wintab-compliant tablet driver.

On a dual boot system (Windows 98 on drive C, Windows NT on drive D), there is a possibility that under Windows NT the installer will point to the Citrix directory on drive C. If this occurs, change the directory during installation.

Windows CE/PC Installation

1. Ensure that the CE device is connected (through network or serial connection) to a Windows 95/98/NT machine with Windows CE Services running (active connection).
2. Run Setup.exe from the installer directory on the Windows 95/98/NT machine.
3. Always choose **use default directory** when asked.
4. The PenX VC Client is automatically installed on the client machine.

5. When installation is completed, hard reset the CE device.

Notes The installer always assumes the default directory is My Handheld PC\Citrix.

Do not forget to hard reset the device after installation (or uninstallation).

Windows CE/FTP Installation

In an ICA session, the client drives are usually labeled with C$ on client D: for the client drive C.

1. Copy the install file (cab file) onto the client drive though an ICA session from the server to the client drive.
2. Exit the ICA session.
3. Find the cab file and double-click the icon to run the installer.
4. Always choose the default directory when asked.
5. When installation is completed, hard reset the device.

Notes The installer always assumes the default directory is My Handheld PC\Citrix.

Do not forget to hard reset the device after installation (or uninstallation).

Usage

How it Works

After both server and client are installed, you can initiate an ICA session from the client through the Remote Application Manager.

The CIC PenX VC virtual channel driver loads automatically (through the Module.ini file in the \Citrix directory). The Module.ini file loads additional DLLs and connects to the local tablet driver.

On the server side, PenX starts with every new connection and establishes the communication to the client device through the opened virtual channel.

How to Use it

You will see an arrow icon in the MetaFrame taskbar when PenX is running.

Start any text editor or word processing program, tap on the yellow arrow (that turns into a pen), and start writing. Ink appears on the screen.

After a time out (usually one second), the ink clears and the recognition result is displayed at the location of the flashing cursor.

Preferences/Options

Whenever you log off or disconnect from the server and then log on again, PenX is running. You can also manually start and exit PenX from the PenX Handwriter Settings control panel.

You can control other settings like ink color and thickness, recognition time-out time, etc. from the PenX Handwriter settings.

Every user has his or her own settings on the server, independent from other PenX users on the server.

Notes If you turn off PenX through the Control Panel, PenX does not automatically restart on a new connection.

You control the entire PenX configuration from the server's PenX Handwriter Settings control panel.

CHAPTER 3

Installing Applications

The second phase of putting a MetaFrame solution into production is to install the applications on your servers and make them available to your end-users. To do so, you must:

1. Understand the special demands a multi-user operating system places on applications
2. Install the applications you plan to publish on your MetaFrame servers

This chapter includes information to assist you with these steps.

For help with:	**See these sections:**
Step 1	"Application Integration"
Step 2	"Software Application Notes"

Application Integration

When integrating an application into a MetaFrame environment, the main areas of consideration are:

- Application installation and configuration
- Application compatibility
- Application security
- Application video performance

Some applications have characteristics that, although relatively benign in a single-user environment, can lead to decreased performance or application incompatibilities in a MetaFrame multiuser distributed presentation environment. Understanding and avoiding these characteristics (if possible) helps ensure the smooth integration of an application into a MetaFrame environment.

As a general rule, follow the application guidelines below when selecting or developing applications:

- Win32 (32-bit Windows) applications are preferred over Win16 (16-bit Windows) applications. Terminal Server runs Win16 applications through a process called Win16 on Win32 (WOW), which causes Win16 applications to have higher processor requirements than comparable Win32 applications.
- The Windows INI files must be accessed using the proper Windows NT APIs. This is needed so the INI file synchronization features of Terminal Server will work properly.
- Applications (mostly DOS applications) that poll a hardware device or the keyboard rather than waiting for an event can have an adverse effect on system performance. The DOSKBD command can be used to tune DOS applications that perform excessive keyboard polling.
- Use the Windows NT APIs instead of custom coding whenever possible. Many Windows NT APIs have Citrix MultiWin enhancements to seamlessly support a multiuser environment.
- Avoid hard coding of paths and network identifiers.
- NetWare applications must be able to run in bindery mode.
- DOS graphics are not supported on ICA connections.
- Avoid using bitmaps in graphics; use vector-based graphics instead. Use the raster operator to “brush” graphics on the screen for best performance on an ICA device.
- VxDs are not supported in a Windows NT environment.
- When developing Win32 applications, make sure that the DLLs do not have to be moved in memory; instead, use fixed DLL addresses. The Windows NT SDK includes tools to help with this.

The following sections discuss some of these guidelines in greater detail.

Application Installation and Configuration

In a multiuser environment such as MetaFrame, it is essential that all users be able to make use of the same applications concurrently without interfering with each other’s preference settings or data.

The first and most important step is to assign each user a unique home directory; for example, C:\Users\%Username%. By default, all users use the directory \User\Default on the MetaFrame server as their home directory. For applications to work properly, utilize User Manager for Domains to assign a separate home directory to each user.

▶ **To configure existing users to use separate home directories**

1. Log on as an administrator and run User Manager for Domains.

2. If you are logged into the domain and want to change local users, from the **User** menu choose **Select Domain** and type in the name of the MetaFrame server where the user accounts are.
3. Select the users you want to change. To select multiple users, press and hold the SHIFT key while using the up and down arrow keys. To select all users in a specific group, from the **User** menu choose **Select Users**.
4. From the **User** menu, choose **Properties**.
5. Click on the **Profile** button.
6. Click on the radio button next to **Local Path** and enter ***x*:\users\%username%**, where *x* is the drive where MetaFrame is installed (usually drive C).
7. Click **OK** to return to the **User Properties** dialog box.
8. Click **OK** to return to the User Manager for Domains main screen.

DOS and OS/2 text applications can generally be installed and used as-is. DOS applications that perform keyboard polling may need tuning with the DOSKBD command to avoid excessive resource consumption.

Windows applications often use Windows features such as the system Registry and INI files. Some of the information in these files is common to all users and some information is user-specific. This may require some application customization, as discussed in this section.

There are two ways to install 16- or 32-bit Windows applications in a MetaFrame environment: user-global and user-specific.

User-Specific

User-specific means that the application is installed by a specific user for his or her own use only. The default installation is user-specific. Any INI or other files the application tries to place in the default Windows directory are installed to that user’s home Windows directory. Even if the application is installed to a network or shared directory, other users do not have access to all the DLL and INI files needed to run the application and must do a user-specific install for themselves. In short, a separate install must be done for each user who wants to use the application.

If an application is installed using the user-specific method, no special considerations regarding the storage and retrieval of data are needed. However, because the application must be completely installed once for each user, this method can consume a large amount of disk space and adds to administrative overhead in larger environments.

Some applications offer the option of doing a *network* installation. This process copies the installation diskettes or CD-ROM files to a common directory on the network from which individual users can then run a SETUP or INSTALL utility, which copies the required INI files to their home Windows directory. While it does use less space on the MetaFrame server than multiple user-specific installations, it still requires that a separate process be run for each user.

User-Global

Citrix recommends using the *user-global* method of installing Windows applications. With this method, an application is installed once by an administrator and can be run by anyone who logs onto that MetaFrame server.

To perform a user-global install, use either of the following methods:

- Use the Add/Remove Programs utility in Control Panel to initiate the installation
- Use the **change user /install** command at the command prompt before installing the application and **change user /execute** after installing the application

The Add/Remove Programs utility and the **change user /install** command place the session into *install mode*. This ensures that INI files are installed to the Terminal Server system directory instead of the user's home Windows directory. When the installation is complete, the Add/Remove Programs utility and **change user /execute** command place the session back into *execute mode*. When a user starts the application for the first time, the required user-specific files are automatically copied to the user's home directory.

Most Win32 applications install in a pseudo user-global fashion by default, even when the session is not in install mode, because they make use of Terminal Server's registry, where each user can have a unique set of registry settings. Win16 applications use INI files for configuration settings so they **must** be installed using install mode in order for multiple users to get separate copies of these files. It is recommended that you always install any Windows application, whether 16- or 32-bit, using install mode. For security reasons, it is also recommended that you install applications on Windows NT file system (NTFS)-formatted drives rather than on FAT-formatted drives.

▶ **To perform a user-global install using Add/Remove Programs (recommended)**

1. Log on to the MetaFrame server as an administrator.
2. Close all applications and ensure no users are connected to the server. Disable further logons by typing **change logon /disable** at a command prompt.
3. Open Control Panel.
4. Double-click **Add/Remove Programs**.

5. In the **Add/Remove Programs Properties** dialog box, click **Install**.
6. The **Install Program from Floppy Disk or CD-ROM** dialog box appears. Insert the application disk or compact disk and click **Next**.
7. In the **Run Installation Program** dialog box, click **Browse** if the system cannot find the installation program. Click **Next** to run the installation program.
8. In the **Change User Option** dialog box, click **All users begin with common application settings** and then click **Next**.
9. Install the application on a local NTFS drive as directed by the installation program.
10. In the **Finish Admin Install** dialog box, click **Finish**.
11. Enable user logons by typing **change logon /enable** at a command prompt.

▶ **To perform a user-global install using the change user command**

1. Log on to the MetaFrame server as an administrator.
2. Close all applications and ensure no users are connected to the server. Disable further logons by typing **change logon /disable** at a command prompt.
3. At a command prompt, type **change user /install**.

   This command places the system in *install mode* and allows Terminal Server to keep track of the user-specific application registry entries, initialization (.INI) files, and Dynamic Linked Library (.DLL) files the application adds to the Terminal Server system during installation.
4. Install the application following instructions in the documentation.

   If you are asked to enter your name during the installation process, use a generic name because the name is the default for all users. Configure any default program settings you want **all** users to have.
5. When installation is complete, at a command prompt, type **change user /execute**.

   This command returns the system to *execute mode*.
6. Enable user logons by typing **change logon /enable** at a command prompt. Make sure that any shared resources (such as network drives or printers) are set up for each user before running the application. Check the software documentation for any notes that apply to the installation or use of the application.
7. It is generally a good idea to write-protect the application's directory (and \Wtsrv if you have not already done so) from all non-administrator users. This allows users to read the program files but protects them from inadvertent changes or deletions. See "Application Installation and Security" in Chapter 6 of the *Terminal Server Administrator's Guide* for more information.

Note If you installed to an NTFS partition, the security options in Windows NT Explorer allow you to set the security to a wide array of options and restrict access only to specific user groups. If the application is installed on a FAT partition, you can use the ATTRIB command to mark the files and directories as read-only but cannot use the advanced security features of NTFS. For this reason, Citrix recommends that Terminal Server, MetaFrame, and applications be installed on NTFS partitions. While using NTFS is not a must, it does provide a wider range of security options. If the applications reside on a NetWare file server, use the FILER program to set the security options.

If you need to determine if the system is in execution or installation mode, type **change user /query** at the command prompt.

The exact actions performed when a user-global application is started can be tuned and optimized by creating and setting compatibility bits in registry variables associated with the application. See Chapter 6, "Application Installation and Security" of the *Terminal Server Administrator's Guide* for more information on optimizing your applications using registry variables.

Application Compatibility

Many older applications are not compatible with MetaFrame's multiuser environment. Several Application Compatible Scripts (ACS) are available to help ensure that the applications run in such an environment. The ACS are in the **%SystemRoot%\System32\Application Compatibility Scripts** folder on the MetaFrame server.

Documentation on the applications that have been tested is in the Terminal.doc file on the Terminal Server CD.

Application Security

Terminal Server includes an added security feature called the*Application Security Registration Utility*. This utility allows an administrator to restrict user execution access to an authorized list of applications. When application security is enabled, any attempt by non-adminstrator users to execute an application not on the list returns an error message. Administrators can access any application whether it is on the list or not.

Application Security does not allow adding an application that does not reside on the hard drive of the MetaFrame server. Attempting to do so generates an error. This way non-administrator users do not have access to applications that reside on the network when Application Security is enabled.

Application Security can also be run from a command prompt by typing**appsec**.

Application Video Performance

The Citrix Independent Computing Architecture (ICA) protocol provides high-performance Windows presentation services over low-bandwidth connections. ICA is a robust and extensible protocol that includes definitions for the following capabilities:

- Full-screen text presentation
- Graphical Windows application screen presentation
- Keyboard and mouse input
- Session control
- Framing for asynchronous connections
- Error detection and recovery
- Encryption
- Data compression
- File system redirection
- Print redirection
- COM port redirection
- Multiple generic virtual channels
- Cut and paste across clients and servers
- General purpose Citrix server browsing

The Thinwire Virtual Channel

The thinwire protocol is an ICA virtual channel protocol used to transmit presentation commands from Windows applications running on the application server to the client. The thinwire protocol is highly tuned for transmission of Windows object display over low-bandwidth connections. This is accomplished through:

- Command- and object-specific intelligent compression with state persistence; that is, run-length encoding for bitmaps
- Outboard complex clipping and complex curve drawing
- Intelligent caching of Windows objects such as bitmaps, brushes, glyphs, and pointers
- Remote SaveScreenBitmaps
- Cross-session persistent caching

To enable thinwire to most efficiently distribute the Windows image to the ICA client, use the following guidelines:

- Use vector graphics instead of bit-mapped images for graphics

- Use the raster operator to “brush” graphics to the screen

Bitmaps require more bandwidth than vector graphics because all of the image data for each unique bitmap must be transmitted from the server at least once. ICA compensates for this by caching each unique bitmap on the client system. When a bitmap is to be displayed, it is compared with the client’s locally cached bitmaps. If the displayed bitmap matches one that is already cached at the client, ICA sends a command telling the client to redisplay the local copy instead of sending the image over the wire.

Blinking cursors cause unnecessary bandwidth utilization because every blink requires data packets to be transmitted. Applications that do not use a blinking cursor or that allow the blinking cursor to be disabled are preferred.

Software Application Notes

The products listed in this section have been tested and found to be compatible with MetaFrame. Other products work well with MetaFrame but Citrix cannot guarantee the compatibility of untested products.

Because MetaFrame is an add-on to Microsoft Windows NT Server, Terminal Server Edition, most Windows NT 4.0-compatible applications can be expected to work. Review the following application notes for detailed application integration tips and techniques.

Accounting Software

Great Plains Dynamics C/S+ and Dynamics

Great Plains Software develops, markets, and supports accounting and financial management software worldwide, offering solutions ranging from midrange client/server systems to small business integrated accounting software.

Great Plains Dynamics C/S+ is a client/server financial management suite for Microsoft BackOffice. Dynamics C/S+ offers a complete suite of Internet-ready financial applications and tools in a flexible three-tier client/server architecture. Dynamics C/S+ for SQL Server is exclusively optimized for Microsoft SQL Server. ISAM database options are also available for Dynamics C/S+.

Great Plains Dynamics is an accounting solution for growing companies with $1 to $50 million in revenues seeking financial information access throughout the deployment of strategic technologies and the Internet. Dynamics is a complete financial management solution with more than 20 financial modules and tools and hundreds of Dynamics companion products.

Citrix MetaFrame extends Dynamics C/S+ and Dynamics into WAN and dial-in environments without sacrificing performance. By running the client portion of Great Plains Dynamics or Dynamics C/S+ on a MetaFrame server, you can use Citrix's advanced ICA protocol to provide local LAN performance to client PCs on the local LAN, over a WAN, or even to dial-in users in the field. Using ICA, only the keyboard, mouse, and video information are transferred between the MetaFrame server and the ICA client; all the interaction between the Great Plains server and client machines takes place over the high-speed LAN.

The two companies' combined products provide customers with a state-of-the-art client/server financial management solution that can be economically deployed enterprise-wide across a wide area network, while delivering a high level of performance to all users, no matter where they are.

Requirements

Hardware Requirements

- Server PC with Pentium processor or greater for Dynamics Server; dual-processor SMP system recommended for Dynamics C/S+ Server. See the Great Plains Installation: Procedures manual for detailed system requirements.
- MetaFrame server with Pentium processor or greater for Dynamics Client; a dual-processor SMP system is recommended for Dynamics C/S+ Client. The system should contain 32MB RAM plus 8-10MB per remote client, and at least 400MB available disk space.
- ICA Client PCs. See the Citrix ICA Client documentation.

Software Requirements

- MetaFrame Version 1.0 or higher
- ICA Client (DOS, Win16, or Win32)
- Great Plains Dynamics or Dynamics C/S+

Supported Databases and Operating Environments

Dynamics C/S+ Client/Server Systems

Note For best performance, implement the MetaFrame server on a physical server different from the database engine.

Database software	Dynamics C/S+ clients	Database server	Application server	Networking software
MS SQL Server 6.5	Citrix MetaFrame 1.0 or higher	Windows NT Server 3.51 or higher (Intel or Alpha)	Windows NT Server 3.51 or higher (Intel or Alpha) Windows NT Workstation 3.51 or higher (Intel or Alpha)	Windows NT Server 3.51 or higher (Intel or Alpha)
Btrieve Server for NT	Citrix MetaFrame 1.0 or higher	Windows NT Server 3.51 or higher (Intel only)	Windows NT Server 3.51 or higher (Intel only) Windows NT Workstation 3.51 or higher (Intel only)	Windows NT Server 3.51 or higher (Intel only)
Faircom Server	Citrix MetaFrame 1.0 or higher	Windows NT Server 3.51 or higher (Intel or Alpha)	Windows NT Server 3.51 or higher (Intel or Alpha) Windows NT Workstation 3.51 or higher (Intel or Alpha)	Windows NT Server 3.51 or higher (Intel or Alpha)

Dynamics Client/Server Systems

Note For best performance, implement the MetaFrame server on a physical server different from the database engine. By keeping the servers separate, performance on both can be optimized and maintained.

Database software	Dynamics clients	Servers	Networking software
Btrieve Server for NT	Citrix MetaFrame 1.0 or higher	Windows NT Server 3.51 or higher (Intel) Citrix MetaFrame 1.0 or higher	Windows NT Server 3.51 or higher (Intel)
Btrieve Server for NetWare	Citrix MetaFrame 1.0 or higher	NetWare 3.12, 4.10, or 4.11	NetWare 3.12, 4.10, or 4.11
c-tree Plus	Citrix MetaFrame 1.0 or higher	Windows NT Server 3.51 or higher (Intel) NetWare 3.12, 4.10, or 4.11 Citrix MetaFrame 1.0 or higher	Windows NT Server 3.51 or higher (Intel) NetWare 3.12, 4.10, or 4.11

Dynamics Stand-alone Systems

Database	Operating environments
Btrieve Workstation	Citrix MetaFrame 1.0 or higher
c-tree Plus	Citrix MetaFrame 1.0 or higher

Installation

▶ **To Install Great Plains Dynamics C/S+ or Dynamics**

1. Verify system requirements. Make sure your system meets the recommended minimum requirements for a Dynamics or Dynamics C/S+ system and that your system is prepared for installation. See the instructions in the Dynamics or Dynamics C/S+ *Installation: Procedures Manual* and the MetaFrame documentation.
2. Install MetaFrame. See the MetaFrame documentation for detailed installation procedures.
3. Review database server information, if necessary. Depending on your database server choice, review the Dynamics or Dynamics C/S+*Installation: Procedures Manual* to properly configure your database.
4. Install Dynamics or Dynamics C/S+ on one client and on a server. It is recommended that you install the Dynamics or Dynamics C/S+ database on a server different from your MetaFrame server. You should also install a client on a machine other than the MetaFrame server. This allows you to verify the correct installation of Dynamics or Dynamics C/S+ before you set up your MetaFrame server. The MetaFrame server can then be set up as another client. Once this is accomplished, all client machines on your network can be configured to access your Dynamics or Dynamics CS+ database.
5. Check the mapped drives or UNC (universal naming convention) pathnames that each client uses to identify the server. Be sure that each client identifies the Dynamics or Dynamics C/S+ folder on the server the same way; for instance, all clients should identify the C:\Dynamics folder on the server using the same ID, such as F:\Dynamics or F:\.
6. Install Dynamics or Dynamics C/S+ applications on a client computer and install data on the server computer, following the instructions in the Dynamics or Dynamics C/S+ *Installation: Procedures Manual.*
7. When installing Dynamics, do not use your server to install data; it will prevent your clients from locating the data and you will need to enter a location translation.
8. Use Dynamics or Dynamics C/S+ Utilities. See the Dynamics or Dynamics C/S+ *Installation: Procedures Manual* for information on how to define your account framework and synchronize it with your dictionary, and to register Dynamics or Dynamics C/S+.

9. Perform initial setup procedures. Follow the instructions in the Dynamics or Dynamics C/S+ *Installation: Procedures Manual* to start the program for the first time and perform initial setup procedures such as creating a company, adding users, and setting user access. You must complete these procedures before you begin using Dynamics or Dynamics C/S+.
10. Install and set up Dynamics or Dynamics C/S+ on all additional client computers, including the MetaFrame server and the remote ICA client sessions.

Administrative Software

Softblox AppScape/Manage

Note This application note was provided by Softblox, Inc., 1201 West Peachtree Street, Atlanta, GA 30309.

AppScape/Manage delivers the benefits of reducing total cost of operation (TCO) by allowing the administrator to control, restrict, and log the use of specific features within users' applications. AppScape/Manage controls availability of functionality within applications to provide a custom interface based on each user's needs. Non-essential or problematic application activity is prevented. Corporate data is protected from accidental misuse. Network and bandwidth-clogging features such as splash screens are removed and user productivity increases.

The AppScape/Manage Administrator module is installed and run on a MetaFrame, Microsoft Windows NT 4.0, or Windows NT 4.0 Server, Terminal Server Edition server.

The AppScape/Manage Runtime module is installed on any server to which clients can log on. Users connect to the MetaFrame server as usual, with AppScape monitoring the usage.

Requirements

Hardware Requirements (Server)

- IBM compatible 586/Pentium server
- 133MHz or faster
- 64MB memory
- 32MB disk space

Software Requirements

- MetaFrame Version 1.8 or higher
- Microsoft Windows NT 4.0, Terminal Server Edition
- Softblox AppScape/Manage

Installation

▶ **To install AppScape/Manage Administrator**

1. Log on to the computer as an administrator.
2. Insert the AppScape CD-ROM and view the Readme.txt file located in the root directory. Readme.txt can include updated information that you need before or during installation.
3. After viewing Readme.txt, run Setup.exe, located in the AppScape CD root directory.
4. After Setup initializes, a Welcome window appears. Follow the on-screen instructions in this window, making sure all other applications are closed. Click **Next**.
5. Read and accept or reject the Software License agreement. If you do not accept the terms of the agreement, press **No** to exit Setup and return all physical copies of the software to Softblox. If you accept the terms of the agreement, press **Yes**.
6. Enter your name and company information in the **User Information Window**.
7. Enter your serial number or leave blank for a timed evaluation license. Click **Next**.
8. Keep the default **Typical Installation** by choosing to install all components. Choose the destination folder where you want to install AppScape/Manage. Click **Next**.
9. Select any optional components you want to install. Click **Next**.
10. Select the name of your program folder. Click **Next**.
11. Verify that the settings you selected are correct. Click **Next**.
12. Click **Finish to Restart Computer**.
13. Log on to the computer with the same account.
14. Setup registers the administrator.
15. Select **Interaction Modules to Install**. Click **Import**.

AppScape/Manage Setup is complete.

Quick Start Instructions for Running AppScape/Manage

Note AppScape supports multiple methods to complete many tasks. These Quick Start Instructions demonstrate only one method.

Starting AppScape Administrator

AppScape can modify application behavior on a user-by-user basis. An application's behavior is modified based on AppScape rules. AppScape comes with several pre-packaged sets of rules (you can also define your own custom rules as described later in this note).

An AppScape policy links users and rules. At its simplest, a policy links a single user and rule, causing that rule to be enforced on that user.

Creating a New Policy

1. In the AppScape Administrator's menu bar, click the **AppScape** menu, point at **New**, and then select **Policy**.

   The **Rule Wizard's New Policy** dialog box appears.
2. In the **Name** field, type **Disable Printing**.
3. In the **Description** field, type **Disable Printing in Word and Excel.**
4. Click **Next**.

   The **Policy Wizard's Select Rules** dialog box appears.
5. Click the listbox by the **Available Rules** label and select **Elements** in the drop-down list that appears.

   The **Available Rules** dialog box now lists the defined rule elements (instead of rule packages).
6. In the **Available Rules** dialog box, scroll to the **Disable Printing in Word 97** entry. Click on that entry and then click **Add**.

   Disable Printing in Word 97 now appears in the **Selected Rules** dialog box.
7. Click **Next**.

   The Policy Wizard's **Select Users** dialog box appears. Specify the users to whom the selected rules will apply.
8. Click the listbox by the **Available Users** label and select **NT users** in the drop-down list that appears.

   The **Available Users** dialog box now lists all Windows NT users known to this server (in the currently active domain).
9. For this example, use yourself as a test user. In the **Available Users** dialog box, click your own username and then click **Add**.
10. Click **Next**.

The Rule Wizard's **Select Schedule** dialog box appears. Specify an optional schedule for the policy. The default **<no schedule>** means the rule is always enforced.

11. Click **Next**.

    The Rule Wizard's **Summary** dialog box appears.

12. Click **Finish**.

Note As you become more advanced, you may find it easier to create a policy than drag and drop rules and users into the existing policy.

13. Expand the tree view for **Rules** and expand **Excel 97 Rule Package** under **Packages**.
14. Drag **Disable Printing in Excel 97** to the **Disable Printing** policy you just created under **Policies**.
15. Click the **Disable Printing** policy to make it consist of both rules.

You have created and edited a policy that disables printing when you run Word 97 and Excel 97. However, this policy has no effect until you update the AppScape monitors, as described next.

Activating the New Policy

New policies (and changes in existing policies) are not activated until the AppScape application monitors are updated. These monitors oversee user operations and induce the changes in application behavior specified by rules that are applied to users through policies.

To update the monitors, click the **Apply Policy Changes** button in the AppScape Administrator Toolbar.

Your newly created Policy is now active.

Testing the New Rule and Policy

You have now completed all the steps to modify the behavior of Word 97 and Excel 97 for your own user account. To test this, run Word 97 or Excel 97. Notice that print functions are no longer available, including:

- No Print button in the toolbars
- No Print option in the **File** menu

Because the policy you created specifies only your account, this behaviors appears only when you are logged on under that username. To confirm this, log on with a different username and you will see that Word 97 and Excel 97 operate as usual.

To learn more about AppScape, see the complete electronic documentation on the CD-ROM and continue exploring AppScape Administrator.

Anti-Virus Software

Inoculan 4 for Windows NT

Cheyenne Software Inoculan 4 provides virus protection for Windows NT and Citrix MetaFrame. MetaFrame extends Inoculan's capabilities by allowing multiple users to simultaneously utilize Inoculan's virus scanning ability. Additionally, Inoculan can detect and prevent viruses from being passed between MetaFrame servers and ICA Clients. This document describes a tested method of configuring Inoculan using MetaFrame.

Requirements

Hardware Requirements

- MetaFrame server

Software Requirements

- MetaFrame Version 1.0
- Inoculan Version 4.00 (Build 270)
- Virus Signature File Version 4.00

Installing Inoculan

1. Download the latest Virus Signature update file from the Cheyenne Web site (www.cheyenne.com).
2. Log on at the console as an administrator.
3. At a command prompt, type **change user /install** and press ENTER.
4. Run Inoculan Setup.exe.
5. Enter the license key.
6. Enter the user information.
7. Choose the setup type (Express was chosen for this test).
8. Select the directories for the Inoculan home directory and Alert home directory.
9. In the **Options** dialog box, choose the Internet applications to be integrated with Inoculan, if any, and if the Inoculan Real-time Quick Access Monitor is to be placed in the startup menu. (Internet Explorer and the Real-time startup option were chosen.)
10. Click **Finish**.

11. When installation is complete, run Updatent.exe (downloaded during Step 1).
12. At a command prompt, type **change user /execute**.
13. Reboot your computer.

Verifying Installation of Inoculan

Follow the procedure below to verify that Inoculan is correctly installed and configured:

1. Select **Start**, **Programs**, and then **Inoculan for Windows NT**.
2. Click **Local Scanner**.
3. In the **Directories** dialog box, select the directory that contains the Inoculan program.
4. Select **Scan** and then **Start Scanning**.
5. Verify that the program finds Inoculan's test virus, Virtest.com.

Backup Software

Cheyenne ARCserve Enterprise Edition Version 6.0 with ARCserve Service Pack 3

Cheyenne ARCserve Single Server Edition is a backup program that allows you to back up data from MetaFrame servers or other machines on your network. This document describes a tested method of configuring ARCserve using MetaFrame.

Hardware Requirements

- MetaFrame server with a tape drive (a Compaq Proliant 4000 with an Exabyte EXB-4200c tape drive was used for this test installation)

Software Requirements

- MetaFrame Version 1.0
- ARCserve for Windows NT Single Server Edition, Version 6.0 with ARCserve Service Pack 3 (available from Cheyenne's Web site at www.cheyenne.com)

Installing ARCserve

1. Log on to the MetaFrame server as an administrator.
2. At a command prompt, type **change user /install** and press ENTER.
3. Run Setup.exe.
4. Choose the setup type (Full setup was chosen).
5. Type your name and company information.

6. Fill in the CD registration key.
7. Select installation location.
8. Enter the ARCserve System Account administrator.
9. Select to have ARCserve services start automatically at reboot.
10. Run Update.exe to install ARCserve's Service Pack 3.
11. At a command prompt, type **change user /execute** and press ENTER.

Verifying Installation of ARCserve

1. Open ARCserve Manager.
2. In the **Quick Access** dialog box, click **Device Manager**.
3. Select **Device** and then **Format**.
4. Enter a tape name and an expiration date.
5. Verify that the tape formatted properly.
6. Select **Manager** and then **Backup**.
7. On the **Source** tab, select a directory.
8. On the **Destination** tab, select the tape you formatted above.
9. On the **Schedule** tab, select **Run Now**.
10. On the menu bar, select **Backup**, then **Run**, and then **Schedule**.
11. Verify that the backup is successful.

Note Make sure the tape drive you use was not installed through Windows NT Setup. If it was, use the following procedure to remove the tape device.

1. In Control Panel, double-click **Devices**, highlight the tape device, and click **Stop** to disable the tape device.
2. Click **Close** and reboot the server.
3. From the **Main** menu, double-click **MetaFrame Setup**. From the **Options** pull-down menu, click **Add/Remove Tape Devices** to remove the tape device.

Client Platforms

IBM OS/2 Warp Version 4.0

The ICA Win16, DOS, and Win16 Web Clients are supported on OS/2 Warp Version 4.0.

Note Cut, Copy, and Paste operations only work when cutting or copying data from the ICA Client and pasting it to the WIN-OS2 or OS/2 session. Data cut or copied from the OS/2 or separate WIN-OS2 session (not the one running the ICA Client) cannot be pasted to the ICA Client.

The following connectivity methods are supported for the ICA Win16 and DOS Clients:

Client	TCP/IP	IPX	SPX	NetBIOS	Async (direct)	Async (modem)
DOS	No	Yes	No	Yes	Yes	Yes
Win16	Yes	No	No	Yes	Yes	Yes

In addition to using the Win16 and DOS Clients, you can configure the ICA Web Client (Win16 version) for use with the IBM OS/2 Web Explorer.

Software Requirements

- IBM OS/2 Warp 4.0
  - File and Print Client Services
  - TCP/IP Services
  - NetWare Client Services
- Citrix MetaFrame Version 1.0
  - ICA DOS Client
  - ICA Win16 Client
  - ICA Win16 Web Client, available on the Citrix Web site at http://download.citrix.com

Installation

OS/2 Installation

Install OS/2 Warp Version 4.0 following the standard installation procedure. Use the default settings. Install networking support for File and Print Client Services, Novell NetWare, TCP/IP Client Services, and the NetWare client. Verify that the network adapter settings are correct. Select the workstation name, description (if desired), and domain name. Choose the protocol you want to use. For TCP/IP, specify the hostname (usually the same as the workstation name), the IP address, the subnet mask, the router address, and the domain name as required by your configuration, or use DHCP if a DHCP server is present on the LAN.

IBM OS/2 Warp Version 4.0 includes network and TCP/IP protocols and software as part of the operating system. Follow the instructions for installing the additional network and TCP/IP software as part of the installation of the system. Network and TCP/IP software for WINOS2 and virtual DOS are installed as defaults during the installation.

WINOS2 Setup

Before installing the ICA Client, you must set the WINOS2 settings to allow the ICA Client to operate properly with DDE and Clipboard. Establish the settings as follows:

Note You may elect not to make these settings if you do not intend to use the DDE or Clipboard functions.

1. Under OS/2 System Folder, select **System Setup** and then **WIN-OS/2 Setup**.
2. Under **WIN-OS/2 Setup Settings**, select the **Data Exchange** tab.
3. In the **Data Exchange Settings** dialog box, choose **Public** for both selections. This is required for DDE and Clipboard operation.
4. Close all the previous selections; this portion of the settings is complete.
5. Under OS/2 System Folder, select **Command Prompts**.
6. Go to the **Settings** page of either the seamless WINOS2 or full screen WINOS2 icon. (The right mouse button brings up a menu; click on **Properties**.)
7. Select the **Session** tab, then select **WIN-OS/2 Properties**. Make sure the **All DOS and WIN-OS/2 Settings** radio button is highlighted and click **OK**.
8. Set WIN_RUN_MODE to 3.1 Enhanced Compatibility.
9. Set WIN_DDE to On.
10. Set WIN_CLIPBOARD to On.
11. Click **Save** and close the notebook.

12. Close all the previous selections; this portion of the settings is complete.
13. When using IBM LAN and NetBIOS, add the following line to the AUTOEXEC.BAT:

    ```
    x:\ibmcom\ltsvcfg n1=1
    ```

    where *x* is the OS/2 system drive. This command enables the NAME_NUMBER_1 support required for NetBIOS connections.

Client Installation on OS/2

Before installing the client, decide what protocols you will use. Client installation is simple; insert the ICA Client diskette in drive A and run **setup** in a WINOS2 session.

Client Protocol

TCP/IP

If you choose TCP/IP, make sure you have the server hostname handy and that OS/2 TCP/IP and DOS TCP/IP are installed.

IBM LAN

All IBM LAN software must be installed prior to installing the client. You must know the server name, the client name, and the password. The following line must be in AUTOEXEC.BAT to allow NetBIOS to work:

```
c:\ibmcom\lstvcfg n1=1
```

Dial-In

When installation starts, you are asked if you want to select the Dial-In option. **Do not** select this option at this time. Once installation is complete and you are setting up the local user, you may elect to use the Dial-In option to allow a modem connection.

ICA Win16 Client

Before installing the ICA Win16 Client, decide what network protocols and hardware you will use.

IPX and SPX connections are not supported at this time because OS/2 does not support VxDs. TCP/IP connections are supported without any changes. Serial Dial-In and direct connect connections are supported without any changes. NetBIOS connections are supported if you load NAME_NUMBER_1 support.

NetBIOS connections require you to load NAME_NUMBER_1 support before running the client. This support is not enabled by default. Include the following line in the AUTOEXEC.BAT or in a .BAT file that starts the ICA Client:

```
x:\ibmcom\ltsvcfg n1=1
```

where *x* is the OS/2 system drive.

ICA DOS Client

Change the ICA DOS Client session by following the procedure below:

- Right click on the DOS Full Screen icon
- Select **Properties**
- Select the **Sessions** tab
- Select **DOS Properties**
- Select **All DOS Settings**
- Change the DOS_FILES setting to 40

  The default value of 20 causes the ICA DOS Client to exit with an "insufficient files" error message.

DOS sessions under OS/2 Warp load NetWare support (TBMI2 and NETX) by default; IPX connections are supported without any changes. SPX is not supported.

TCP/IP support also is loaded by default. When creating a TCP/IP remote application entry, specify TCP/IP–VSL as the connection type. Include the following line in the AUTOEXEC.BAT or in a .BAT file that starts the DOS Client:

```
x:\wfclient\mibmtcp.exe
```

NetBIOS connections require you to load NAME_NUMBER_1 support before running the client. This support is not enabled by default. Include the following line in the AUTOEXEC.BAT or in a .BAT file that starts the DOS Client:

```
x:\ibmcom\ltsvcfg n1=1
```

where *x* is the OS/2 system drive.

DOS async connections require changes to the default DOS settings for the session. The following changes support direct connect and modem connections at up to 57.6Kbps:

COM_DIRECT_ACCESS	On
COM_HOLD	On
COM_RECEIVE_BUFFER_FLUSH	None
COM_SELECT	All
DOS_DEVICE	*x*:/OS2/MDOS/COMDD.SYS (see note below)
DOS_FILES	40
HW_ROM_TO_RAM	On
HW_TIMER	On

IDLE_SECONDS	60
IDLE_SENSITIVITY	100

Note *x* is the OS/2 system drive. Add this device driver statement to the list of device drivers.

ICA Win16 Web Client and Web Explorer

The IBM OS/2 Web Explorer is an OS/2-based Web browser. The procedure below describes how to configure the IBM OS/2 Web Explorer for use with the Citrix ICA Web Client.

1. Download the ICA Win16 Web Client from the Citrix Demo Web page at http://download.citrix.com. Follow the directions on the page to install the 16-bit Web client – Wfplug16.exe.
2. Edit the file C:\Mptn\Etc\Explore.ini. In the [advanced] section specify a Mailcap file if one does not exist by adding C:\Mptn\Etc\Mailcap to the end of the mailcap= statement. In the [advanced] section, specify an Extmap file if one does not exist by adding C:\Mptn\Etc\Extmap to the end of the Extmap= statement. Save the file and exit the editor.
3. Edit or create the file C:\Mptn\Etc\Mailcap. Add the line:

   ```
   application/x-ica; c:\OS2\MDOS\WINOS2\System\WFICA16.EXE %s
   ```

   Save the file and exit the editor.
4. Edit or create the file C:\Mptn\Etc\Extmap. Add the line:

   ```
   application/x-ica ica
   ```

   Save the file and exit the editor.
5. Restart the Web Explorer.

Printer Setup

Local Printing

1. Verify that the WIN-OS/2 printer drivers are installed on a local machine.
2. To access your local printer, connect to the MetaFrame server. Click**Start**, select **Settings**, and then **Printers**.

   Note You must have administrator privileges on the server to add or remove a printer.

3. Double-click **Add Printer**.

   The **Add Printer Wizard** dialog box appears.
4. Select **Network Printer Server** and click **Next**.
5. Double-click **Client Network** and then **Client**.

6. Select the printer and manufacturer, and follow the on-screen instructions. When a printer is connected, a printer description appears in the **Printers** dialog box.

Printing Using a Network Printer

1. Make sure the printer is physically attached to the network server. The network server must have the printer driver installed.
2. The printer must be shared and all members must have full access to it and its settings.
3. Click **Start**, select **Settings**, **Printers**.
4. Double-click **Add Printer**.

   The **Add Printer Wizard** dialog box appears.
5. Select **Network Printer Server** and click **Next**.
6. Locate the network printer and follow the on-screen instructions to continue with installation.
7. When the printer object is created, the printer is accessible by the Clients. MetaFrame server applications can now print.
8. The Client automatically has a print object created in the Client Print Manager. The Client user has to select the print object as the default to configure the server printer as the default printer.

Printing from the MetaFrame Server

The printer object for a MetaFrame printer is created using the MetaFrame Print Manager.

1. Create the printer object as a shared object.
2. Once the printer object is created, the printer is accessible by the Clients. Applications running on the MetaFrame server can now print on the server printer. The Client automatically has a print object created in the Client Print Manager. The Client user has the option of selecting the print object as the default if the user needs the server printer to be the default printer.

DDE and OLE

DDE and OLE are supported within the Citrix ICA Clients. There is no interoperability between the ICA Clients and WIN-OS2 or OS/2 sessions.

Network and CD-ROM Drives

All non-local drives are supported by executing the following command at a command prompt:

```
net use x: \\client\y:
```

where *x*: is the drive to be mapped to and *y*: is the non-local drive supported by OS/2.

E-Mail Software

Microsoft Exchange Server (Enterprise Edition) Version 5.0 and Microsoft Exchange Client Version 5.0

Microsoft Exchange Server is a client/server corporate messaging system that incorporates e-mail, scheduling, electronic forms, document sharing, and custom applications in a single product. Microsoft Exchange consists of two parts: Exchange Server and Exchange Client. This document describes a tested method for installing and configuring Microsoft Exchange Server 5.0 and Microsoft Exchange Client 5.0 using a MetaFrame server.

In a standard configuration, Microsoft Exchange Server is installed and run as a service on the primary domain controller (PDC), which can be a MetaFrame server or a Microsoft Windows NT 4.0 Terminal Server Edition server. The Exchange Client is installed on all other MetaFrame servers. Users connect to the MetaFrame servers and run the Microsoft Exchange Client, which then accesses the Microsoft Exchange Server.

Software Requirements

- MetaFrame Version 1.0
- Microsoft Windows NT 4.0 Terminal Server Edition (optional)
- Microsoft Exchange Server Version 5.0 and Microsoft Exchange Client Version 5.0

Installing and Configuring Microsoft Exchange Server 5.0

Installing Microsoft Exchange Server 5.0

1. Install and configure MetaFrame as a primary domain controller (PDC). Make sure that the page file size is equal to at least 1.5 times the amount of physical RAM and that there is at least 250MB of free hard drive space.
2. Log on to the console of the MetaFrame server as an administrator.
3. At the command prompt, type **change user /install** and press ENTER. This places the user session in install mode.
4. Insert the Microsoft Exchange Server 5.0 CD-ROM into the CD-ROM drive.
5. Run Server\Setup\i386\Setup.exe from the Exchange Server 5.0 CD-ROM.
6. Click **OK** in the Microsoft Exchange Server Setup window.
7. Microsoft Exchange Setup offers three choices:

- Typical Installation
- Complete/Custom Installation
- Minimum Installation

If you are installing Exchange 5.0 for the first time, select Typical Installation. Typical Installation was chosen for this test.

8. Enter the CD Key and click **OK**.
9. Click **OK** in the MetaFrame Server **Licensing Mode** dialog box.
10. Enter the required information in the **Choose Licensing Mode** dialog box.
11. Check **I Agree** in the **Per Server Licensing** dialog box and then click **OK**.
12. Add the number of licenses purchased or required for this Exchange Server and click **Continue**.
13. If Microsoft Exchange 5.0 was previously installed on your system, at this point you can make changes to an existing site that you may already have created. For new installs, select **Create a New Site**. Enter your organization name and a user-defined site name. Record this data for future use.
14. Setup confirms the creation of a new site.
15. Setup asks for an account name that will be used to log on to the system to start Exchange services when the system boots. Although this can be any user account, it is recommended that the administrator account be used.
16. Source files are now copied to your system.
17. When installation is completed, you can run the Optimizer immediately or run it later at your convenience.
18. At the command prompt, type **change user /execute** and press ENTER.

Installation of Microsoft Exchange Server 5.0 is now complete.

Verifying Installation of Microsoft Exchange Server 5.0

Follow the procedure below to verify that Microsoft Exchange Server 5.0 is correctly installed and configured.

1. From Control Panel, double-click **Services**. Scroll down the Services list and verify that the following services are listed and are automatically started:
   - Microsoft Exchange Directory
   - Microsoft Exchange Information Store
   - Microsoft Exchange Message Transfer Agent
   - Microsoft Exchange System Attendant
2. Click the **Server Start** button and select **Programs**, then **Microsoft Exchange**. Verify that the following are listed:
   - Microsoft Exchange Administrator

- Microsoft Exchange Migration Wizard
- Microsoft Exchange Optimizer
- Microsoft Exchange Server Health
- Microsoft Exchange Server History
- Microsoft Exchange Server IMS Queues
- Microsoft Exchange Server IMS Statistics
- Microsoft Exchange Server IMS Traffic
- Microsoft Exchange Server Load
- Microsoft Exchange Server Queues
- Microsoft Exchange Server Users

Configuring Microsoft Exchange Server 5.0

After installing Microsoft Exchange Server 5.0, the server needs to be configured for users to log on and retrieve mail. Because Microsoft Exchange Server resides on a MetaFrame server, all users with mailboxes on this Microsoft Exchange Server will also be MetaFrame users. However, MetaFrame users do not automatically have Exchange mailboxes. Use the following procedure to configure Exchange users.

1. Open Microsoft Exchange Administrator.
2. Type the server name to which you want to connect or click **Browse**. The server is typically the MetaFrameserver on which Microsoft Exchange is installed.
3. In the left side of the **Administrator** dialog box, expand the site name icon and click **Recipients**.
4. From the **File** menu, select **New Mailbox** to create mailboxes. Click **Primary Windows NT Account** to associate this new mailbox with an existing account on the domain. If an account does not exist, the form allows creation of new accounts.

Installing and Configuring Microsoft Exchange Client 5.0

Special Considerations

If Microsoft Exchange Client 5.0 is being installed on the MetaFrame server containing the Microsoft Exchange 5.0 Server, perform the following steps to ensure a successful Exchange Client installation. If Microsoft Exchange Client 5.0 is being installed on any other MetaFrame servers, go to “Installing Microsoft Exchange Client 5.0” later in this chapter.

1. Log on to the MetaFrame server as an administrator.
2. From the Control Panel, open **Services** and stop the following services:

- Messenger
- Microsoft Exchange Directory
- Microsoft Exchange Information Store
- Microsoft Exchange Message Transfer Agent
- Microsoft Exchange System Attendant

3. Close the **Services** dialog box and the Control Panel.
4. Install Microsoft Exchange Client 5.0 as described below, skipping Steps 1 and 2.

Installing Microsoft Exchange Client 5.0

Note Windows Messaging forms do not work for multiple users.

After installing Microsoft Exchange Client, run the script %SystemRoot%\Application Compatibilty Scripts\Install\Winmsg.Cmd. This script adds %systemroot%\Application Compatibility\Scripts\Logon \WmsgUsr.Cmd to UsrLogon.Cmd.

When a user logs on, the %SystemRoot%\Forms subdirectory is copied to the user's home drive.

Running this script is not required if you run the Office 97 installation script instead.

1. Install and configure MetaFrame.
2. Log on to the console of the MetaFrame server as an administrator.
3. At a command prompt, type **change user /install** and press ENTER.
4. From the Microsoft Exchange Client CD, run *x*:\Eng\Winnt\i386\Setup.exe, where *x* is the CD-ROM drive.
5. After accepting the copyright policies, type your name and company information.
6. Change the default installation path if desired.
7. Microsoft Exchange Setup offers three choices:
   - Typical Installation
   - Complete/Custom Installation
   - Minimum Installation

   If you are installing Exchange 5.0 Client for the first time, select Typical Installation.
8. Click **OK** when setup is complete.
9. At a command prompt, type **change user /execute** and press ENTER.

Note If Microsoft Exchange Server 5.0 was installed on the same system where the Exchange Client was installed, make sure that the Exchange Server services you stopped during installation are started again before proceeding to the next section.

10. Check that the permissions for Everyone in the %SystemRoot%\Forms folder are Change.
11. Check that the permissions for Everyone in the %SystemRoot%\System32 \Oleaut32.dll are Read.

Configuring Microsoft Exchange Client 5.0

Once Microsoft Exchange Server and Client are installed and configured, users can log on to a MetaFrame server on the network and access their mailboxes on the Microsoft Exchange 5.0 Server using the Microsoft Exchange 5.0 Client.

Before you can access e-mail, you must perform the following steps to configure Microsoft Exchange 5.0 Client.

1. Log on to a MetaFrame server that has Exchange Client 5.0 installed.
2. Double-click **Inbox Desktop** or select **Start**, **Programs**, and then **Microsoft Exchange**.
3. When the Setup Wizard appears, verify that Microsoft Exchange Server is checked and that Microsoft Mail and Internet Mail are not checked; click **Next**.
4. Enter the name of the Microsoft Exchange Server. This is typically the name of the server on which Microsoft Exchange 5.0 Server is installed. Also enter the mailbox name; this is typically the username.
5. Select if you travel with the computer and click **Next**.
6. In the **Personal Address Book** dialog box, save Mailbox.pab in the user's home directory.
7. After completing the Setup Wizard, the Exchange Inbox appears.

Setup of Microsoft Exchange 5.0 Client is now complete.

Microsoft Exchange Server (Enterprise Edition) Version 5.5 and Microsoft Exchange Client Version 5.0

Microsoft Exchange Server is a client/server corporate messaging system that incorporates e-mail, scheduling, electronic forms, document sharing, and custom applications in a single product. Microsoft Exchange consists of two parts: Exchange Server and Exchange Client. This document describes a tested method for configuring Microsoft Exchange Server 5.5 and Microsoft Exchange Client 5.0 using a MetaFrame server.

For this application note, two configurations were tested. In the first configuration, Microsoft Exchange Server 5.5 and Microsoft Exchange Client 5.0 were both installed on a MetaFrame server. For the second configuration, Microsoft Exchange Server 5.5 was installed on a dedicated Windows NT 4.0 Terminal Server Edition server and Microsoft Exchange Client 5.0 was installed on a MetaFrame server. With both configurations, multiple users can simultaneously run the client software by creating ICA sessions on the MetaFrameserver. This document does not describe the installation of Microsoft Exchange Server on Terminal Server. For installation on Terminal Server, see the*Microsoft Exchange 5.5 Installation Guide*.

Software Requirements

- MetaFrame Version 1.0
- Microsoft Windows NT 4.0 Terminal Server Edition (optional)
- Microsoft Exchange Server Version 5.5 and Microsoft Exchange Client Version 5.0

Installing and Configuring Microsoft Exchange Server 5.5

Installing Microsoft Exchange Server 5.5

1. Install and configure the MetaFrame server.
2. Log on to the console of the server as a domain administrator.
3. At a command prompt, type **change user /install** and press ENTER. This places the user session in install mode.
4. Run Server\Setup\i386\Setup.exe on the Microsoft Exchange Server 5.5 CD-ROM.
5. Click **Accept** in the Microsoft **Exchange Server Setup** dialog box.
6. Microsoft Exchange Setup offers three choices:
   - Typical Installation
   - Complete/Custom Installation
   - Minimum Installation

   Typical Installation was chosen for this test.
7. Enter the CD Key and click **OK**.
8. Check the **I agree** box in the Microsoft Licensing window and then click **OK**
9. If Microsoft Exchange 5.5 was previously installed on your system, at this point you can make changes to an existing site that you may already have created. For new installs, select **Create a New Site**. Enter your organization name and a user-defined site name.
10. Setup confirms the creation of a new site.

11. Setup asks for an account name and password to be used to log on to the system to start Exchange services when the system boots. Although this can be any user account, it is recommended that the administrator account be used.
12. Source files are now copied to your system.
13. When installation is completed, you can run the Optimizer immediately or run it later at your convenience.
14. At a command prompt, type **change user /execute** and press ENTER.

Installation of Microsoft Exchange Server 5.5 is now complete.

Verifying Installation of Microsoft Exchange Server 5.5

Follow the procedure below to verify that Microsoft Exchange Server 5.5 is correctly installed.

1. From Control Panel, double-click **Services**. Scroll down the Services list and verify that the following services are listed and are automatically started:
   - Microsoft Exchange Directory
   - Microsoft Exchange Event Service
   - Microsoft Exchange Information Store
   - Microsoft Exchange Message Transfer Agent
   - Microsoft Exchange System Attendant
2. Click the **Server Start** button and select **Programs**, then **Microsoft Exchange**. Verify that the following are listed:
   - Microsoft Exchange Administrator
   - Microsoft Exchange Migration Wizard
   - Microsoft Exchange Optimizer
   - Microsoft Exchange Server Health
   - Microsoft Exchange Server History
   - Microsoft Exchange Server IMS Queues
   - Microsoft Exchange Server IMS Statistics
   - Microsoft Exchange Server IMS Traffic
   - Microsoft Exchange Server Load
   - Microsoft Exchange Server Queues
   - Microsoft Exchange Server Users

Configuring Microsoft Exchange Server 5.5

After installing Microsoft Exchange Server 5.5, configure the server for users to log on and retrieve mail. Because Microsoft Exchange Server resides on a MetaFrame server, all users with mailboxes on this Microsoft Exchange Server will also be MetaFrame users. However, MetaFrame users do not automatically have Exchange mailboxes.

▶ **To configure Exchange users**

1. Open Microsoft Exchange Administrator.
2. Type the server name to which you want to connect or click **Browse**. The server is typically the MetaFrame server on which Microsoft Exchange is installed.
3. In the left side of the **Administrator** dialog box, expand the site name icon and click **Recipients**.
4. From the **File** menu, select **New Mailbox** to create mailboxes. Click **Primary Windows NT Account** to associate this new mailbox with an existing account on the domain. If an account does not exist, the form allows creation of new accounts.

Installing and Configuring Microsoft Exchange Client 5.0

Installing Microsoft Exchange Client 5.0

Perform the following steps to ensure a successful Exchange Client installation:

1. Log on to the MetaFrame server as an administrator.

   If Microsoft Exchange Client is not being installed on the same server as Microsoft Exchange Server, skip Steps 2 and 3.
2. From the Control Panel, open **Services** and stop the following services:
   - Messenger
   - Microsoft Exchange Directory
   - Microsoft Exchange Event Service
   - Microsoft Exchange Information Store
   - Microsoft Exchange Message Transfer Agent
   - Microsoft Exchange System Attendant
3. Close the **Services** dialog box and the Control Panel.
4. At a command prompt, type **change user /install** and press ENTER.
5. From the Microsoft Exchange Client CD, run *x*:\Eng\Winnt\i386\Setup.exe, where *x* is the CD-ROM drive.
6. After accepting the copyright policies, enter your name and company information.

7. Change the default installation path if desired.
8. Microsoft Exchange Setup offers three choices:
   - Typical
   - Complete
   - Custom Installation
9. Click **OK** when setup is complete.
10. At a command prompt, type **change user /execute** and press ENTER.
11. If Microsoft Exchange Server 5.5 is installed on the same system where the Exchange Client is installed, make sure that the Exchange Server services you stopped during installation are started again before proceeding to the next section.
12. Check that the permissions for Everyone in the %SystemRoot%\Forms folder are Change.
13. Check that the permissions for Everyone in the %SystemRoot%\System32 \Oleaut32.dll are Read.

Configuring Microsoft Exchange Client 5.0

Once Microsoft Exchange Server and Client are installed and configured, users can log on to a MetaFrame server on the network and access their mailboxes on the Microsoft Exchange 5.5 Server using the Microsoft Exchange 5.0 Client.

Before you can access e-mail, you must perform the following steps to configure Microsoft Exchange Client 5.0.

1. Log on to a MetaFrame server that has Exchange Client 5.0 installed.
2. Double-click **Inbox Desktop** or select **Start**, **Programs**, and then **Microsoft Exchange**.
3. When the Setup Wizard appears, verify that Microsoft Exchange Server is checked and that Microsoft Mail and Internet Mail are not checked; click **Next**.
4. Type the name of the Microsoft Exchange Server. This is typically the name of the server on which Microsoft Exchange 5.5 Server is installed. Also enter the mailbox name; this is typically the username.
5. Select if you travel with the computer and click **Next**.
6. In the **Personal Address Book** dialog box, save Mailbox.pab in the user’s home directory.
7. After completing the Setup Wizard, the Exchange Inbox appears.

Setup of Microsoft Exchange 5.0 Client is now complete.

Microsoft Outlook 98

Outlook is the latest client messaging software from Microsoft. It combines e-mail and scheduling functions seamlessly into one interface.

Requirements

Hardware Requirements

- Server capable of running Microsoft Windows NT 4.0 Terminal Server Edition and MetaFrame

Software Requirements

- MetaFrame Version 1.0
- Microsoft Windows NT Server 4.0, Terminal Server Edition
- Outlook 98

Installation

▶ **To install Outlook 98 on a Windows NT 4.0 Terminal Server Edition with MetaFrame installed**

Note If Outlook 98 and Exchange Server Version 5.0 will be installed on the same MetaFrame/Terminal Server server, Outlook 98 must be installed first.

1. Log on as an administrator and insert the Outlook 98 CD-ROM into the CD drive.
2. When the **Microsoft Outlook** dialog box appears, exit the dialog box.
3. At a command prompt, type **change user /install**. Then run Setup.exe on the root of the Outlook 98 CD.
4. Click **Install Outlook 98** when the **Setup** dialog box appears.
5. Click **Standard Installation**.
6. Click **Corporate email**.
7. Click **Upgrade Only Newer Items**.
8. Allow installation to complete.
9. At a command prompt, type **change user /execute**.
10. Click **OK** to restart the server.
11. When Outlook installation is complete, run Winmsg.cmd from the %SystemRoot\Application Compatibility\Install folder.
12. Follow the directions on the screen. When application tuning is complete, logoff and then back on for the settings to take effect.

Configuration

1. From each Citrix ICA Client, log on to the MetaFrame/Terminal Server server.
2. Select **Start**, **Programs**, and then **Outlook 98** to launch Outlook.
3. In the Outlook Setup Wizard, select only **MS Exchange Server** and click **Next**.
4. Specify the location of the Exchange Server and the owner of the mail account, then click **Next**.
5. Click **No** when asked if you travel with this computer, then click **Next**.
6. Place the Personal Address Book on the user's home drive or a local client drive, then click **Next**.
7. Specify whether or not to add Outlook to the Startup folder and click **Next**.
8. Click **Finish** to complete the configuration.
9. Click **Yes** to make Outlook your default manager for mail, news, and contacts.

Encryption Software

JAWS Data Encryption for the Desktop

Note The information in this technical note was provided by Jaws Technologies Inc., 1013-17th Avenue, SW, Calgary, Alberta, Canada T2T 0A7.

JAWS Data Encryption for the Desktop provides the most sensitive files with fast, compact, and easy-to-use protection. Driven by the JAWS L5 encryption algorithm, you can use this product to safeguard any digital data. This is especially important to Citrix ICA Client users because their data does not reside on their own local drives.

JAWS Data Encryption for the Desktop is a file-based application. A graphical interface much like Windows Explorer allows you to select one or more files that are to be encrypted or decrypted. Once the file(s) are selected, you can choose the appropriate operation from the tool bar. The encryption/decryption is done in-place, meaning that the contents of the selected file(s) are overwritten with the results of the operation. You must encrypt with a private password (or more accurately, a pass phrase) and decrypt with the same password. This process provides a high level of security by ensuring that only those who have the required passwords can view or use data.

Requirements

Hardware Requirements

- 4MB RAM or higher
- A Windows compatible mouse or other pointing device

Software Requirements

- Citrix MetaFrame for Windows NT Server 4.0, Terminal Server Edition
- JAWS Data Encryption for the Desktop, Version 2.1

Installation

Installation is done utilizing a fully automated GUI script that involves six steps. The program installs as either an administrator or user application and can be installed from a client session.

During the installation you are asked to:

- Confirm that the installation is to proceed
- Accept the license agreement
- Accept the default installation directory or browse for a new one
- Accept the name of the Start Menu group or enter a new one
- Accept the copying of files to the hard drive
- Enter your name and company name for registration purposes

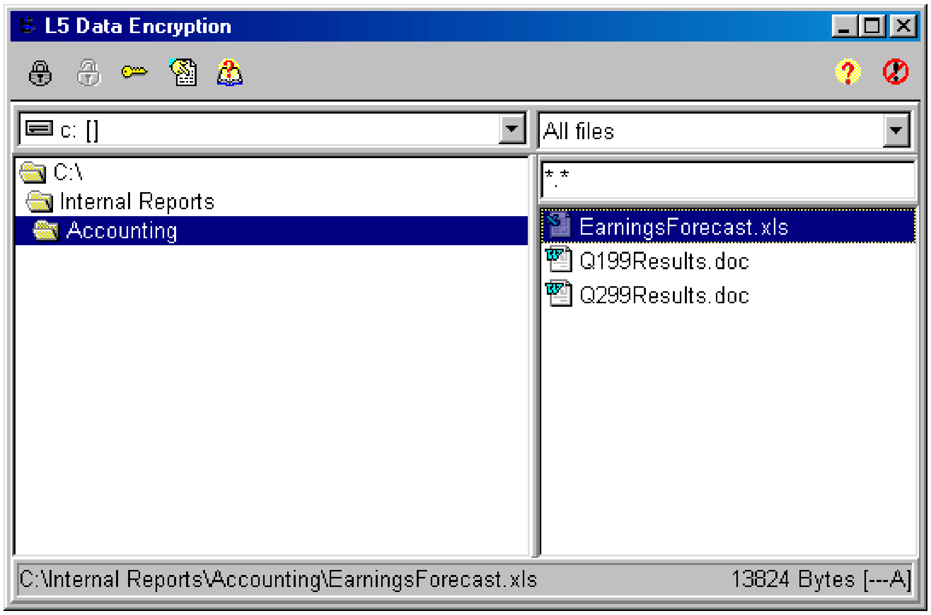
After installation is complete you can access the program from the Start Menu. The entry is called L5 Data Encryption. You must have Execute permission to use the program. This is granted by default.

Usage

1. Start the program from the **Start** Menu.

   The **L5 Data Encryption** dialog box appears.
2. Select a file or a group of files.

   Note You can either encrypt or decrypt files by selecting the appropriate tool button. Only one of the two buttons is enabled, depending on the state of the file. For example, selecting a non-encrypted file enables the decrypt button; selecting an encrypted file enables the decrypt button.



c: []

All files

.

C:\Internal Reports\Accounting\EarningsForecast.xls 13824 Bytes [---A]

The program supports drag-and-drop operations on files and folders. Drag the files or folders that need to be encrypted or decrypted from Explorer or any other Windows drag-and-drop compliant application and drop them on either the program's shortcut or the program window itself. The program scans the incoming files, prompts for the password, and then carries out the encryption or decryption.

Troubleshooting

The following are recommendations for common problems.

Program will not install.

Ensure that you have sufficient disk space remaining on your system to install the program and that you have network permission to write to the drive where you are attempting to install the program.

Program will not load after installation.

Ensure that the media the program is being read from is defect-free and the link to the program software provided by Windows has not been de-registered or moved. Ensure that your system meets the system requirements. If these steps do not alleviate the problem, attempt to reinstall the software from your original distribution media. Setup automatically overwrites any file that is corrupted or removed.

My list of available files is empty.

Check the File Mask box located directly above the File Selection List. If this does not have asterisks (*.*) displayed in the text box, your list of files is limited according to that file mask. Change it to *.*. If this does not reveal more files, try changing the directory in which you are searching for files to process. If files still do not appear in the list, you may not have access to read that directory or drive on that system. Check your network security settings or contact your network administrator for assistance.

I get a "File Access Denied" Message when Encrypting.

From File Manager (Explorer in Windows 95/NT), choose the file you want to work with and either press ALT+ENTER or choose **File** and then **Properties** from the **Main** menu. If the read-only check box is checked, uncheck it and try to encrypt the file again. If this error still persists, you may not have network access to write to the file you are requesting. Check your network preferences or contact your network administrator for assistance.

For additional information about JAWS Data Encryption, contact Jaws technical support at:

Voice: (403) 508-5055
Toll-Free 1-888-301-JAWS (5297)
Fax: (403) 508-5058
support@jawstech.com
http://www.jawstech.com

Fax Software

Zetafax Version 5.0

Zetafax software allows users connected to a network to fax documents from within applications such as Word or Excel. Once Zetafax is installed, a user can fax a document by selecting **Zetafax FaxMerge Printer** from the print menu. The file Zetafax.spl is created and spooled to a directory where it is collected by the Zetafax application and faxed.

MetaFrame extends Zetafax's capabilities by allowing multiple users to send faxes concurrently.

Software Requirements

- MetaFrame Version 1.0
- Zetafax Version 5.0

Installing and Configuring Zetafax 5.0

With the standard Zetafax configuration, spooled fax files are sent to a common location. To prevent concurrent MetaFrame users from overwriting each other's spooled files, each user's home directory is mapped to a common drive letter.

Having a common drive letter mapped to a user's home directory accomplishes two things. It allows the spooling from the Zetafax FaxMerge Printer queue to be set to one location, the single mapped drive letter, and still have the files sent to each user's home directory. Similarly, it allows the Zetafax workstation to look for the spooled files in one location and find them in each user's home directory.

The following instructions assume each user has an assigned home directory with full rights to that directory.

Preliminary Home Directory Setup

For each user, including the administrator:

1. Share the user's home directory and set the share name to the user's name.
2. In User Manager for Domains, select a user and open **Properties** from the **User** menu.
3. Under **Profile**, connect drive Z (or another unused drive letter) to *\\server\%username%*.
4. Log out and log back in. Drive Z (or the drive you specified) is now accessible to each user.

Installing Zetafax Software

1. At a command prompt, type **change user /install**.
2. Install the Zetafax software.
3. Open Zetafax Workstation Setup, select **Install Workstation – standard settings**, and follow the installation instructions.
4. In Workstation Setup, select **Edit Configuration – advanced settings after installation**.
   A. Leave the first entry blank so the Zetafax user name can be determined by the user's network name.
   B. Click **OK** to use the English language.
   C. Type **Z:** for the storage destination of the spooled print files and workstation log.
   D. Click **OK** to exit the configuration editor.
5. When installation is complete, type **change user /execute** at a command prompt.

Printer Setup

1. Click **Start**. Select **Settings** and then **Printers**.
2. Click **Zetafax FaxMerge Printer** and select **Properties** from the **File** menu.
3. Select **Ports** and check the box next to A:\Zetafax.spl.
4. Close the **Properties** and the **Printers** dialog boxes.

Note To fax from a Citrix ICA Client session, the Zetafax workstation must be open in the session.

Financial Software

PeopleSoft 6.x

Note This application note was provided by PeopleSoft. All trade names referred to are the Servicemark, Trademark, or Registered Trademark of the respective manufacturers.

The information contained in this document is subject to change without notice.

This document provides guidelines on configuring and installing Microsoft Windows NT 4.0, Terminal Server Edition - with or without Citrix MetaFrame - for use with PeopleSoft applications.

Supported Configurations

Be sure to check with your administrator to get the latest information on supported configurations, including PeopleSoft versions, Terminal Server versions, and Citrix MetaFrame versions.

CPU and Memory Recommendations

As noted in the latest *PeopleSoft Hardware and Software Requirements Guide,* the recommended minimum client hardware configuration is a Pentium 133 CPU with at least 32MB of RAM. Based on these figures, the following table represents the recommended CPU and memory for a typical Terminal Server running PeopleSoft clients.

Note Sizing is a relative process and, depending on your specific requirements, these numbers can skew either way; this information is only meant as a starting point. Your environment - hardware, applications, user activity level, and so on - dictates your actual needs.

Concurrent users	Processor required	RAM
10–12	One P6 200 or above	256MB+
20–24	Two P6 200 or above	512MB+
30–36	Three PII 233 or above	768MB+
40–48	Four PII 233 or above	1GB+

Concurrent users	Processor required	RAM
48+	Add Terminal Servers based on above model	

Terminal Server Usage Restrictions

The Terminal Server will be servicing many clients, in essence acting as the operating system for all users connected to it. With this in mind, keep the Terminal Server free of PeopleSoft processes that can be handled by other servers. Here are some recommendations for process distribution:

- Never run the database server on the Terminal Server. Run it on a separate machine.
- Never run the PeopleSoft application server on the Terminal Server. Run it on a separate machine.
- Never run Process Scheduler on the Terminal Server. Run it on your database server or on a separate server.
- If possible, use a separate file server to act as the repository for non-shared user files, including PeopleSoft cache files. This puts the burden of read/write file I/O on a separate server, reducing the overhead for the Terminal Server and allowing more of its resources to be devoted to processing user applications.
- Use a high-speed network connection between the Terminal Server and any auxiliary servers, including, but not limited to, database servers, application servers, Process Scheduler servers, and file servers.

User Home Directories

Because multiple Terminal Server clients run on a single server, it is important that each user have his or her own dedicated file area (commonly referred to as a home directory) for non-shared files such as temp and cache files.

PeopleSoft Cache Files

In a client/server environment, each PeopleSoft user has a set of cache files stored on his or her client machine. In the Terminal Server environment, each user must also have a unique set of cache files. You can achieve this by assigning each Terminal Server user a home directory, preferably on a separate server, and using Configuration Manager to point the cache files directory to a subdirectory of that home directory.

Specifying a User’s Cache Files Directory under a Dedicated Home Directory

Only one Terminal Server user should be able to read and write data to each PeopleSoft cache directory.

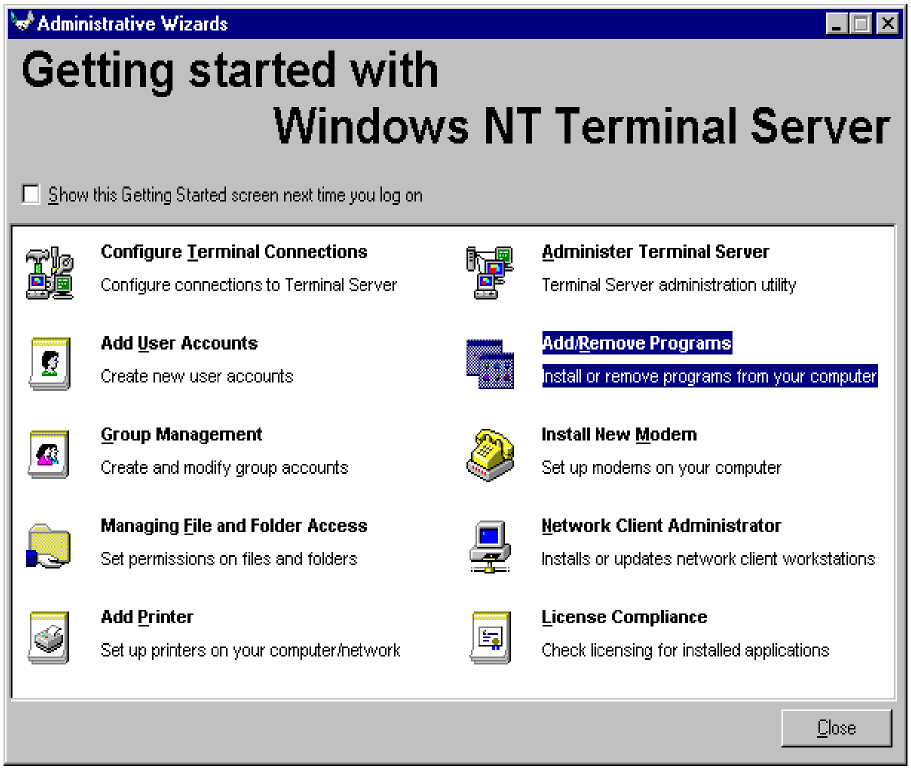
It is equally important that only one PeopleTools instance has access to each set of cache files. If multiple PeopleTools instances access the same set of cache data, you could experience application exception errors. This can happen if a user ends a Terminal Server session improperly, then starts another session. To avoid this, see “Ending a Terminal Server Session” later in this chapter.

Anonymous Users

If your Terminal Server environment uses anonymous logon IDs, make sure that each anonymous ID has its own home directory area and that only one instance of each anonymous user can be logged in at the same time.

Installing Applications

When installing applications on the Terminal Server, such as Microsoft Office or PeopleSoft, if you want all users to be able to access these applications, use the Add/Remove Programs Administrative Wizard and make sure all users begin with common application settings.



Administrative Wizards

Getting started with Windows NT Terminal Server

☐ Show this Getting Started screen next time you log on

Configure Terminal Connections
Configure connections to Terminal Server

Administer Terminal Server
Terminal Server administration utility

Add User Accounts
Create new user accounts

Add/Remove Programs
Install or remove programs from your computer

Group Management
Create and modify group accounts

Install New Modem
Set up modems on your computer

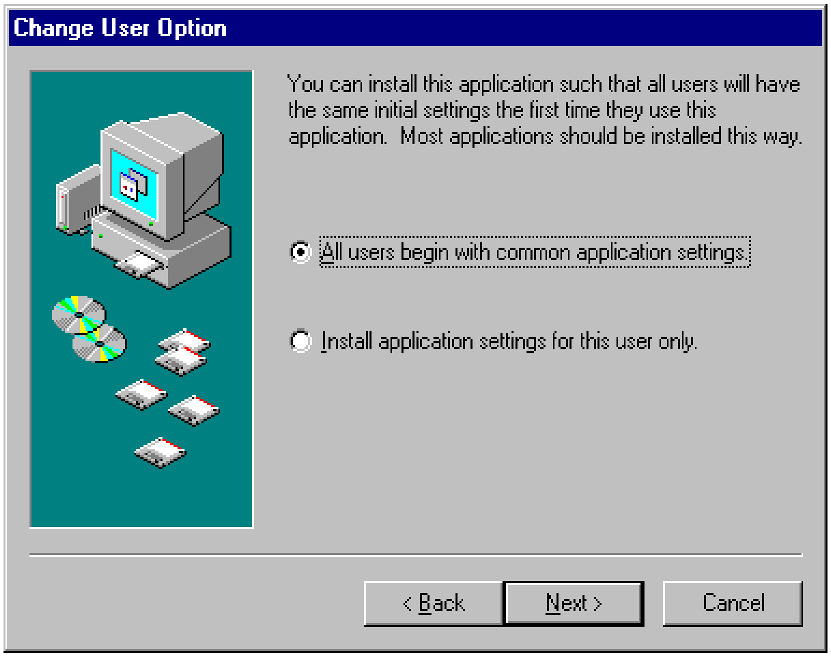
Managing File and Folder Access
Set permissions on files and folders

Network Client Administrator
Installs or updates network client workstations

Add Printer
Set up printers on your computer/network

License Compliance
Check licensing for installed applications

Close



Change User Option

You can install this application such that all users will have the same initial settings the first time they use this application. Most applications should be installed this way.

● All users begin with common application settings.

○ Install application settings for this user only.

Ending a Terminal Server Session

▶ **To end a Terminal Server session**

Click **Start** and then **Logoff** in the session taskbar.

- Or -

Click **Start** and then **Disconnect** in the session taskbar.

- Or -

Click the **Close Window** button at the upper right corner of the title bar.

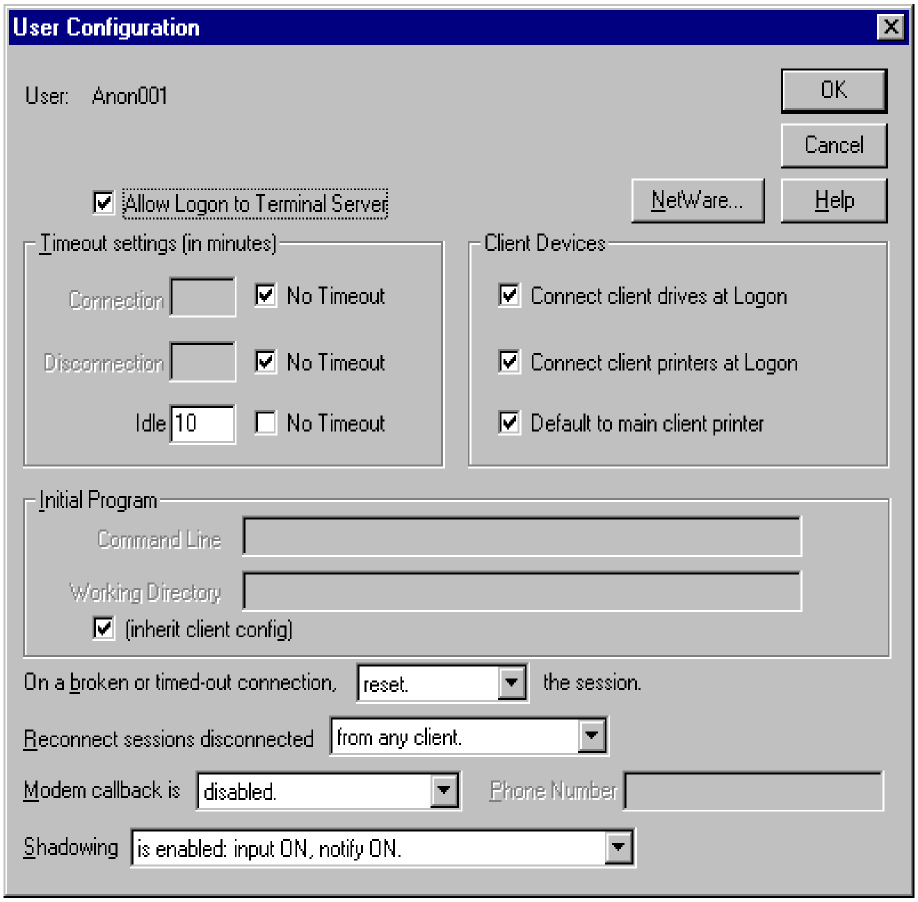
The recommended way to end a Terminal Server session is option 1. This ends the user session and closes down all running programs, including PeopleTools. This ensures that no PeopleTools programs are left running. The next time a PeopleTools program is launched, it will not conflict with any other PeopleTools program run in the previous session. This ensures a clean set of cache files for each user's PeopleTools program.

If you choose options 2 or 3, it is possible for "phantom" programs to be running when users reconnect. This means that multiple instances of PeopleTools are running without the user knowing it. These multiple instances of PeopleTools can corrupt the cache files, causing a system access violation and shutting down PeopleTools.

To further ensure that users are safely closing programs when they leave a session, administrators can set an option in each user's profile. This can be done in two places.

Option 1

1. In User Manager, double-click the user whose profile you want to change.
2. In the **User Properties** dialog box, click **Config** at the bottom of the box.
3. In the **User Configuration** dialog box, change **On a broken or timed-out connection** to **reset** and click **OK**.
4. Click **OK** again and exit User Manager.



User: Anon001

☑ Allow Logon to Terminal Server

Connection ☑ No Timeout

Disconnection ☑ No Timeout

Idle 10 □ No Timeout

☑ Connect client drives at Logon

☑ Connect client printers at Logon

☑ Default to main client printer

Command Line

Working Directory

☑ (inherit client config)

On a broken or timed-out connection, reset. the session.

Reconnect sessions disconnected from any client.

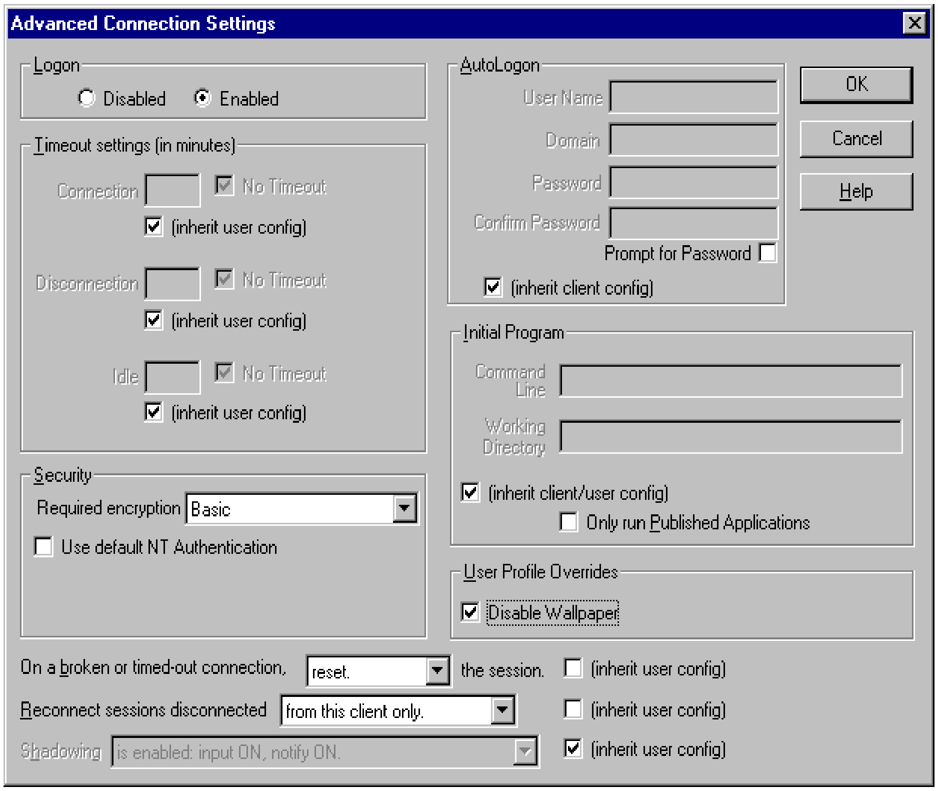
Modem callback is disabled. Phone Number

Shadowing is enabled: input ON, notify ON.

Option 2

1. Click **Start**, select **Administrative Tools (Common)**, and click **Terminal Server Connection Configuration**.

2. In the **Terminal Server Connection Configuration** dialog box, double-click a connection.
3. In the **Edit Connection** dialog box, click **Advanced**.
4. In the **Advanced Connection Settings** dialog box, change **On a broken or timed-out connection** to **reset** and click **OK**.
5. Click **OK** again and exit Terminal Server Connection Configuration.



Logon: ○ Disabled ● Enabled

Timeout settings (in minutes)

Connection ☑ No Timeout ☑ (inherit user config)

Disconnection ☑ No Timeout ☑ (inherit user config)

Idle ☑ No Timeout ☑ (inherit user config)

Security

Required encryption: Basic

□ Use default NT Authentication

AutoLogon

User Name

Domain

Password

Confirm Password

Prompt for Password □

☑ (inherit client config)

Initial Program

Command Line

Working Directory

☑ (inherit client/user config)

□ Only run Published Applications

User Profile Overrides

☑ Disable Wallpaper

On a broken or timed-out connection, reset. the session. □ (inherit user config)

Reconnect sessions disconnected from this client only. □ (inherit user config)

Shadowing is enabled: input ON, notify ON. ☑ (inherit user config)

Performance Tuning Considerations

This section offers suggestions on how to improve the performance of PeopleSoft applications on Terminal Server.

Background Wallpaper

Terminal Server sessions carry display characteristics over the network to the end user. The fewer graphics that need to travel the network, the better the performance for the end user. For this reason, the administrator may want to disable background desktop wallpaper.

PeopleSoft Splash Screen

If you are concerned about the network traffic generated by the PeopleSoft splash screen when signing on from a Terminal Server client, you can disable it.

To disable the splash screen at startup, add the following command line parameter to the Pstools.exe command used to start PeopleTools:

```
-ss NO
```

The entire command line would look like this:

```
N:\PT750\BIN\CLIENT\WINX86\PSTOOLS.EXE –ss NO
```

Troubleshooting

If you are experiencing problems running PeopleSoft applications in your Terminal Server environment, read this section for tips and answers to known issues.

Application Errors

Sometimes when certain users access applications such as Crystal Reports, they get an error message stating dlls or system files are missing. Why does it happen?

Windows Terminal Server is a multiuser operating system. When an application gets installed, it can be installed in one of two ways, either as an application for the specific user installing the application or as an application for all users of the system.

When installing an application, if all users are to have access to it, make sure it gets installed for all users. See “Installing Applications” earlier in this chapter.

File ID Limits

With more concurrent users on Windows Terminal Server, the server frequently gets Event ID 2009 errors in the Event Log? What is this and why does it happen?

Windows NT 4.0 has a limitation of open file handles (FIDs). For each SMB virtual circuit, there is a limit of 2048 FIDs. If client sessions are accessing the same file server, all clients share the SMB virtual circuit; therefore, all clients contribute to the 2048 FID limitation.

This is also true for mappings to the local Windows Terminal Server server. Because most home directory mappings are done by connecting to a shared resource, even if client sessions access a local Terminal Server drive, if a drive mapping is used (for example, virtual drive is mapped with the net use command), all clients have the 2048 FID limitation.

PeopleSoft uses numerous files when running. It is recommended that you use a separate file server to limit resource contention. When using a separate file server, all clients are subject to the combined 2048 FID limit. A solution is to spread users across multiple file servers. The actual limit of users per server is based on actual usage. For example, users who use third-party applications on top of PeopleSoft would use more FIDs.

Host Connectivity Software

Hummingbird eXceed 5 for Windows NT

Hummingbird eXceed 5 for Windows NT is a comprehensive X Window server application for Windows NT and MetaFrame servers. eXceed works with your TCP/IP network to access X applications (also known as X clients) on host computers running X Windows. The eXceed software turns your system into a PC X server. In the X Windows environment, a PC X server is also referred to as an X Windows terminal or server. The X Windows desktop runs as an application on the MetaFrame server. An ICA Client session connected to the MetaFrame server can use eXceed to run X Windows-based applications on a host computer running the X Window environment. The benefits of using Hummingbird eXceed for Windows NT on a MetaFrame server include:

- The ability to deliver an X Windows desktop over a low bandwidth connection with excellent performance
- The MetaFrame server and ICA Client sessions can replace expensive X Terminals

Software Requirements

- Hummingbird eXceed 5 for Windows NT Version 5.0.1
- Microsoft Windows NT Server 4.0, Terminal Server Edition
- MetaFrame Version 1.0

Installation

There are three steps to installation and configuration.

- Installing the Hummingbird Application Software on the MetaFrame server
- Installing the ICA Client software for each user
- Configuring the ICA Client software for each user

Installing Hummingbird Application Software

The first step in installing eXceed 5 is to install the shared server portion of the Hummingbird Application Software on the MetaFrame server.

1. Log on to the MetaFrame server as an administrator.
2. At a command prompt, type **change user /install** and press ENTER.
3. Insert the Hummingbird eXceed 5 CD-ROM into a CD-ROM drive on the MetaFrame server.
4. At a command prompt, change the working directory to the \Exceed directory on the eXceed 5 CD-ROM.
5. Type **expand msvcrt20.dl_ %systemroot%\system32\msvcrt20.dll** and press ENTER.
6. Type **expand ctl3d32.dl_ %systemroot%\system32\ctl3d32.dll** and press ENTER.
7. Type **expand mfc30.dl_ %systemroot%\system32\mfc30.dll** and press ENTER.
8. Run Setup from the \Exceed directory on the CD-ROM.
9. When Setup starts, select **Shared User Installation** and then **Express**. Specify a local directory on the MetaFrame server (for example, C:\Win32app\Exceed).
10. When installation is complete, type **change user /execute** and press ENTER.

    The eXceed 5 shared server is now installed. Each user who will use eXceed must perform an installation from the C:\Exceed\Userins directory. This process is detailed below. If the administrator has already installed the client software, go directly to “Client Configuration” later in this chapter. All other users must perform a client software installation from the shared directory.

Installing Hummingbird Client Software

This section describes the client-side installation of the Hummingbird Application Software. This must be done by each MetaFrame user who will run the Hummingbird eXceed application.

1. Log on to the MetaFrame server as a user.
2. Run Setup from the \Exceed\Userins directory created in Step 7 above.
3. The first Setup popup asks you to specify the eXceed home directory. Specify the directory created in Step 9 above.
4. The next popup asks you to specify the user’s home directory. Specify the user’s home directory; for example, %SystemRoot%\Profiles\DanielA\Exceed.
5. For users without rights to \%SystemRoot%\System32, three errors will appear during the file copy, each saying “MoveFileEx: Error#{5}. The requested access was denied.” Click **OK** each time. This indicates the administrator copied the files to the proper directory in Steps 5, 6, and 7 above.
6. Each user must select a password to configure the X configuration setup.

7. You are asked if you want to tune the video display. Click **Yes** if MSVCRT20.DLL was copied into the %SystemRoot%\System32 directory. If it was not, click **No**.

Client Configuration

This section describes the client-side configuration of the Hummingbird Application Software. This configuration must be done by each MetaFrame user who will run eXceed.

1. After the eXceed client software is installed, double-click on the Xconfig icon in the eXceed program group.
2. Double-click the Communication icon. Set the mode to XDMCP-indirect and select a unique display number for each user.

Note Each user must have a unique display number. If two users have the same user number, incorrect program operation can occur.

3. Select **Configure** and enter the IP address of the X server running XDM.
4. Click **OK** twice.
5. Select the Windows Mode icon and set the Window mode to **Single**.
6. Click **OK**.
7. Select the Transports icon, enter the broadcast address, and click **OK**.
8. Close the Xconfig window and run the eXceed icon in the eXceed program group to run an X-Windows session from the selected XDM server.

Note At this time eXceed does not support multiuser 3270 connectivity under MetaFrame.

Modem Connectivity Software

Comtrol RocketModem

The Comtrol RocketModem is a multimodem, ISA bus expansion card. This document describes a tested configuration of Comtrol RocketModem with Citrix MetaFrame.

Requirements

Hardware Requirements

- Dell OptiPlex GXi with one Pentium processor
- Comtrol RocketModem card with four modems

Software Requirements

- MetaFrame Version 1.0
- Comtrol RocketModem Device Driver Version 3.14

Installing Comtrol RocketModem Card

1. Turn the computer off, remove the computer cover, and select a slot to install the controller.
2. Remove the expansion slot cover and insert the RocketModem card.
3. Replace the covers and restart the system.

Installing Comtrol RocketModem Device Driver

1. In Control Panel, double-click **Network**.
2. Click the **Adapters** tab and then click **Add**.
3. Click **Have Disk**.
4. Enter the path of the installation files and click **OK**.
5. In **Select OEM Option**, select **Comtrol RocketPort/RocketModem** and click **OK**.
6. In **RocketPort/RocketModem NT Setup**, select an I/O address range (180-1c3 hex default was chosen for this installation) and select the starting COM port for the first controller.

Note Make sure that these selections do not conflict with an existing I/O address range or with COM ports already in use.

7. In the remaining **RocketPort/RocketModem Setup** dialog boxes, click **OK**.
8. Close the **Network Settings** dialog box.
9. Click **Yes** to reboot the system.

Setting up Comtrol RocketModem

1. In Control Panel, double-click **Modems**.
2. Click **Add**.
3. Allow the modem installation procedure to detect the modem.
4. Select the first COM port used for the RocketModem and click **Next**.
5. When the Comtrol V.34 RocketModem is found, click **Next**.
6. Select all ports in the range assigned to the RocketModem board and click **Next**.
7. Enter location information and click **Next**.

8. Click **Finish** to complete the setup.
9. Click **Close**.

Terminal Connection Configuration Using Comtrol RocketModem

1. Click **Start**, select **Programs**, then **Administrative Tools**, and then **Terminal Server Connection Configuration**.
2. In the **Terminal Server Connection Configuration** dialog box, click **Connection** and select **New**.
3. Enter a connection name, select **Citrix ICA 3.0** for type, select **Async** for transport, select one of the RocketModem COM ports for device, and then click **OK**.
4. In the **Reboot Message** dialog box, click **OK**.
5. Repeat Steps 1–4 for additional terminal connections.
6. Reboot the server.

Configuring ICA Clients to use Comtrol RocketModem

1. Using a text editor, open \System32\RAS\Modem.inf.
2. Using a text editor, open \Program Files\Citrix\ICA Client\Modem.ini.
3. Maintaining alphabetical order, add the name of the RocketModem that is listed in the Modem.inf file to the top portion of the Modem.ini file and add an equal sign at the end of the modem name; for example, Comtrol RocketModem=.
4. Copy the initialization strings from the Modem.inf file and paste them at the end of the Modem.ini file.
5. Close the Modem.inf file and save and close the Modem.ini file.
6. With the text editor, open \Program Files\Citrix\ICA Client\Wfclient.ini.
7. Below the last COM port listed in the Windows COM Port Name section of the Wfclient.ini file, add the COM port followed by an equal sign for each port to be used by the RocketModems; for example, COM5=.
8. Save the Wfclient.ini file and close the text editor.

Citrix ICA Clients can now access the RocketModems.

Verifying the Installation of Comtrol RocketModem

Follow the procedure below to verify that the Comtrol RocketModem is correctly installed and configured:

1. Connect the modem ports to phone ports.

2. Click **Start**. Select **Programs**, **Accessories**, then **Hyperterminal**, and click **HyperTerminal**.

Note If this is the first time you are using HyperTerminal, enter an area code and click **Close**. When prompted, type a modem name.

3. Type a name in **Connection Description** and click **OK**.
4. In the **Connect To** field, enter an area code and a phone number that can be used for testing.
5. In the pull down list to the right of the **Connect** dialog box, select the first of the RocketModems.
6. In the **Connect** field, click **Dial**.
7. Verify the connection is made.
8. Repeat Steps 1–7 for each RocketModem.

SpartaCom SAPS Server for Windows NT Version 3.20

SpartaCom SAPS Server for Windows NT enables COM port sharing with SAPS Clients. This document describes a tested method for configuring SpartaCom SAPS Server using MetaFrame. This document also discusses the current limitations of SAPS.

Requirements

Hardware Requirements

- MetaFrame server

Software Requirements

- MetaFrame Version 1.0
- SpartaCom SAPS Server Version 3.20
- SpartaCom SAPS Client Version 3.20

Installing SpartaCom SAPS Server

1. Log on to the console of the MetaFrame server as an administrator.
2. At a command prompt, type **change user /install** and press ENTER. This places the user session in install mode.
3. Run Setup.exe from the SAPS Server diskette. The **Welcome** dialog box appears.
4. In **Welcome**, click **Next**.
5. Select **Install SAPS Server and its Manager** and click **Next**.

6. In the **User Information** dialog box, enter the appropriate **Name** and **Company**.
7. In the **Registration Confirmation** dialog box, click **Yes**.
8. Enter the installation location and click **OK**.
9. In the **Select Program Folder** dialog box, click **Next**.
10. Enter the license key and click **Next**.
11. Uncheck the **Yes, I want to launch SAPS Server Manager now** box and click **Finish**.
12. At a command prompt, type **change user /execute** and press ENTER. This returns the user session to execute mode.

Installing SpartaCom SAPS Client

1. In Control Panel, double-click **Network**.
2. Select the **Services** tab and click **Add**.
3. Click **Have Disk**.
4. Insert the SAPS Client for Windows NT diskette into the disk drive and click **OK**.
5. When **SpartaCom Asynchronous Port Sharing - Windows NT Client** appears in the **Select OEM Option** dialog box, click **OK**.
6. Enter the license key and click **OK**.
7. In **SAPS Ports Configuration**, set the names of the four ports and click **OK**.
8. Click **Yes** to view the Readme files or click **No** if you don’t want to view the Readme files.
9. Close **Network Settings**.
10. Reboot the server.

Configuring SpartaCom SAPS Server

1. Click **Start** and select **Programs**, then **SAPS**, and then **SAPS Server Manager**.
2. From the **Configuration** menu, select **Shares**.
3. Click **New**.
4. Enter a share name and the COM port to be shared; that is, WFCOM3 for the share name and COM3 for the shared port. Do not select more than one COM port for a given share name.
5. Repeat Steps 2–4 for any additional ports to be shared.
6. Close the **Shares** dialog box.
7. In Control Panel, double-click **SAPS Port Redirector**.

8. Select one of the SAPS ports and click **Settings**.
9. Enter the network path to the shared COM port that was established in Step 4; for example, \\servername\WFCOM3, where *servername* is the name of the MetaFrame server. Do not select **Use Pools**.
10. Repeat Steps 8 and 9 for any other ports to be redirected.
11. Close the **SAPS Port Redirector** dialog box.

The shared COM ports can now be accessed remotely through an ICA session.

SpartaCom SAPS Limitations

SpartaCom SAPS Server does not support COM port pooling with MetaFrame. This is a limitation of the SAPS software and not MetaFrame. If a SAPS client tries to access a port that is in use, pooling automatically finds an unused port and assigns it to the SAPS client. This feature works correctly unless a SAPS client tries to use more than one shared port from the same machine. In this case, pooling fails and the SAPS client receives an “Access is Denied” message when trying to access the second port. With MetaFrame, multiple sessions can run on the same machine, so pooling fails.

Networking Software

Microsoft Windows NT Multi-Protocol Routing Service

This document describes how to install and integrate the Microsoft Windows NT Multi-Protocol Routing Service on a Microsoft Windows NT Server 4.0, Terminal Server Edition. Multi-Protocol Routing enables small- to medium-sized organizations to deploy a Terminal Server as a low cost LAN-to-LAN routing solution for TCP/IP and IPX networks, eliminating the need for a dedicated router. The Multi-Protocol Routing Service can also be used to link LANs that have different network topologies (such as Ethernet and Token Ring). Each packet sent over a LAN has a packet header that contains source and destination address fields. Using the packet header information, the routing service receives network packets from a source and routes them to their destination using the shortest path available. This reduces network traffic on other LAN segments, optimizing network performance.

The Multi-Protocol Routing Service allows Terminal Server to act as a router for the network. Any ICA Client on any attached network loop can establish a remote session from a MetaFrame server on any other network loop using the TCP/IP and IPX protocols.

The Multi-Protocol Routing Service consists of three services:

- Routing Information Protocol (RIP) for TCP/IP

- DHCP Relay Agent for the Dynamic Host Configuration Protocol (DHCP)
- RIP for NWLink IPX/SPX Compatible Transport

RIP is a protocol used by routers to dynamically exchange routing information. After installing RIP for IP and IPX, Terminal Server routes these protocols and dynamically exchanges routing information with other routers running the RIP protocol. The DHCP relay agent allows the Terminal Server router to forward DHCP requests to DHCP servers on other subnets. This allows one DHCP server to service multiple IP subnets.

Requirements

Hardware Requirements

- Terminal Server with two or more network cards for full Multi-Protocol Routing functionality

Software Requirements

- MetaFrame Version 1.0
- Microsoft Windows NT Server 4.0, Terminal Server Edition

Installation

1. Click **Start**, select **Settings**, and click Control Panel.
2. On Control Panel, double-click Network.

   The **Network** dialog box appears.
3. From the **Services** tab, click **Add**.

   The **Select Network Services** dialog box appears. Install the following services:

   - RIP for Internet Protocol (requires static IP addresses for each network card)
   - DHCP Relay Agent (select only if you want to route DHCP request)
   - RIP for NWLink IPX/SPX compatible transport

   When prompted, enter the path of MPR distribution files; these are located on the Terminal Server compact disk.
4. After installing the RIP for Internet Protocol, a screen appears telling you that RIP for Internet Protocol requires a static IP address for each network card. Click **OK** to configure the IP information during setup of RIP for IP. After installing the DHCP relay agent, you are asked to enter the IP address of DHCP servers to which you want to send DHCP requests. Leave Maximum Hops and Seconds Threshold at their default values.

Configuration and Troubleshooting

RIP for IP

After RIP for IP is installed, you need to add static IP addresses for each of the network cards.

1. In the **Network** dialog box, click the **Protocols** tab and double click on **TCP/IP Protocol**.

   The **Microsoft TCP/IP Properties** dialog box opens.
2. Click the **Routing** tab. Make sure **Enable IP Forwarding** is checked.
3. Click the **IP Address** tab.

   The **Adapter** field lists all the network cards installed on your machine.
4. Click **Specify an IP address**.
5. Specify the IP address and the subnet of each network card.
6. In the **Default Gateway** field, enter the IP address of the network where you want to route the packets.

Note At a command prompt, type **route print** to see what routes your machine has. You can also use the **ping** and **tracert** commands to troubleshoot or verify that the Multi-Protocol Routing service is working for TCP/IP.

After installing RIP, Terminal Server starts exchanging routing information with other RIP routers. For more information on TCP/IP, see the appropriate Terminal Server documentation.

RIP for NWLink IPX/SPX Compatible Transport

When installing RIP for IPX, Setup displays a message that NetBIOS Broadcast Propagation is currently disabled. If you are using NetBIOS over IPX or are unsure, choose **Yes** to enable broadcast of type 20 packets. Reboot the Terminal Server as directed. The Enable RIP Routing box in the NWLink IPX/SPX configuration is automatically checked when installing RIP for IPX.

If no network number is defined for the segment to which Terminal Server is connected, you must define a unique network number for that segment. For example, if you have a Terminal Server with two network interface cards and the first network card is connected to an existing Novell network, you can leave the network number blank because Terminal Server auto-detects the network number for that segment. If the second network card is connected to the Microsoft network; no IPX network number is defined for this segment. You must type in a unique network number for this segment. Use Ipxroute.exe to determine the network number of your network adapter. Ensure that the same frame types are selected for both network adapters.

Productivity Software

Symantec ACT! Version 3

Symantec's ACT! 3.0 is a business contact management program. MetaFrame extends ACT!'s capabilities by allowing multiple users to simultaneously use ACT! with shared or unshared contact databases. This document describes a tested method of configuring ACT! 3.0 using MetaFrame.

Requirements

Hardware Requirements

- MetaFrame server

Software Requirements

- MetaFrame Version 1.0
- ACT! Version 3

Installing ACT!

1. At a command prompt, type **change user /install**.
2. Run Setup.exe from the ACT! CD-ROM.
3. Fill in the user information.
4. Select the installation location.
5. Select the type of installation (Typical was chosen for this test configuration).
6. Complete registration information.
7. At a command prompt, type **change user /execute**.

Configuring ACT!

On MetaFrame, ACT! can be set up to allow a shared database to be used simultaneously by multiple users and for unshared databases to be used by individuals. In either case, permissions must be set to allow proper access.

All users who share a common database must have access to both the database file (that is, Contacts.dbf) and the directory that contains the database file (for example, C:\Act\Database). If a user does not have the correct permissions when he or she starts ACT! for the first time, the Database Setup Wizard will not accept any database filenames. When this happens, the user must exit the Setup Wizard and choose **New** from the **File** pull-down menu to create a database and save it in a location where he or she has sufficient rights.

Verifying Installation of ACT!

Follow the procedure below to verify that ACT! is correctly installed and configured:

1. Click **Start**, select **Programs**, **ACT! 3.0 for Windows,** and then **ACT! 3.0**.
2. Follow the Setup Wizard (default values were used in the test configuration).
3. Enter **My Record** information.
4. Click **Contact** and then **New Contact** from the menu bar to add a new contact.
5. From the menu bar, select **Lookup**, then **Company,** and enter the name of a current contact with the company name you selected.

Note ACT! does not allow any two users of a shared database to make concurrent changes to the same contact record. Once a user starts to change a record, that user must save the changes or switch to a different record before others can make changes to the record. ACT! allows users of a shared database to make concurrent changes to different contact records.

Additionally, if an alarm is set for a scheduled activity, all users concurrently running ACT! and using the same database receive the alarm.

Corel WordPerfect Suite 8

Corel WordPerfect Suite 8 is an office application suite that includes WordPerfect, Quattro Pro, and Presentations. MetaFrame extends WordPerfect Suite 8 capabilities by allowing multiple users to concurrently use any of the suite's programs. This document describes a tested method for configuring WordPerfect Suite 8 using MetaFrame.

Requirements

Hardware Requirements

- MetaFrame server

Software Requirements

- MetaFrame Version 1.0
- Corel WordPerfect Suite 8

Installing Corel WordPerfect Suite 8

1. Install and configure MetaFrame as a standalone server or a domain controller.
2. Log on to the console of the MetaFrame server as an administrator.
3. At a command prompt, type **change user /install** and press ENTER. This places the user session in install mode.

4. Insert the Corel WordPerfect Suite 8 CD in the CD-ROM drive.
5. When AutoRun displays the Corel WordPerfect Suite 8 Applications Disk window, click **Corel WordPerfect Suite Setup**.
6. Click **Next** in the **Welcome** dialog box and **Yes** in the **License Agreement** dialog box.
7. Enter the appropriate information in the **Registration Information** dialog box.
8. Select the type of installation: **Typical**, **Compact**, **Custom**, or **Run From CD-ROM**. (For this installation, Typical was chosen.)
9. Enter the installation location.
10. Select the components to be installed. (All components were selected during this installation.)
11. Click **Install** in the **Ready to Install** dialog box.
12. When installation is complete, click **OK** to exit setup.
13. At a command prompt, type **change user /execute** and press ENTER.

Verifying Installation of Corel WordPerfect Suite 8

Follow the procedure below to verify that WordPerfect Suite 8 is correctly installed and configured:

1. Select **Corel Desktop Application Director 8** from the Accessories program group.
2. Double-click the WordPerfect icon and verify that WordPerfect starts correctly.
3. Repeat Step 2 for Quattro Pro and Presentations.

Lotus Notes 4.0 for Windows NT

This application note describes how to integrate Lotus Notes 4.0 server and workstation software with MetaFrame. Lotus Notes is a workgroup environment for developing applications that enable groups of people to share information and work together. Lotus Notes enables you to communicate with colleagues, collaborate in teams, and coordinate strategic business processes.

There are two parts to the Notes installation.

- Installing Lotus Notes Server for Windows NT on a Windows Terminal Server/MetaFrame server
- Installing Lotus Notes Workstation for Windows NT that can also run on a MetaFrame server

If a Lotus Notes server is already running in your network and you are not installing Notes on a MetaFrame server, proceed to the Installing Lotus Notes workstation section later in this chapter. If you plan on running both Lotus Notes erver and Lotus Notes workstations on a MetaFrame server, follow the directions in both the server and workstation install sections.

Installation Note Although both the Lotus Notes server and many copies of Lotus Notes workstation for Windows can run on a single MetaFrame server, this may not be the best solution. If the system running MetaFrame is a high end, multiprocessor machine with a large amount of RAM and a very fast hard disk subsystem, this configuration will work fine. However, if the MetaFrame servers are configured to meet only MetaFrame needs, you need to add more computing resources to that machine or consider running Lotus Notes server on a separate machine. It is recommended that you have a standalone Windows NT Server to run Lotus Notes server and run the Lotus Notes workstation client on the MetaFrame servers. This allows Lotus Notes server to use all of the system resources of a separate machine. The MetaFrame server(s) with the Lotus clients can then support multiple remote or network users who want to access the Lotus Notes server.

Lotus Notes Workstation for Windows NT allows you to do a public install. It is suggested that you do a single public install to the MetaFrame server or to any available network server. Users who want to set themselves up for Lotus Notes access can then run the standard Lotus Notes workstation installation from the public install by changing into that directory and running Setup.

Requirements

Hardware Requirements

- One MetaFrame server

— or —

- One MetaFrame server and one Windows NT 4.0 server

Software Requirements

- MetaFrame Version 1.0
- Citrix ICA Client
- Lotus Notes Release 4.0

Installation

▶ **To install Lotus Notes Server for Windows NT on a MetaFrame Server**

1. It is recommended that you create an administrative user specifically for Lotus Notes on the MetaFrame server that will run the Lotus Notes server. Log on to the MetaFrame server as this administrative user.

2. Before proceeding with the Notes server installation, you must run **change user /install** from the command prompt, if you want to run Notes server as an automatic service. However, this does not allow you to run the Administrators Personal Workstation at the same time that the Notes server is running. Therefore, it is recommended that you run the Administrators Personal Workstation from a workstation rather than the Notes server.
3. Proceed with installing Lotus Notes server for NT. Run install from the Win32\Install directory on the Lotus Notes 4.0 CD-ROM or from the floppy diskettes made from the Win32\Disk_Kit directory. Register the software.
4. In the **Install Options** dialog box, click **Server Install** and select directories and the group under which you want to install.
5. After installation of the Notes server is complete, Notes places the Lotus Notes Server and Workstation icons in a Common program group on your desktop. Move these icons to a Personal Program Group. This situation only arises if you are using a single MetaFrame server for the Notes server and client workstation installs (see the Installation Note above).
6. The first time you double-click the Notes Workstation icon, Notes Setup starts automatically. You must complete server setup before working in Notes. If you try to start Notes server without first completing Notes setup, the server exits with the message: "You must first run the workstation server setup program to set up your system. To restart the setup process, double-click the Notes workstation icon."
7. Proceed with Lotus Notes installation. See Lotus Notes documentation for specifics of the Lotus Notes server setup.
8. When server setup is complete, you need to name the port (that is, SPX; LAN0) under Tools, Server Administration, Servers, Servers View. Double-click the appropriate server and edit Server and Network Configuration.
9. Running Notes as an automatic service is useful if you need to start the server from a remote location or to restart automatically after a system failure. You can install the Lotus Notes server as a service from the Notes program directory (C:\Notes).

   A. At the command prompt, type **cd \notes** and press ENTER.

   B. At the C:\Notes prompt, type **ntsvinst -c** and press ENTER.

   C. Click **Start**, select **Settings**, and click **Control Panel**.

   D. Double-click the Services icon.

   E. Double-click **Lotus Notes Server - Manual**.

   F. Select **Automatic** as the startup type and select **System Account** in the **Log On As** dialog box.

   G. Select **Allow Service to Interact with Desktop**.

10. Reboot the MetaFrame server to start the Lotus Notes server, or run **change user /execute** from the command prompt and double-click the Notes server icon to start the Notes server manually.

▶ **To install the Lotus Notes Workstation Program for Windows on a MetaFrame Server**

1. Log on to the MetaFrame server that you are going to install the Notes client on using the desired Citrix ICA client (DOS, Win16, or Win32). Log on as the user for whom you want to set up the Lotus Notes workstation for Windows program.
2. If you did a public install of the Lotus Notes workstation for Windows program, **net use** the directory on the network, change to the Notes public directory, and run the install program. If a public install was not done, load the CD-ROM or floppy diskettes and do a normal install of the workstation program. Run install from the Win32\Install directory or from the floppy diskettes created from the Win32\Disk_Kit directory.
3. When the install program is launched, you may receive a message telling you there are multiple copies of Notes for Windows on the hard disk. This is to be expected because there may be many clients using this particular MetaFrame server as a Notes workstation.
4. At the **Install Options** panel, choose **Standard Install** and point your Program and Data drive paths to the users Windows directory; for example, \Wtsrv\Profiles\Daniela\Notes and \Wtsrv\Profiles\Daniela\Notes\Data. Select **Program Group** and proceed with workstation installation. If the selected User Profile Path is not the default, you must provide the Profile Path Name.
5. Repeat Steps 1-4 for each user who wants to set up the Lotus Notes workstation program for Windows.

Lotus SmartSuite 97

This application note describes how to install Lotus SmartSuite 97 on a MetaFrame server.

Lotus SmartSuite 97 is a package of 32-bit software applications that operate together to make work easier and communication more effective. The package includes Lotus SmartCenter 97 and SuiteStart 97 (command centers that access desktop applications and application files), Lotus 1-2-3 97 (a spreadsheet program), Lotus Word Pro 97 (a word processor), Lotus Approach 97 (a database), Lotus Freelance Graphics 97 (a presentation graphics package), Lotus Organizer 97 (a personal information management tool), and Lotus ScreenCam 97 (a show-and-tell communication tool).

Organizer 97 and ScreenCam 97 are not supported under MetaFrame Version 1.0. During installation, you are asked if you want to install the ScreenCam files. Errors in installation **will occur** if these files are installed.

Software Requirements

- Microsoft Windows NT Server 4.0, Terminal Server Edition
- MetaFrame Version 1.0
- Lotus SmartSuite 97

Installation

There are three ways to install Lotus SmartSuite 97:

- Standard
- File Server
- Network Distribution.

A standard installation olaces the product on the MetaFrame server's hard disk. This allows ICA clients to access the applications from the MetaFrame server desktop.

A file server installation allows Lotus applications to be shared by multiple "node" users on networks such as Windows NT or Novell NetWare. The main portion of the applications reside in one location, or sharepoint, and all node users are configured to use the applications from that location. All users must have access to this shared location through a network or on a local machine.

A distribution installation copies the contents of the Lotus diskettes or CD-ROM to the MetaFrame server. You can then use the copy on the MetaFrame server to perform subsequent standard, file server, or network distribution installs. This installation is useful if you will be running several standard installs to other machines. You can run Install from the distribution location on the MetaFrame server or network sharepoint rather than installing from disk or CD-ROM on each machine.

▶ **To perform a standard installation of Lotus SmartSuite 97 on a MetaFrame server**

1. Log on to the MetaFrame server as a local administrator.
2. At a command prompt, type **change user /install**.
3. Run Install.exe from the SmartSuite 97 CD-ROM.
4. Continue the installation following the directions in the SmartSuite 97 manual, with the following exception:

   ScreenCam 97 does not run on MetaFrame 1.0 or Windows NT. Do not install the files. If the files are installed, the installation terminates with the error: "CAM+1359: Path/file access error."
5. After installation, the program prompts you to restart the computer. Click **Restart**.

▶ **To perform a file server installation of Lotus SmartSuite 97 on a MetaFrame server**

1. Log on to the MetaFrame server as a local administrator.
2. At the command prompt, type **change user /install**.
3. Run Install.exe from the SmartSuite 97 CD-ROM.
4. Check the **File Server or Multiple User Install** check box at the bottom of the initial **Welcome** dialog box.
5. Click the **File Server Install** radio button when prompted for the type of network installation.
6. Continue the installation following the directions in the *SmartSuite 97 Network Administrator Manual* or the SmartSuite 97 Readnet.txt file., with the following exception:

   ScreenCam 97 does not run on MetaFrame 1.0 or Windows NT. Do not install the files. If the files are installed, the installation terminates with the error: "CAM+1359: Path/file access error."
7. At the command prompt, type **change user /execute**.
8. Open the <Path>\Application Compatibility Scripts\Logon\SS97Usr.cmd file. Uncomment the appropriate node install program (Interactive or Scripted) and update the path to the install program if needed. Save and exit the file.

   Note The change to SS97Usr.cmd is done only once for all users.

   The interactive mode requires input from the end user, including the path to store the node data and which components to install.

   The scripted or batch mode uses a script file that the administrator sets up. With this method, there is no chance for the user to enter incorrect configuration information. Because it is easier for the end user and is safer, it is the recommended method.
9. Run the <Path>\ Application Compatibility Scripts\Install\Ssuite97.cmd script.

   When prompted, enter a drive letter to be used to map to each user's home directory.

   If you have no preference, drive W is suggested. When you complete this task, save the file and exit.

   Note Once you choose a drive letter, it applies for all users for all applications.
10. When the script completes, log off the system and log back on before using the application. Make sure the application compatibility script has added SS97Usr.cmd in the Startup folder.

    A. Right click **Start**.

B. Click **Open All Users**.

C. Double-click **Programs**.

D. Double-click **Startup**. Verify that SS97Usr.cmd is present.

11. After the installation completes, run a node install for each user. This installation program varies for interactive mode and scripted mode.

    If run in interactive mode, each user is prompted for individual setup.

    Note When selecting the drive and parent folder where the SmartSuite applications are to be installed, drive C must be changed to match the drive settings set during the execution of Ssuite97.cmd. By choosing to install a node over shared Lotus files, you can corrupt Smart Suite. It is recommended that you create a response file and run in batch mode.

    Scripted or batch mode is accomplished by reading and modifying the Instsuit.rsp file contained on the SmartSuite 97 CD-ROM. The CD also contains a text file, Readnet.txt, that contains more information about this topic.

12. The client can now run the applications by accessing the sharepoint where Lotus SmartSuite 97 was installed.

▶ **To perform a network distribution installation of Lotus SmartSuite 97 on a MetaFrame server**

1. Log on to the MetaFrame server as a local administrator.
2. Run Install.exe from the SmartSuite 97 CD-ROM.
3. Check the **File Server or Multiple User Install** check box at the bottom of the initial **Welcome** dialog box.
4. Click the **Network Distribution Install** radio button when prompted for the type of network installation.
5. Continue the installation following the directions in the *SmartSuite 97 Network Administrator Manual* or the SmartSuite 97 Readnet.txt file.
6. The client can now install SmartSuite 97 by accessing Install.exe using the sharepoint on the network or by logging onto the MetaFrame server where the installation was executed and running Install.exe from there.

Microsoft Office 97

This application note describes how to install Microsoft Office 97 on a MetaFrame server.

There are four outstanding issues with Office 97 at the present time:

- Error initializing the Visual Basic environment with a user who does not have administrative rights
- Office Startup icons are not added to a common Startup Group on the MetaFrame server
- Clip art insertion from client does not work due to read-only permissions
- Hyperlink insertion for users produces Internet Explorer (IE) error

Solutions to these problems are presented later in this chapter.

Software Requirements

- MetaFrame Version 1.0
- Microsoft Office 97

Installation

▶ **To install Microsoft Office 97 on a MetaFrame server**

1. Log on to the console as a local administrator.
2. At a command prompt, type **change user /install**.
3. Run Setup.exe from the Office 97 CD-ROM.
4. Continue the installation following the directions in the Office 97 manual.

Note If the server drives were remapped during MetaFrame installation, the following error messages appear when 84% of Microsoft Office 97 is installed:

“Setup tried to create an invalid path using C:\MSoffice\Winword and Bookshelf.dll.”

“Setup tried to create an invalid path using C:\MSoffice\Winword and Bshelf94.dot.”

“Setup tried to create an invalid path using C:\MSoffice\Winword and Bsword.hlp.”

If these error messages appear, click **OK**. They do not affect installation.

5. After setup, the program prompts you to restart the computer. Click **Restart Windows**.

When installation is complete, each user must follow the procedure below.

1. Copy Microsoft Office\Templates\Normal.dot to each user’s home directory.
2. Log on to the MetaFrame host and open Word 97.
3. From the **Tools** pull-down menu, select **Options**, **File Locations**, **User Templates**, and change the directory to the user’s home directory.

System Integration

Error Initializing the Visual Basic Environment

Users who do not have administrative rights receive the error message “Error Initializing the Visual Basic Environment” when they try to run the Visual Basic Editor included in Office 97 or when they try to run a macro in an Office program. This error is generated because the user does not have Read permission for the Oleaut32.dll file. Perform the following steps to resolve the problem:

1. Log on as a local administrator.
2. Open Windows NT Explorer.
3. Open the system root directory (C:\%SystemRoot%).
4. Open the System32 directory.
5. Click **Oleaut32.dll**.
6. Under the **Security** menu, select **Permissions**.
7. Add the Everyone group and give it Read permission.
8. Click **OK** and exit Explorer.

Office Startup Icons are not Added to the Startup Group

Office Startup icons are not created in a Common Startup group. So that all users can use the startup programs in Office 97, the icons must be put into a Common Startup group. Add the icons to the Common Startup group as follows:

1. Log on as a local administrator.
2. If a Common Startup group does not exist, click **New** under the **File** menu in Program Manager to create a new group. Select the Common group and name it Startup.
3. At a command prompt, type **change user /install**.
4. Move the selected office startup icons from the Startup group to the Common Startup group.
5. At a command prompt, type **change user /execute**.

The Office Startup programs will now run at startup.

Clip Art Insertion from Client Does Not Work Due to Read-Only Permissions

Office 97 keeps track of clip art used in a file called Artgalry.cag. The Everyone group does not have Write access to this file. To change the permissions on this file:

1. Log onto the console as a local administrator.
2. Open Excel 97.

3. From the **Insert** pull-down menu, select **Object** and then **Microsoft ClipArt Gallery**. Click **Close** to exit ClipArt.
4. In the **Main** menu, click **File Manager**.
5. Locate and highlight the %SystemRoot%\Artgalry.cag file.
6. From the **Security** pull-down menu, select **Permissions**.
7. Highlight the Everyone group.
8. Change the permissions to **Special Access**.
9. Read and Execute permissions should already be selected. Add Write permissions only. The only permissions that should be selected are Read, Write, and Execute.
10. Click **OK** to exit.

Hyperlink Insertion for Users Produces Internet Explorer (IE) Error

Office 97 allows the insertion of hyperlinks into documents or spreadsheets. Clicking on a hyperlink from Internet Explorer automatically opens the browser and loads the target destination. When a user (not an administrator) inserts one of these hyperlinks, the following error message appears: "Error initializing the cache. Shutdown all programs and run scandisk or chkdsk. Delete the Cache, Cookies, and History directories in your Windows directory and then restart IE. If the problem persists, reinstall IE."

This message apppears because the user does not have rights to certain directories accessed by the hyperlink insertion operation. Click **OK** to add the hyperlink to the document or spreadsheet.

To prevent this error from constantly occurring, you can give full control permission to the Everyone group for the following directories:

\%SystemRoot%\Temporary Internet files

\%SystemRoot%\Cookies

\%SystemRoot%\History

Note Use caution when giving users full control permission for these directories.

Remarks

Find Fast builds indexes to speed up finding documents from the Open dialog box in any Microsoft Office program. When Find Fast is installed with Office, it automatically creates an index on each local drive of your computer to cover all of your Office documents. Find Fast indexes are not created on removable drives or read-only media, such as CD-ROM drives. Once created, an index is automatically updated for faster searching.

In the MetaFrame environment, Find Fast runs independently for each user. When Find Fast is triggered, the application uses about 95–100% of the CPU, resulting in unneeded and unwanted load on the system. If Find Fast is triggered by multiple users, the system becomes temporarily unresponsive. Therefore, administrators should consider removing Find Fast from the server.

▶ **To remove FindFast**

1. Log onto the console as an administrator.
2. Right click the **Start** button.
3. From the popup menu, choose **Open All Users**.

   A new window opens titled %SystemRoot%\Profiles\All Users\Start Menu.
4. Double-click the Programs folder.
5. Double-click the Startup folder.
6. Highlight the FindFast shortcut.
7. Press DELETE.
8. Click **OK**.

Microsoft Office 2000

This application note describes how to install Microsoft Office 2000 on a MetaFrame server.

There are four outstanding issues with the installation of Office 2000 at the present time:

- Do not set any features to **Run from Network**, **Run from CD**, or **Installed on First Use**. These settings do not work in a Terminal Server environment
- Set the Outlook features that you want to install to **Run from My Computer**. Set all other features to **Not Available**
- Some features of Outlook 2000 do not work properly in the Windows Terminal Server environment. Please refer to the Microsoft Office Resource Kit Journal Located at the Microsoft Web site. (http://www.microsoft.com/office/ork/2000/journ/OutlTermSrvr.htm)
- By default, Windows Terminal clients do not have write access to the registry on the Terminal Server computer. For more information on this issue, please refer to the Microsoft Office Resource Kit Journal Located at the Microsoft Web site. (http://www.microsoft.com/office/ork/2000/journ/OutlTermSrvr.htm)

Solutions to these problems are presented at the Microsoft Web Sites listed in the above section.

Note Before installing Microsoft Office 2000 on Windows NT 4.0, Terminal Server Edition, Please familiarize yourself with the Microsoft Office Resource Kit Journal Article titled "**Installing Office in a Windows Terminal Server Environment**". This article can be found at the Microsoft Web site. (http://www.microsoft.com/office/ork/2000/Two/30t3.htm)

Software Requirements

- Microsoft Windows NT, Terminal Server Edition with Service Pack 4 or higher
- MetaFrame Version 1.0 or Greater
- Microsoft Office 2000

Installation

▶ **To Install Microsoft Office 2000 on a MetaFrame Server**

1. Logon to the console as a local administrator.
2. At a command prompt, type **change user /install**.
3. Copy the termsrvr.mst transform file from the Office 2000 Resource kit or from the Microsoft Web Site.

   Note The exact location for termsrvr.mst is as follows:

   On the Microsoft Web Site:

   http://www.microsoft.com/office/ork/2000/appndx/toolbox.htm (Download ORKTools.exe). After expansion, termsrvr.mst will be located in \Toolbox\Tools\TERMSRVR

   On the Microsoft Office 2000 Resource Kit:

   <CD-ROM>:\PFILES\ORKTools\Toolbox\Tools\TERMSRVR

4. From a command line, run <cd-rom drive letter>:\Setup.exe TRANSFORMS="<Location of ORKTools>\termsrvr.mst".
5. Proceed with the installation until you reach the license agreement. Accept the terms of this agreement by clicking the "Next" button.
6. If you wish to perform a Normal or Default installation, click the "Install Now" button. Allow the installer to complete the installation and then skip to step 12.
7. If you wish to perform a Custom installation, click the "Custom Install" button.
8. Select the location in which to install Office 2000. (Remember, 453 MB are needed on the installation drive in order to install)
9. Select Microsoft Internet Explorer 5.0 – Standard and click next.

10. Select the applications that you wish to install. By default the recommended applications are selected. Unselected applications or applications that are marked unavailable were marked as such because of compatibility or performance issues. For more information about these applications, refer to the Microsoft Office Resource Kit Journal Article titled "**Installing Office in a Windows Terminal Server Environment**". This article can be found at the Microsoft Web site. (http://www.microsoft.com/office/ork/2000/Two/30t3.htm).
11. After you have chosen which applications to install, click the "Next" button and allow the Microsoft Office 2000 Installer to continue with the installation.
12. You may be asked to reboot the system to complete setup. Click**Restart Windows**.
13. Windows will continue to update and configure Office 2000 after the machine reboots. Once installation is complete, you may want to restart the machine once more to reinitialize the server.

When installation is complete, you can customize Microsoft Office 2000 even further. For more information on how to accomplish this, refer to the Microsoft Office 2000 Resource Kit Journal titled "Installing Office in a Windows Terminal Server Environment". Refer to the section titled "How to Install Office Disc 1 on a Windows Terminal Server". This Document can be located at the Microsoft Web Site (http://www.microsoft.com/office/ork/2000/Two/30t3.htm).

System Integration

Refer to the Microsoft Office 2000 Resource Kit Journal titled "Installing Office in a Windows Terminal Server Environment" for more information on System Integration issues and recommendations. This document can be located at the Microsoft Web Site (http://www.microsoft.com/office/ork/2000/Two/30t3.htm).

Novell GroupWise 5.5

Groupwise 5.5 is Novell's latest version of their groupware software. It is closely linked with NDS and now supports multiple clients and multiple protocol access, including SMTP and POP services and a Web-based GUI client. There are several installation options for GroupWise, including running a post office on a Windows NT server. For simplicity, this document discusses installing GroupWise Domain and Post Office services on a Novell NetWare server, although the directions also apply to post offices running on a Windows NT server. This document is limited to discussing only the Windows 32-bit version of Novell's client software.

Test Configuration

- One NetWare 5.0 server
- One MetaFrame 1.0 server

Software Requirements

- At least one NetWare 4.1x or higher server with GroupWise 5.5 Domain and Post Office services installed
- Windows Terminal Server CD (if Windows Messaging is not installed on the MetaFrame server)
- The GroupWise 5.5 CD

Installation

▶ **To install the GroupWise 5.5 client on a MetaFrame server**

1. At a command prompt, type **Change User /Install**.
2. Install the GroupWise 5.5 CD into the appropriate drive and run Setup.exe from the \Clients\Win32 directory.
3. If the Windows Messaging System files are not installed on your MetaFrame server, you receive the following message:

   "Windows Messaging System is required to run GroupWise 5.5 but is not found on your computer."

   Click **Next** to install the Messaging System (requires Windows Terminal Server CD). The system reboots.

   Important After the system reboots, at a command prompt, type **Change User /Install**.

4. Select the **Standard** installation.
5. Select the location where you want to install GroupWise.
6. Select the components of GroupWise you want to install.
7. Select the group name for the GroupWise application icons.
8. Select the components you want to install into the startup folder. These components are launched at startup for all users.
9. Select the **Language** to install.
10. Click **Next** to begin the file copy process.
11. When the files are copied, exit the installation application without launching it.
12. At a command prompt, type **Change User /Execute** to change the mode back to execute.

Usage

Follow the usage directions in the *GroupWise 5.5 User's Guide*.

Troubleshooting

See “Troubleshooting”in the *GroupWise 5.5 User’s Guide.*

Novell ManageWise Version 2.6

Novell’s ManageWise Version 2.6 was not designed to be a multiuser product. As a result, there are few options for how to install it on MetaFrame except as it is installed for Windows NT. It can be made multiuser by manually pointing the location of the databases that the application uses for storing and retrieving data to a virtual location (like a user’s home directory) so that it is different for each user. If you do decide to do this, you also need to manually copy the database files to that directory for each user, change each user’s Nms.ini file, and then point the two database entries to the virtual directory. This means that more disk space is needed to store each set of databases for each user. Forcing ManageWise to be multiuser is not recommended.

Test Configuration

- MetaFrame Version 1.0 server with Novell’s 32-bit client for Windows NT
- NetWare Version 5 server
- ManageWise Version 2.6

Software Requirements

- NetWare Version 4.1x or higher
- MetaFrame Version 1.0

Installation

▶ **To install ManageWise Version 2.6 on a MetaFrame server**

1. Log on to the MetaFrame server and into the NDS tree as an administrator.
2. On the MetaFrame server, at a command prompt, type**change user /install**.
3. Run Setup.exe from the ManageWise CD-ROM.
4. After navigating through the introductory screens, select the drive letter that is mapped to the SYS: volume of your NetWare server.
5. Add a license and choose the type of installation you want (Custom or Typical).
6. Continue through the summary screen. There is a significant delay in the installation program after the summary screen. Do not reset the computer; installation will continue.
7. Have the installation program update the Autoexec.ncf and Net$log.dat files.
8. Complete the installation and exit Setup.exe.

9. At a command prompt, type **change user /execute**.

Usage

Follow the usage directions in the ManageWise Version 2.6 *User's Guide*.

Troubleshooting

See the Troubleshooting section in the ManageWise Version 2.6 *User's Guide*.

Programmers' Software

Microsoft Visual Basic Version 5.0 Enterprise Edition

Microsoft Visual Basic Version 5.0 allows users to create applications for Microsoft Windows. MetaFrame extends Visual Basic's capabilities by allowing multiple users to concurrently create, modify, and run Visual Basic applications. This document describes a tested method for installing and using Microsoft Visual Basic Version 5.0 Enterprise Edition with MetaFrame.

Software Requirements

- MetaFrame Version 1.0 or later
- Microsoft Visual Basic Version 5.0 Enterprise Edition

Installing Microsoft Visual Basic

1. Log on to the console of the MetaFrame server as an administrator.
2. At a command prompt, type **change user /install** and press ENTER. This places the user session in install mode.
3. Run Setup.exe.
4. In **Name and Organization Information** enter the appropriate information.
5. Enter the installation location.
6. Select the type of installation: **Typical**, **Compact**, or **Custom**. (For this installation, Typical was chosen.)
7. When installation is complete, click **OK** to exit Setup.
8. At a command prompt, type **change user /execute** and press ENTER.
9. Reboot the computer.

Verifying Installation of Microsoft Visual Basic Version 5.0

To verify that Visual Basic 5.0 is correctly installed and configured:

1. In Windows NT, click **Start**, select **Programs**, and click **Visual Basic**.

2. In **New Project**, click **Existing**.
3. In **Directories**, select *x*/Vb/Samples/Pguide/Biblio, where *x* is the directory that Visual Basic was installed in.
4. In **File Name**, double-click **Biblio.vbp**.
5. After the file loads, expand the Forms directory in the upper right side window.
6. Double-click **Form1**.
7. When the form loads, verify that the form can be changed and saved.
8. From a MetaFrame session, verify that a user without administrative rights can repeat Steps 1 through 7.

Note Visual Basic 5.0 must be installed in a directory where users without administrative rights have Change or Full Control permissions. Without these permissions, users cannot create applications that contain databases.

SCSI Monitoring Software

ARK2000

Note This application note was provided by Ark Research Corp., 1190 Saratoga Ave. Suite 110, San Jose, CA 95129-3433.

The purpose of this document is to explain how to install and setup an ARK2000 system within a Citrix WinFrame or MetaFrame environment. An ARK2000 system will allow both local and remote mirroring of the Citrix server's SCSI subsystem. The remote mirror must have a second ARK2000 system in place to receive the commands. The way in which the ARK systems work is by inserting the ARK system in the middle of the SCSI chain and redirecting the SCSI commands to multiple local copies and/or multiple remote copies.

Requirements

In order to utilize the ARK2000 systems, the following requirements must be met:

- Disk(s) requiring to be mirrored must be SCSI. (Either Narrow, Wide, Ultra or LVD).
- Disk(s) being mirrored must be on a separate controller from any other drives that will not be mirrored via the Ark systems.
- Disk(s) must also be accessible externally. (Usually within a separate rack enclosure).
- The Primary drive (drive being mirrored) must be of the same size or smaller than the Secondary drive (drive being mirrored to).

- A separate and dedicated APC Smart UPS and monitor cable. (SMUPS 250 or better.)
- For Wide Area Mirroring, it is highly advisable to utilize T1 lines at 1.54Mb/s or better communication speeds.

Installation (Local Site)

Installation of the ARK2000 is fairly simple as outlined in the following steps. Each will be detailed later.

1. Separate your SCSI drives from the host server (Citrix WinFrame or MetaFrame system).
2. Cable your host server to port 69 or 70 on the ARK2000.
3. Cable your SCSI drives to port 68 or 71 on the ARK2000.
4. If installing a second SCSI channel (for high availability/performance) you will then need to connect the second channel to port 69 or 70 on the ARK2000.
5. If using a second set of SCSI drives (for high availability/performance), you will then need to connect the second set of drives to port 68 or 71 on the ARK2000.
6. If connecting to a remote site for mirroring, you must connect one or both of the Ethernet 10/100 ports to the WAN backbone. (If utilizing less than a 200Mb/s WAN connection, only one Ethernet port is needed.)
7. Connect the APC monitoring cable to the back of the ARK2000 system and the UPS.

Installation (Remote Site)

Installation of the ARK2000 at the remote site is as follows:

1. Connect the remote SCSI drives to port 68 or 71 on the ARK2000 system.
2. Connect a second APC Smart UPS to the ARK2000 system.
3. Connect one or both of the Ethernet 10/100 ports to the WAN backbone.
4. If stand-by host will be utilized at this location, connect the SCSI channel from the host to port 69 or 70 on the ARK2000 system.

Installation Detail

In order for the ARK2000 system to mirror the SCSI drives, the system must be placed in the middle of the SCSI chain between the host server and the SCSI disk subsystem. In order to do this, you must first determine what type and how many SCSI channels are in use and how the SCSI drives are configured (i.e. SCSI ID's and LUN numbers). Appendix A is a worksheet you should fill out completely to help in this setup process.

Note All ARK2000 SCSI ports utilize VHDCI connectors. Once you have determined the SCSI subsystem, you then need to obtain the proper SCSI cables to complete the connections (i.e. VHDCI to HD68 or VHDCI to HD50).

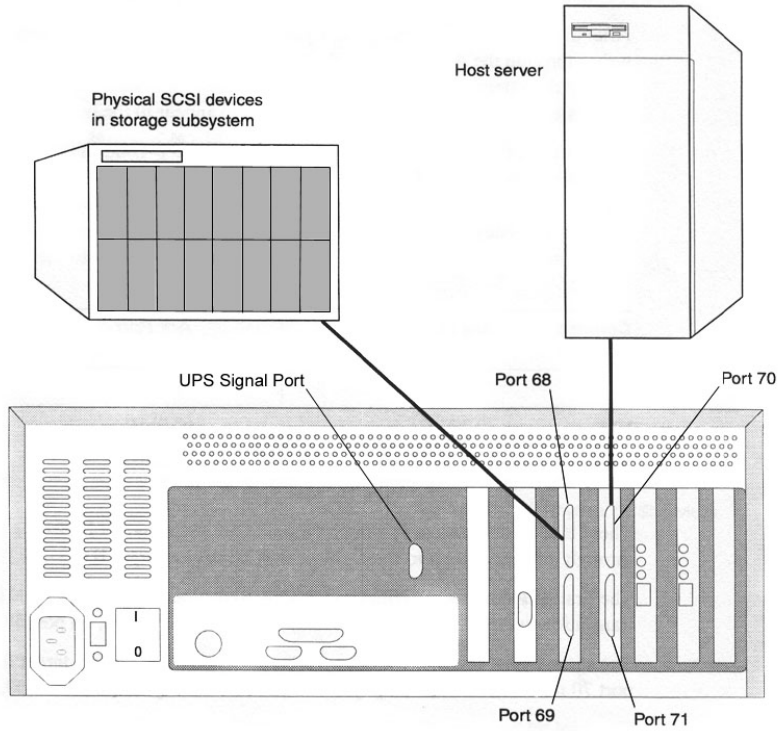


Diagram 1

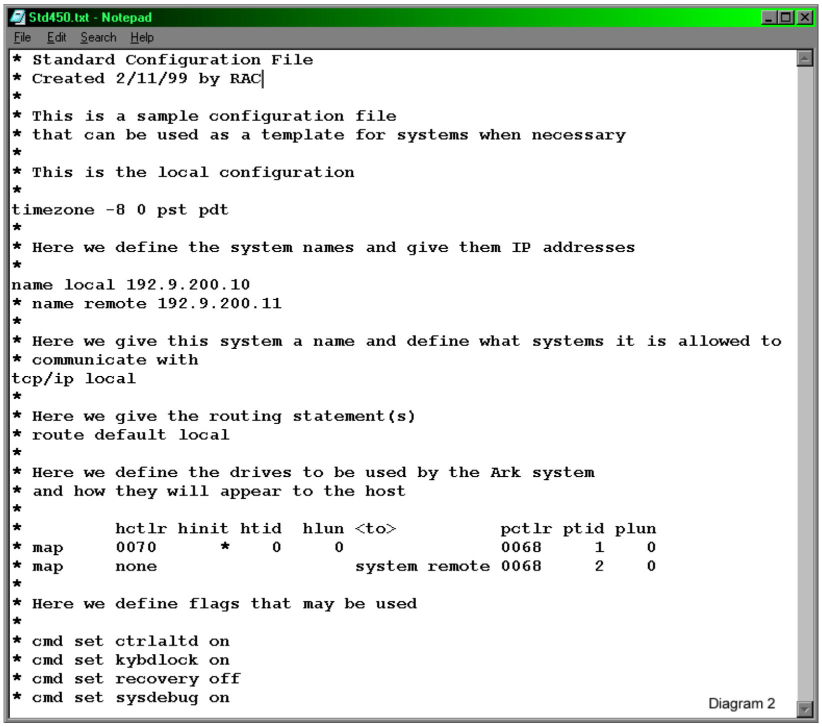
The ARK2000 system has four separate SCSI channels that may be utilized to connect both host systems and SCSI drives to. The ports are 68, 69, 70 and 71; see diag. 1. Again, it is important to note what is connected to each of these ports for the MAP statements later. The ARK system supports a wide range of configurations that are detailed in the *Configuration Planning Guide*, this document only describes a basic configuration with a single primary drive and a single secondary drive. If your config-uration is different, please consult the *Configuration Planning Guide* to help you with your specific configuration. You may also obtain support via email at support@arkres.com.

After configuring the SCSI devices, cable the ARK2000 system to the network backbone. If utilizing a WAN connect-ion for the remote site, a standard 10Base-T or 100Base-T connect-ion from the router to the ARK 2000 is required. If utilizing a LAN for the remote site, a standard 10Base-T or 100Base-T connection from a hub to the ARK2000 is required. A cross-over cable may also be utilized if only connecting between the two ARK systems.

Configuration

Once the Ark System is physically installed, you will then need to configure the Ark system. This is done by creating and editing the CONFIG files on the ARK system. With the ARK systems, you should have received a 3½ inch bootable floppy with system and configuration files on it. You need to edit the configuration file called **STD450.CNF**.

Note If you have Microsoft NetMeeting installed on your system where you are editing these files, I would recommend renaming the file from a command prompt to STD450.TXT to avoid the OS confusing this file with a NetMeeting file. It is also recommended to use a non-proportional font when editing the config files. The files are space delimited and NOT tab delimited (so don't use tabs).



```
* Standard Configuration File
* Created 2/11/99 by RAC
*
* This is a sample configuration file
* that can be used as a template for systems when necessary
*
* This is the local configuration
*
timezone -8 0 pst pdt
*
* Here we define the system names and give them IP addresses
*
name local 192.9.200.10
* name remote 192.9.200.11
*
* Here we give this system a name and define what systems it is allowed to
* communicate with
tcp/ip local
*
* Here we give the routing statement(s)
* route default local
*
* Here we define the drives to be used by the Ark system
* and how they will appear to the host
*
*         hctlr hinit htid  hlun <to>          pctlr ptid plun
* map     0070      *    0     0               0068     1    0
* map     none                   system remote 0068     2    0
*
* Here we define flags that may be used
*
* cmd set ctrlaltd on
* cmd set kybdlock on
* cmd set recovery off
* cmd set sysdebug on
```

Diagram 2

Once you have obtained the config file, you should see something like Diag. 2. Using the worksheet from Appendix A, you will need to change some of the statements within the sample config file to reflect your environment. For this document, We have two local drives connected via SCSI Wide HD68 cables to a single host controller on a Citrix MetaFrame server. We will mirror these to a remote site. Appendix A (Sample) gives the details we will use to walk through this configuration.

When editing the config file, lines with * denote remark statements and do nothing. The first actual line we come to is TIMEZONE, which describes what time zone the ARK system is in. In this example we should have the following:

Local Config

```
timezone -5 0 est edt
```

Remote Config

```
timezone –9 0 pst pdt
```

Next, we need to setup the TCP/IP network and names. From the sample worksheet, we determine the following statements are needed:

- The name statements act like a host file to define systems by name.
- The tcp/ip statement defines first the name of the ARK system utilizing this file and with the keyword netmask defines the network subnet mask and the final parameter specifies which other ARK systems are allowed to communicate with this system.
- The route statement sets up how the ARK system will communicate with system outside of the local IP segment.

Local Config

```
name LOCAL 206.102.20.10
name REMOTE 207.102.20.10

tcp/ip LOCAL netmask 255.255.255.0 REMOTE

route default 206.102.20.1
```

Remote Config

```
name LOCAL 206.102.20.10
name REMOTE 207.102.20.10

tcp/ip REMOTE netmask 255.255.255.0 LOCAL

route default 207.102.20.1
```

Next, we need to setup the drive mappings for the local and remote systems. Again using the worksheet, the following lines are needed:

Local Config

```
map    0070    *    0    0             0068    0    0
map    0070    *    1    0             0068    3    0
map    none              system remote  0068    0    0
map    none              system remote  0068    1    0
```

Remote Config

```
map    none                             0068    0    0
map    none                             0068    1    0
```

Lastly, we need to tell the ARK systems who may access the units from telnet or ftp. To do this we need to add the following statements:

- The cmd statement is used when issuing a command from within the ARK config file and is not required when issuing the command from the command line prompt.
- The defuser statement defines what TCP/IP address may access the ARK system along with the username and password for the user. The ‘a’ suffix denotes what operating modes the user may invoke.

```
cmd defuser 206.102.20.87 user password a
```

Once all these parameters have been added, you should end up with something like this for the local config file:

```
* Standard Configuration File
* Created 2/11/99 by RAC
*
* This is a sample configuration file
* that can be used as a template for systems when necessary
*
* This is the local configuration
timezone -5 0 est edt
*
* Here we define the system names and give them IP addresses
name LOCAL 206.102.20.10
name REMOTE 207.102.20.10
*
* Here we give this system a name and define what systems it is
* allowed to communicate with
tcp/ip LOCAL netmask 255.255.255.0 REMOTE
*
* Here we give the routing statement(s)
route default 206.102.20.1
*
* Here we define the drives to be used by the Ark system
* and how they will appear to the host
*
```

```
*      hctlr hinit htid  hlun        <to>     pctlr ptid plun
map    0070    *    0    0                    0068    0    0
map    0070    *    1    0                    0068    3    0
map    none                    system remote  0068    0    0
map    none                    system remote  0068    1    0
*
cmd defuser 206.102.20.87 user password a
```

After saving these configuration files, they must then be loaded onto the Ark systems. This may be done either by booting the Ark systems from a floppy or by an FTP session to the Ark systems. The simplest way to load the new config files for the first time is to copy the config files to the Ark Tools diskette and then boot from the diskette. This will boot the system into a DR-DOS prompt. From the A:> prompt, type

```
WARKFLCB <name of config file>
```

This will write the config file to the Ark system's flash memory. Once this is done, reboot the system and the configuration should be active. This process needs to be done on all Ark systems. After the initial load of the configurations, any changes or updates to the config files may be accomplished through an FTP session. Simply PUT the config file on the Ark system as CONFIG.0, CONFIG.1, CONFIG.2 or CONFIG.3. To activate a deferent configuration file once the file is uploaded, type the following:

```
CONFIG ACTCONF <NUMBER>
```

Number being the number of the configuration file that you want to activate. After activating a configuration, you must issue a **WARMBOOT** to complete the load of the new configuration.

Establishing Copies

Once the configuration is in place, the last step is to establish the copies of the mirrors. In this example, the following commands would be issued to facilitate the mirroring of the disks.

```
ECOPY 680000 80680000
ECOPY 680100 80680300
```

The parameters for the first ECOPY specify that the disk at port 68, SCSI ID 00 and LUN 00 will be copied to the remote Ark systems disk at port 68, SCSI ID 00 and LUN 00. Similarly, the second ECOPY command specifies that the disk at port 68, SCSI ID 01 and LUN 00 will be copied to the remote Ark system disk at port 68, SCSI ID 03 and LUN 00. If additional drives will be mirrored, separate ECOPY commands must be issued for all copies. After the copies have completed, you are done.

Conclusion

Congratulations! At this point, the Citrix server should see both of the local drives attached to the local Ark system and should be operating normally. Diagram 3 depicts how the system is now configured. Depending on you network bandwidth and the amount of data being written to the drives, some degradation of performance may be noticed. The system is now in a fault tolerant state and if any of the drives fail, the alternate drive will automatically take over and continue to process requests from the Citrix server.

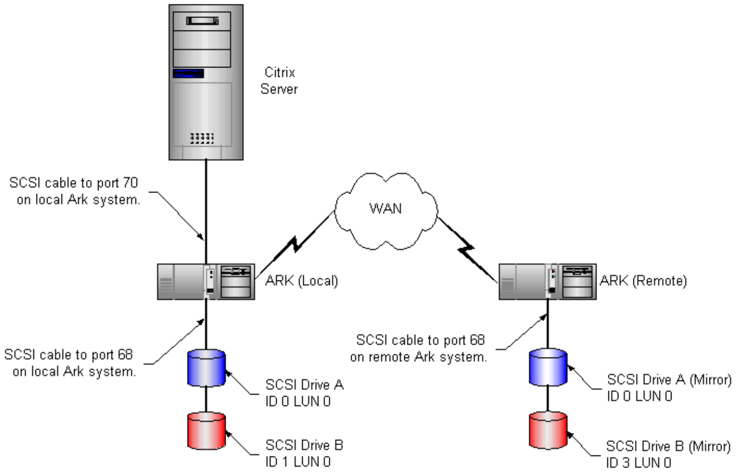

Citrix Server
SCSI cable to port 70 on local Ark system.
WAN
ARK (Local)
ARK (Remote)
SCSI cable to port 68 on local Ark system.
SCSI cable to port 68 on remote Ark system.
SCSI Drive A ID 0 LUN 0
SCSI Drive B ID 1 LUN 0
SCSI Drive A (Mirror) ID 0 LUN 0
SCSI Drive B (Mirror) ID 3 LUN 0

Diagram 3

Appendix A (Sample)

Current Host/Drive Configuration

DRIVE #	Host Channel	SCSI ID	SCSI LUN	SCSI Connection
1	1	0	0	WIDE HD68
2	1	3	0	WIDE HD68

New Configuration with ARK in place

DRIVE #	ARK Host Port	Virtual SCSI ID	Virtual SCSI LUN	ARK Drive Port	Physical ID	Physical LUN
1	70	0	0	68	0	0
2	70	1	0	68	3	0

Remote Site Configuration

DRIVE #	ARK Host Port	Virtual SCSI ID	Virtual SCSI LUN	ARK Drive Port	Physical ID	Physical LUN
1	NONE			68	0	0
2	NONE			68	1	0

Network Configuration

ARK #	NAME	TCP/IP	Mask	Gateway
1	LOCAL	206.102.20.10	255.255.255.0	206.102.20.1
2	REMOTE	207.102.20.10	255.255.255.0	207.102.20.1

Notes

Local system is in New York, and Remote is in California (Time Zones).

Appendix A (Configuration Worksheet)

Current Host/Drive Configuration

DRIVE #	Host Channel	SCSI ID	SCSI LUN	SCSI Connection

New Configuration with ARK in place

DRIVE #	ARK Host Port	Virtual SCSI ID	Virt. SCSI LUN	ARK Drive Port	Physical ID	Physical LUN

Remote Site Configuration

DRIVE #	ARK Host Port	Virtual SCSI ID	Virt. SCSI LUN	ARK Drive Port	Physical ID	Physical LUN

Network Configuration

ARK #	NAME	TCP/IP	Mask	Gateway

Notes

CHAPTER 4

Securing the Enterprise

The third phase of putting a MetaFrame solution into production is to secure your data, applications, and systems from unauthorized use and attack. This chapter provides the following sections to assist you:

- Defining User Rights
- Protecting Against Viruses and Trojan Horses
- Auditing System Activity
- Securing Data and Applications

Defining User Rights

In MetaFrame, Terminal Server, and Windows NT, there are several ways to define and enhance users' workstation environments. You can define network connections, available applications, Windows program groups, and Windows desktop appearance. If you want, you can prevent users from changing the desktop environment you create.

If you need to set up a large number of users who have similar characteristics on a MetaFrame server, it is convenient to create a *user template*. This template can be configured with the desktop configuration, applications, and network drives that the user needs and can then be used as a pattern to create new users when needed.

User Profiles

The most powerful method you have of managing user environments is through *user profiles*. A profile is a file that serves as a snapshot of a user's desktop environment. With profiles, you can also restrict users' ability to change these settings. You can create profiles for users who have domain accounts and store these profiles on servers. Each user can have a single profile with one configuration that is loaded when the user logs on.

You can control what users can and cannot do on their workstations and on the rest of the network in several ways. The most important method, and the one most often utilized, is to use the predefined local groups. Adding a user to one of these groups gives the user a large set of predefined rights and abilities. (For more information on what each predefined local group can do, see “Working With User and Group Accounts” in the Terminal Server *Concepts and Planning Guide.*)

Another way to restrict users’ abilities is by limiting their logon hours and the network computers they are allowed to use.

Permissions on each file, directory, or printer shared on the network define who can and cannot access those resources. You can assign permissions to local groups, global groups, and directly to individual users. It is not recommended that you assign permissions to individual users, however, because this is hard to maintain for large numbers of users.

You can monitor what users do by *auditing* actions and resources. Auditing an action or resource causes an entry to be written to the Event Log whenever that action is performed or that resource is accessed.

Although not recommended, you can directly manipulate *user rights* (also called *rights*) that specify what actions local groups, global groups, and users can perform. Using the predefined local groups and their predetermined sets of rights serves most needs. If you need to grant rights to other groups or users, or fine-tune what rights the predetermined groups have, you have the ability to do so.

Finally, you can also control a user’s desktop environment by assigning the user a *profile*. For more information about profiles, see “Setting Up Users” in the Terminal Server *Administrator’s Guide.*

Granting Access to Anonymous Users

If you use the Terminal Server Security Configuration utility to configure your MetaFrame server for High Security and you want to allow anonymous users access to your system, you must allow Read and Execute permissions to the following list of files for the Anonymous group. You also must specifically allow access to any applications you want to be available for anonymous users. These changes are necessary because anonymous users are not members of the Users group.

%SystemRoot%\System32\Userinit.exe
% SystemRoot %\ System32\Winlogon.exe
% SystemRoot %\ System32\Winsta.dll
% SystemRoot %\ System32\Clib.dll
% SystemRoot %\ System32\Regapi.dll
% SystemRoot %\ System32\Ulmreg.dll
% SystemRoot %\ System32\Ctxsku.dll
% SystemRoot %\ System32\Samlib.dll
% SystemRoot %\ System32\Winspool.drv
% SystemRoot %\ System32\Mpr.dll

Novell NDS for NT

NDS for NT is a Novell product that allows you to manage your Windows NT domain users and groups with the NetWare Administrator tool by replacing the Security Accounts Manager (SAM) DLL files that ship with Windows NT with its own. The installation extends the NDS framework for Windows NT domain users and groups and then redirects the SAM calls to the NDS service. You can then manage the users and groups in a domain from one application, NetWare Administrator. This does **not** prevent you from using the Windows NT User Manager for Domains. Changes made with either tool appear in the NDS framework.

Note NDS for NT is a NetWare 4.1x server based tool, not NetWare 5. Also, the installation of this product removes Microsoft's Client Service for NetWare and replaces it with the IntraNetWare client.

Important Make sure that you do **not** have the Novell Client 32 for NT that comes with NetWare 5 (Version 4.50.819) installed because the installation will not recognize it and will remove it.

Test Configuration

- NetWare Version 4.11 server

  Note You may need to add memory to the NetWare server.

- MetaFrame Version 1.0 server (must be a PDC)
- NDS for NT

Software Requirements

- NetWare Version 4.1x or higher
- MetaFrame Version 1.0

Installation

▶ **To install NDS for NT on a MetaFrame server**

1. At a command prompt, type **change user /install**.
2. From the NDS for NT CD, run Winsetup.exe.
3. Click **Install NDS for NT**.
4. Continue through the information screens and let the install process remove the Microsoft Client Service for NetWare (if it is installed).

5. Reboot the server. Make sure that you log on to the server with the same account that you used when you began the installation.
6. The **Domain Object Welcome** wizard appears after login. Continue past the Welcome screen.
7. Select the NDS tree on which you want to extend the framework.
8. Select the context where you want the domain and its users and groups to reside.
9. The application tries to match as many Windows NT users as it can to NDS users and presents a list to move. Configure which users you want to move and continue.
10. Once the users are moved, installation of the first component is complete. Reboot your MetaFrame server.
11. Once the MetaFrame server reboots, run Winsetup.exe again. Select **Install NDS for NT Administration Utilities**.
12. Select the NetWare server to which you want to install the utilities (this server is in the tree where you extended the framework earlier.) Make sure you install both the NetWare Administrator and the Domain Object Snap-In.
13. Once the installation is complete, choose **RUN NWADMNNT**.
14. When the **IntraNetWare Application Launcher** dialog box appears, select the tree where you installed NDS for NT and then select **Modify**.
15. When the **Application Snap-In** dialog box appears with a message that NDS has been extended successfully, continue with loading NWADMNNT.

Usage

Follow the usage directions in the *NDS for NT User's Guide*.

Troubleshooting

See “Troubleshooting NDS for NT” in the *NDS for NT User’s Guide*.

Protecting Against Viruses and Trojan Horses

It is extremely important to prevent intentional intrusions into your computer network that take the form of viruses and Trojan horses. *Viruses* are programs that attempt to spread from computer to computer and either cause damage (by erasing or corrupting data) or annoy users (by printing messages or altering what is displayed on the screen) on every computer they infect. *Trojan horses* are programs that masquerade as other common programs while they attempt to capture information.

An example of a Trojan horse is a program that masquerades as a system logon screen in an attempt to capture user names and password information, which the writers of the Trojan horse can later use to access the system.

How to Prevent Trojan Horse Attacks

Terminal Server provides an important safeguard against Trojan horse programs. Before you can log onto a Terminal Server computer, you must press the*secure attention sequence*, CTRL+ALT+DEL. This series of keystrokes always directly invokes the Terminal Server operating system logon screen; Trojan horse programs are never activated this way. Users provide only their username and password to the operating system itself. To ensure the effectiveness of this procedure, make sure your users always press CTRL+ALT+DEL or CTRL+F1 in a MetaFrame session before logging on at a computer, even if the logon window is already on the screen.

The secure attention sequence is also required before a user can unlock a locked workstation or change his or her password.

Another way to guard against Trojan horses is to make your applications Read and Execute only so that they cannot be replaced with programs that masquerade as the original program to illegally obtain information.

How to Prevent Virus Outbreaks

Viruses are usually not intentionally introduced to your system. In most cases, users unknowingly introduce a virus into your network when they obtain what they believe to be a useful, safe program from another source, such as an online bulletin board. Many network users are unaware that they can bring viruses into the network this way. Therefore, one of the best ways to keep your network virus-free is by educating your users.

Have at least one commercial virus-detection program in use and regularly check your file servers for viruses. If possible, make virus-detection software available to your users.

Other ways to protect against computer viruses include the following:

- Set file permissions to make all applications available on network servers and workstations Read and Execute only, preventing them from being replaced by viruses. (For more information about this procedure, see the Terminal Server *Administrator's Guide*.)
- Before putting a new application or file on the network, put it on a computer not attached to the network and check it with your virus detection software. Log on to this computer using a Guest account so that the program being examined cannot modify any important files.

- Regularly use a Windows NT-compatible virus scanner. Consider using the **at** command to periodically run the virus scanning program; for example, late at night when no users are logged on.
- **NEVER LEAVE A DISKETTE IN THE DISKETTE DRIVE OF YOUR SERVER**. If the system is rebooted (for example, because of a power failure), the system may attempt to boot from diskette and become infected.
- Regularly back up the files on your file servers (and workstations, if possible) so that damage is minimized if a virus attack does occur.

Auditing System Activity

You can specify that an audit entry be written to the Event Log whenever certain actions are performed or files are accessed. The audit entry shows the action performed, the user who performed it, and the date and time of the action. You can audit both successful and failed attempts at actions, so the audit trail can show both who actually performed actions on the network and who tried to perform actions that are not permitted.

Note Event Viewer log entries for logon events now include the computer name where the logon attempt originated.

The following table lists the categories of events you can choose to audit and what events are covered by each category. For each of the categories listed below, you can choose whether to audit only successful actions in that category, failed attempts to perform actions in that category, both, or neither.

Category	**Events**
Logon and Logoff	Logon attempts, logoff attempts, and the creating and breaking of network connections to servers.
File and Object Access	Accesses a directory or a file set for auditing in Windows NT Explorer; uses of a printer managed by the computer.
Use Of User Rights	Successful uses of user rights and failed attempts to use rights not assigned to users.
User and Group Management	Creation, deletion, and modification of user and group accounts.
Security Policy Changes	Granting or revoking user rights to users and groups, and establishing and breaking trust relationships with other domains.
Restart, Shutdown, and System	Shutting down and restarting the computer, filling up the audit log, and discarding audit entries if the audit log is already full.
Process Tracking	Starting and stopping processes on the computer.

You specify what types of system events are audited through User Manager. You specify what files are audited and how (provided you have used User Manager to turn on the auditing of file accesses) through Windows NT Explorer.

The following table shows the types of directory and file accesses you can audit.

Directory access	**File access**
Displaying names of files in the directory	Displaying the file's data
Displaying directory attributes	Displaying file attributes
Changing directory attributes	Displaying the file's owner and permissions
Creating subdirectories and files	Changing the file
Going to the directory's subdirectories	Changing file attributes
Displaying the directory's owner and permissions	Running the file
Deleting the directory	Deleting the file
Changing directory permissions	Changing the file's permissions
Changing directory ownership	Changing the file's ownership

The Auditlog Utility

The Auditlog utility is used to generate reports of logon/logoff activity for a MetaFrame server based on the Terminal Server security Event Log. To use Auditlog, logon/logoff accounting must be enabled.

Syntax

Auditlog [*username*|*session*] [/before:*mm/dd/yy*] [/after:*mm/dd/yy*]
[/write:*filename* | [/time | /fail
| /all | /detail]] [/eventlog:*filename*]

Auditlog [/clear[:*filename*]]

Auditlog [/?]

Parameters

username
Generates a report of logon/logoff activity for the specified *username*.

Session
Generates a report of logon/logoff activity for the specified *session*.

/before:*mm/dd/yy*
Reports on logon/logoff activity only before *mm/dd/yy*.

/after:mm/dd/yy
Reports on logon/logoff activity only after *mm/dd/yy*.

/write:*filename*
Specifies the name of an output file. Creates a comma-delimited file that can be imported into an application such as a spreadsheet to produce custom reports or statistics.

/time
Generates a report of logon/logoff activity for each user, displaying logon/logoff times and total time logged on. Useful for gathering usage statistics by user.

/fail
Generates a report of failed logon/logoff attempts.

/all
Generates a report of all logon/logoff activity.

/detail
Generates a detailed report of logon/logoff activity.

/eventlog:*filename*
Specifies the name of a backup security event log to use as input to Auditlog. Create a backup security log from the Event Log Viewer or with the Auditlog/Clear:*filename* utility, which saves the current event log in*filename* and clears the event log.

/clear[:*filename*]]
Closes the current logon/logoff log file, optionally saves it as*filename*, and opens a new log file.

/? (help)
Displays the syntax for the utility and information about the utility's options.

Remarks

Auditlog gives the administrator a powerful tool to verify and maintain system security and correct usage. The information can be extracted as reports or as comma-delimited files that can be used as input to other programs.

You must enable logon/logoff accounting in order to collect the information used by Auditlog. To enable logon/logoff accounting:

1. Log on as an administrator and start User Manager.
2. In User Manager, select **Audit** from the **Policies** pull-down menu and check the **Logon Success** and **Failure** boxes.
3. Click **OK** to save your changes.

You can use the **at** command to set up an automatic procedure that runs Auditlog periodically.

Securing Data and Applications

SecureICA Services

Citrix SecureICA Services enhances the security of ICA connections by allowing users to access Citrix MetaFrame servers over secure communications channels. This section provides details on the SecureICA encryption software.

SecureICA Features

Citrix SecureICA contains features to enhance the security of data communication across any type of connection supported by ICA. SecureICA Services uses the RC5 encryption algorithm from RSA Data Security, Inc. The Citrix server and ICA Client use the Diffie-Hellman key agreement algorithm with a 1024-bit key to generate RC5 keys.

SecureICA Services offers the following features:

- 128-bit encryption during user authentication

  To ensure account security, SecureICA uses 128-bit encryption during the authentication phase.

- Strong session encryption and flexible encryption support

  The 128-bit encryption level is considered virtually impossible to break with current technology. The 40-bit and 56-bit encryption levels require a significant investment in time and money to break with a brute force attack. The availability of 40-bit encryption for global use provides an international data encryption solution.

- Per-connection encryption support

  Different encryption levels can be used for each connection. For example, a dial-up connection with 40-bit encryption and a LAN connection with 128-bit encryption can be used simultaneously.

- Cross client compatibility

  SecureICA Clients are available for DOS, Win16, Win32, and the ICA Web Client Netscape Plug-in and Internet Explorer ActiveX control.

- Enforceable encryption levels

  The Citrix server administrator can enforce minimum encryption levels on a per-connection and per-user (*WINFRAME* only) basis. ICA Client connections are allowed only if the ICA Client is using at least the minimum level.

- Dynamic key generation

  The SecureICA server and client generate unique RC5 keys for each connection. A system service periodically generates new Diffie-Hellman parameters in the background, providing for an enhanced level of security.

Understanding Encryption

Encryption is the process of obscuring the true meaning of a message such that only the intended recipient can understand it.

The encryption process transforms data into a form that is unreadable to anyone without a special piece of information. This information allows the recipient to unscramble or decrypt the message. This piece of information is called a key.

The process used to create the scrambled message is called an *encryption algorithm*.

There are two general types of encryption algorithms. A symmetric key algorithm uses the same key to encrypt and decrypt the scrambled data. This means the secret key must never be revealed to anyone but the intended recipient of the data. The advantage of a symmetric key algorithm is its speed.

The disadvantage of a symmetric key algorithm is that the secret key used to encrypt the data must be sent to whoever needs to decrypt the data. If there was a secure channel to transmit the key, the data could be sent the same way and encryption would be unnecessary.

The second type of algorithm is a public-private key algorithm. It relies on certain mathematical properties to create a set of keys, such that one key can only encrypt data and the other key can only decrypt the data. The encrypt-only key is called a public key. The decrypt-only key is called a private key. A message encrypted with the public key can only be decrypted by the private key.

The public key can be openly transmitted without compromising the security of the encrypted data. Knowing the public key does not allow anyone to decrypt the encrypted data.

Many modern encryption programs combine the two types of algorithms. A symmetric key algorithm encrypts the data. The secret key is exchanged using a public-private key algorithm. This provides for the speed of a symmetric key algorithm with the security of a public-private key algorithm.

RC5 is a symmetric key algorithm. The Diffie-Hellman key agreement algorithm is a public-private key algorithm.

Understanding Government Export Restrictions

The United States government restricts the export of strong cryptography. Encryption strength is usually defined by the size of the keys used to encrypt and decrypt data.

Encryption products using keys greater than 56 bits are usually restricted from export. However, larger keys can be exported for use in authentication products.

SecureICA Services comes in two versions: North American and Global. The North American version of SecureICA Services uses a 128-bit key during user logon. A selectable 40-, 56-, or 128-bit key is used to encrypt the remainder of the session. The Global version uses a 128-bit key during user logon. A 56-bit key is used to encrypt the remainder of the session.

United States export policy regarding encryption has been known to allow for export of stronger data keys to subsidiaries of North American based financial institutions. The export of these stronger keys is controlled on a per-application basis and must be applied for.

Third-Party Security Products

This section contains detailed installation and integration information for the following third-party security devices:

- Security Dynamics ACE/Server Software
- VTCP/SECURE Software

These security devices are placed between a COM port on the MetaFrame server and the modem for that COM port. They control remote access to the MetaFrame server through proprietary access control hardware and software. The remote user dials in to the modem attached to the security device and obtains access to the MetaFrame server by successfully completing an authentication dialog with the security device. Once the user has been authenticated, the security device is transparent to the user.

Several general configuration issues are encountered when using third-party security devices:

- For the MetaFrame server to properly detect when a connection is made or broken, the security device must supply modem signals that can be used by the MetaFrame server to detect when a connection is made or terminated. This varies depending on the security device.
- The client PC and the client software may need to be configured to operate properly with the security device. Some security systems require software or hardware on the client PC.
- The MetaFrame server and the security device itself must be secured from unauthorized tampering. It is recommended that you place all hardware in a secured room to prevent unauthorized personnel from acquiring access to the equipment.
- Most third-party security devices secure remote Dial-In users (or local, directly connected asynchronous users) only. You need to consider how to secure your system from improper access by LAN- or WAN-connected users.

The third-party security devices discussed in this section control remote access to the MetaFrame server through proprietary access control software. Details on access control hardware are available through the individual hardware manufacturers. The software access control devices most often used are based on one of two premisses.

The first method is based on secondary user authentication. In addition to the Primary Windows Authentication, the access control software adds another layer of authentication based on separate user databases. This software control method decreases the likelihood of compromised passwords.

The next method of software access control is based on encrypting data transmissions. In this case, the access control software provides a layer of authentication and then encypts all data packets between the client and server. This software control method prevents eavesdropping on unsecure phone lines or networks.

The access control software listed in this chapter implements one of these two methods to provide security and access control.

Security Dynamics ACE/Server

The Security Dynamics ACE/Server security software provides SecurID identification and authentication of users on TCP/IP networks. There are two pieces to the ACE/Server security software program: the ACE/Server Host and the ACE/Client for Windows NT. The ACE/Server host software operates on Windows Terminal Server and on a wide variety of UNIX-based platforms, while the ACE/Client for Windows NT runs on a MetaFrame server. When used in conjunction with a SecurID token, ACE/Server centrally authenticates a user’s identity, allowing only authorized users access to protected network resources.

Note The Security Dynamics ACE/Server uses the Progress database. This database does not function on multiprocessor machines.

The ACE/Server is a secondary security solution that supplements Terminal Server’s own base security. This additional security can be configured for remote control logins (sessions) and remote access logins (RAS). The ACE/Server acts as a database storing PIN tokens for authenticating users logging onto a MetaFrame server. The ACE/Client is installed on the MetaFrame server and is integrated into the session and RAS logins. Upon login to the MetaFrame server, the user is challenged by both MetaFrame security and SecurID passcode security.

Requirements

The ACE/Server host software operates on Terminal Server and a wide variety of UNIX platforms. This note describes only the configuration tested in the Citrix labs.

Security Dynamics SecurID

ACE/Server Windows NT 4.0 Version

Hardware Requirements

- See Basic Hardware Requirements of Windows NT Version 4.0
- CD-ROM drive

Software Requirements

- Windows NT Server, Terminal Server Edition with Service Pack 3
- Security Dynamics ACE/Server for Windows NT Version 3.01
- Security Dynamics ACE/Client for Windows NT Version 4.0 or higher
- NTFS File System

ACE/Server UNIX Solaris Version

Hardware Requirements

- Sun SPARCstation with CD-ROM drive and 4mm DAT tape

Software Requirements

- Solaris Version 2.5 (UNIX Operating System)
- Progress Software Database Version 7.3C01 with patch 7.3C05
- Security Dynamics ACE/Server Version 2.1
- Security Dynamics ACE/Client for Windows NT Version 4.0 or higher

Citrix MetaFrame

Hardware Requirements

- MetaFrame server

Software Requirements

- MetaFrame Version 1.0 (see "MetaFrame Server Configuration" later in this section)

Integration Overview

The steps to install ACE/Server on a Terminal Server are:

1. Install Terminal Server with Service Pack 3.
2. Install and configure the ACE/Server.
3. Configure a MetaFrame server (detailed below).
4. Install and configure the ACE/Client for Windows NT on the MetaFrame server (detailed below).

Follow the steps below to install ACE/Server on a Solaris UNIX platform.

1. Install the Solaris UNIX Operating System.
2. Install the Progress Database.
3. Install and configure the ACE/Server.
4. Configure a MetaFrame server (detailed below).
5. Install and configure the ACE/Client for Windows NT on the MetaFrame server (detailed below).

MetaFrame Server Configuration

For detailed information regarding MetaFrame server equipment selection and software installation, see the Citrix MetaFrame documentation.

1. Install MetaFrame following the instructions in the Citrix documentation.

Notes The TCP/IP protocol must be installed on the MetaFrame server in order to communicate with the ACE/Server installed on the Sun SPARCstation.

For asynchronous modem connections, the MetaFrame server must have an intelligent multiport board, such as a Digi International, installed and configured.

For remote node connections, RAS must be installed on the Terminal Server. (Remote MetaFrame ICA Dial-In connections do not use RAS.)

2. Reboot the server.

Installing ACE/Client for Windows NT on a MetaFrame Server

1. Obtain a copy of the Sdconf.rec file and place it in the %SystemRoot% \System32 directory on the Installation server. This allows you to set security options and test the installation without having to reboot beforehand.
2. Make sure that the Installation server is configured as a client machine in the ACE/Server database. If this is the first authentication for this MetaFrame server, verify that the **Sent Node Secret** checkbox is unchecked.
3. If the ACE/Client for Windows NT was installed on the MetaFrame server but was reconfigured; that is, the IP address has changed, be sure to delete the Node Secret file. This file, Secureid, is stored in the %SystemRoot%\System32 directory.
4. Insert the ACE/Client for Windows NT diskette in the floppy drive of the MetaFrame server and proceed with the installation as described in the ACE/Client documentation. The ACE/Client can be configured to support remote control connections, remote node connections, or both.

5. When prompted to set security options, do so. For remote control users, select **Enable Local Access Security** on the **Local** tab. You can verify that a user can authenticate by selecting **Test Authentication with ACE/Server** at the top of the window. Authentication problems occur here if the MetaFrame server is not configured as a client in the ACE/Server database, if the Sdconf.rec file is outdated, or if the Securid (Node secret) file is outdated.
6. If you intend to use RAS as a connectivity option on the MetaFrame server, select **Enable Remote Access Security**. This option is disabled if the RAS server has not been installed yet.

Note You may want to have the ACE/Server authenticate everyone who connects through RAS. This is done by selecting **Challenge All Users** on the **Local** tab.

7. After configuring security options, the installation asks whether you want to add users to the Security Dynamics user groups that have been created (see "Usage" later in this section for more details on these groups). Click **Yes** to start the MetaFrame User Manager and create users to add to these groups, as well as to add existing users. Users configured as such are required to provide SecurID authentication.
8. Upon completion of the installation, reboot the MetaFrame server.

Note If the ACE/Client is already installed, the above configuration is accomplished with the Control Panel applet for the ACE/Client.

Connectivity Matrix

The connectivity matrix below identifies currently supported configurations for using the SecurID product and MetaFrame client programs for various operating systems and protocols.

Client operating system	ICA Client	Protocol	Session*	RAS**
DOS	DOS	IPX	X	X
		NetBIOS	X	
		TCP/IP	X	X
		Async null modem	X	
		Async Dial-In	X	
Windows 3.x	Win16	IPX	X	X
		NetBIOS	X	
		TCP/IP	X	X
		Async null modem	X	

Client operating system	ICA Client	Protocol	Session*	RAS**
		Async Dial-In	X	
Windows 95/NT	Win32	IPX	X	X
		NetBIOS	X	X
		TCP/IP	X	X
		Async null modem	X	
		Async Dial-In	X	

*Session connections are remote control connections made using the Citrix ICA Client Independent Computing Architecture (ICA) protocol.

**RAS connections are remote node connections made using the Citrix MetaFrame Dialup Manager for DOS, MetaFrame Dialup Manager for Windows, Windows 95 Dialup Networking, or Remote Access Dialout for Windows NT in conjunction with RAS configured on the MetaFrame server.

Usage

Remote Control Connections

1. Select a configuration from the connectivity matrix above and set up a supported client configuration. (For instructions on installing and configuring a connection with a MetaFrame client, please see the Citrix MetaFrame documentation.
2. Initiate a connection to the MetaFrame server using one of the supported protocols. The standard MetaFrame login screen appears.
3. Log on to the MetaFrame server. If the user specified belongs to the local user group Sdlocal or domain Sdlocal (see “PDC Installations” below), the user is required to provide a SecurID authentication passcode.
4. Respond to the SecurID challenge with a passcode from a SecurID token card.

Bypassing Authentication on a Per-Session Basis

Terminal Server contains a fix that allows the administrator to configure sessions to bypass SecurID logon authentication (not RAS authentication) on a per-session basis. If the user is a member of the Sdlocal group or the server is configured to challenge all users, the user is not challenged. To bypass SecurID authentication for a session:

1. Start Terminal Server Connection Configuration.
2. Select a session.
3. Select **Advanced Session**.
4. Check the **Use Default Authentication** box and click **OK** to save the changes.

Remote Node Connections

1. Configure a machine as specified in the above configuration matrix. Dial into a Terminal Server RAS port. Be sure that the client software is configured to display Terminal mode after dialup. This step is essential or you cannot login. Each user configured in the Sdremote or domain Sdremote user groups is prompted for the *domain*, *username*, and *password*.
2. Upon successful authentication, your *username* and *password* are taken from the RAS client's configuration and verified by the network as with a normal RAS login.

Note Your RAS/Terminal Server log on *username* and your ACE/Server name must be identical.

Primary Domain Controller (PDC) Installations

If the ACE/Client software is installed on a MetaFrame server that is also a primary domain controller (PDC), two additional groups are created during the installation: domain Sdremote and domain Sdlocal. These two groups are used to allow users on any machine that uses the PDC to be authenticated using the SecurID solution.

Note This does not change the requirement that any machine that wants to use SecurID authentication, whether local or domain, must have the ACE/Client installed.

Two example configurations are shown below:

Example 1

An ICA Client, using RAS, connects to the MetaFrame server Server_1 in the domain PDC_EX and the user specified is a member of PDC_EX's domain Sdremote user group. The user is challenged with the SecurID authentication.

Note In this example, both Server_1 and PDC_EX must have the ACE/Client installed.

Example 2

An ICA Client, using ICA remote control, connects to the MetaFrame server named Server_2 and logs into domain PDC_EX2. The user is a member of PDC_EX2's domain Sdlocal group. The user is challenged with the secondary authentication.

Note Both Server_2 and PDC_EX2 must have the ACE/Client installed.

Troubleshooting

When I try to connect to the MetaFrame server using RAS, it drops the connection whenever it tries to verify the username and password on the network.

Do not forget to turn on the terminal mode after dialin option on the RAS client side. This option is essential or you will not be prompted by the SecurID authentication.

When I try to log on to the MetaFrame server using a RAS or session connection, I get a "User access denied" message. The ACE/Server log shows the message "Node verification failed."

There are two possible causes. First, check to see if the client configuration on the ACE/Server has the **Sent Node Secret** box checked. If it does, uncheck it. Next, on the MetaFrame server, look in the %SystemRoot%\System32 directory. If the file Securid exists, delete it. Try to *log on* again. If you still get the failure, delete the Sdconf.rec file from the %SystemRoot%\System32 directory and obtain a current copy from the ACE/Server.

When I try to start Sdadmin on the ACE/Server, I get a "user root not found" message even though I have a root user on the server.

This should only happen on the first login after installation, if ever, and it means that the database is not yet ready to be administered. Run Sdcreadm on the ACE/Server and then try again.

I am trying to get a user to authenticate but the token is not being accepted. I tried to resynchronize the card in the database but that gives an Invalid tokencode error message.

The database is not receiving a value in the range of values that it will accept. Typically, this means that the time zone or the date and time configured on the ACE/Server are not correct. Check the date and time that the ACE/Server reports in the **System, Edit System Parameters** menu. If the time shown there is not correct, make the appropriate adjustments to either the Timezone variable (Start\Control Panel\Date+Time icon) or to the date and time (using the **Date** command).

I have dialup or network users who do not have SecurID cards. How can they connect without being challenged by the ACE/Server?

As an administrator, run Terminal Server Connection Configuration and edit a session. Click **Advanced Session**. Check the **Use Default Authentication** box and click **OK** to save the change.

During installation, I get an "Operating system not supported" error when I run Sdsetup and Sdnewdb.

The documentation provided with the ACE/Server includes a Readme stating that certain operating systems (including newer versions of Solaris) are not included in the installation scripts. It also includes directions for editing those scripts (Sdsetup and Sdnewdb) to make them support those operating systems. Follow the instructions in the ACE/Server documentation.

Windows NT ACE/Server Installation

1. Log on to the Terminal Server console as the local administrator.
2. Run Setup.exe from the ACE/Server\Acesvr\NT_I386 directory on the CD.
3. Place the Security Dynamics license diskette in drive A and click **Next**.
4. Select **Master ACE/Server** and click **Next**.
5. Enter the destination directory where you want to install the master ACE/Server.
6. A window opens asking you whether to install Progress 4GL. Click **Yes**.
7. Proceed with the Progress installation following the Progress Installation Documents provided by Security Dynamics.
8. Install prompts you to reboot. Click **Will Restart System Later**.
5. From Control Panel, click **ACE/Server**, and then **Automatic ACE/Server** startup. Click **OK**.
6. Configure the console display for 800x600 or better video resolution. This minimum display size is necessary for viewing the entire ACE/Server configuration menu. The display can be changed using the **Display** option in Control Panel.
7. Reboot the system.

Windows NT ACE/Server Configuration

1. Log on to the Terminal Server console as the local group administrator.
2. Copy the Sdconf.rec file from the \ACE\Data directory to the %SystemRoot% \System32 directory.
3. Run the ACE/Server Administration program.

Note If an error appears stating the configuration record Computername does not match the host computer name Computername.fdn (Full Domain Name), it may be necessary to edit the %SystemRoot%\Ssystem32\drivers\etc\hosts file and add the IP address of the master server along with the FDN of the server. Double-click the Aceserver configuration icon and enter the FDN name in the **Master Server** section. If you do make modifications, you must copy the Sdconf.rec file and run Server Administration again.

4. From the **Tokens** menu, select **Import** and import the token file(s) you intend to use for this integration.

5. Select **Site** and then **Add**. This is a container for machines you intend to use from this location. It is a client machine management tool, not a physical separation.
6. Add a group. A group is a way to easily associate a selection of client machines with a selection of users. Any user who is designated as a member of a group can log on and get authenticated by any machine also contained in that group.
7. Add one client entry for each machine that will use the SecurID secondary authentication. Each machine's IP address must be resolvable by the server, whether by DNS, NIS, or simply the %SystemRoot%\System32\drivers \etc\hosts file. The machine's type is dependent on the operating system. For Terminal Server and MetaFrame machines, it is NetOS. Be sure to add the clients to the group created above.
8. Add a user entry for each user who will use SecurID authentication. The default shell variable is not relevant for users who will log on from Terminal Server and MetaFrame hosts but is required for users who will login from a UNIX client. Be sure to add the users to the group configured in Step 4 above; all can login from any client configured in that group.

Solaris Installation

Installation of the Solaris operating system is detailed in the documentation provided by Sun Microsystems; however, some general steps are listed below.

1. Place the Solaris installation CD in the CD-ROM drive and turn on the computer. If a previous installation of Solaris or SunOS exists on the machine, interrupt the boot process (with STOP+A), specify **N** for new command mode, and type **boot cdrom**.
2. From this point on, you are in the Solaris installation procedure. The three parts of the installation procedure are: Machine Identification, Software Installation, and Post Installation. The following questions are important to ensure that both Progress and ACE/Server function correctly:

   Machine Identification

Question	Answer
Networked	Yes
Specify Time Zone By	Offset from GMT

   Install Software

Question	Answer
Software Group	<-Entire Distribution

   Be sure to specify a valid root password.

3. When the installation is complete, make the following modification:

   cd /etc
   vi system (or use whatever editor you like)
   and add the following lines to the end of the file:

   ```
   Set SEMSYS:SEMINFO_SEMMNI = 64
   Set SEMSYS:SEMINFO_SEMMNS = 200
   Set SEMSYS:SEMINFO_SEMMNU = 100
   Set SEMSYS:SEMINFO_SEMMSL = 50
   Set SHMSYS:SHMINFO_SHMMAX = 16777216
   Set SHMSYS:SHMINFO_SHMMNI = 100
   Set SHMSYS:SHMINFO_SHMSEG = 16
   ```

4. The Timezone, as set up by the default installation, will not work correctly with the ACE/Server's reliance on GMT (UTC) time. Change the /Etc/Default/Init file to match your particular time zone configuration. In the Eastern US, the TZ field in that file should be changed to EST5EDT4; this indicates Eastern Standard Time, with an offset from UTC of five hours, and Eastern Daylight Time with an offset from UTC of four hours.

5. Modify the /Etc/Services file to include the two lines for the ACE services. They are as follows:

   ```
   securid        5500/udp       # ACE/Server
   securidprop    5510/tcp       # ACE/Server Slave
   ```

Progress Database Installation

Installation of the Progress Database is detailed in the documentation provided by Security Dynamics; however, some general steps are listed below.

1. Log on as root user to the Solaris machine. Insert the Progress Database 4mm DAT into the tape reader. From the console, execute these commands:

   cd /mnt
   cpio -iudcvBm < /dev/rmt/0m
   /proinst

2. Enter the product license Serial Numbers, Reference Numbers, and Control Numbers from the product license addendum sheet that come with the database package. When done, press CTRL+E.

3. Specify the installation directory and let the installation continue. When asked if you want to copy scripts, answer **N** or **No**.

4. Install the patch for the Progress Database. Insert the Progress Patch DAT tape and execute these commands:

   md temp
   cd temp
   tar -xv

Note The process takes several minutes.

5. Follow directions in the Readme.pro file created by the previous command. Use this file to create a shell script (batch file) that updates everything in one command.

Solaris ACE/Server Installation

Installation of the ACE/Server is detailed in the documentation provided by Security Dynamics; however, some general steps are listed below.

1. Place the ACE/Server tape in the DAT drive. On the drive where you intend to install the ACE/Server, execute these commands:

   ```
   mkdir sds
   cd sds
   tar -xv
   ```

2. Edit the Sdsetup and Sdnewdb files to modify the versions of Solaris that are supported.
3. Execute \Sdsetup and follow the installation instructions, answering the questions asked as they apply to your system and configuration.

Solaris ACE/Server Configuration

Configuration of the ACE/Server is detailed in the documentation provided by Security Dynamics; however, some key details are listed below.

1. From the ACE/Server console, start the Sdadmin program.
2. From the **Tokens** menu, select **Import** and import the token file(s) you intend to use for this integration.
3. Select **Site** and then **Add**. This is a container for machines you intend to use from this location. It is a client machine management tool, not a physical separation.
4. Add a group. A group is a way to easily associate a selection of client machines with a selection of users. Any user who is designated as a member of a group can login and get authenticated by any machine also contained in that group.
5. Add one client entry for each machine that will use the SecurID secondary authentication. Each machine's IP address must be resolvable by the server, whether by DNS, NIS, or simply the /Etc/Hosts file. The machine's type is dependent on the operating system. For Terminal Server and MetaFrame machines, it is NetOS. Be sure to add the clients to the group created above.

6. Add a user entry for each user who will use SecurID authentication. The default shell variable is not relevant for users who will log on from Terminal Server and MetaFrame hosts but is required for users who will login from a UNIX client. Be sure to add the users to the group configured in Step 4 above; all can login from any client configured in that group.

VTCP/SECURE Software

Overview

VTCP/SECURE is a security software package that allows remote users to connect to a MetaFrame server over untrusted networks for a secure remote MetaFrame session. This is done by creating a virtual private network that transparently encrypts and validates all data between the Citrix ICA Client and the MetaFrame server.

VTCP/SECURE provides encryption, authentication, and authorization to protect TCP networked computers and incorporates a number of security management features. The encryption, authentication, and key exchange algorithms include DES 40, Triple DES, and Diffie-Hellman. Authentication, authorization, and accounting services are provided through TACACS+ or the internal one-time password authentication service.

Software Requirements

- MetaFrame Server Version 1.0
- VSGATE Server Software Version 2.1a or higher
- VSCLIENT Client Software Version 2.1a or higher
- TCP client WinSock Version 1.1 or higher

Note Client systems require a minimum of 8MB of RAM for VTCP/SECURE and the ICA Client software.

Installation Overview

VTCP/Secure is composed of two parts: the VSCLIENT software that is installed on the client machine and the VSGATE software that is installed on a MetaFrame server or a gateway server to the corporate Intranet. VTCP/SECURE gateways may reside on the UNIX, Windows NT, or Windows 95 operating systems. These gateways allow network connectivity to a MetaFrame server residing on the corporate Intranet. The gateways decrypt data from the remote client for communication on the local Intranet. The VSCLIENT software can reside on Windows operating systems compliant with WinSock 1.1 or higher.

The procedures below describe how to install the VTCP/SECURE gateway software on MetaFrame and how to install and use the VSCLIENT software with Windows 95. In this example, the MetaFrame server itself is directly connected to the Internet without an intervening gateway server. For ICA Client configurations, see the connectivity matrix below. For more detailed information about VTCP/SECURE, see the VTCP/SECURE *Administrators Guide*, the Vamin2.hlp file included with VTCP/SECURE software, or contact Infoexpress, Inc.

Note When connecting any MetaFrame server to an untrusted network, secure your MetaFrame server using the procedures outlined in the MetaFrame documentation.

Quick Start Installation

1. Install the VSGATE software on a MetaFrame server with TCP/IP sessions and Internet networking access.
2. Configure the VSGATE software.
3. Install the VSCLIENT software on a Windows 95 system.
4. Create a VSCLIENT connection entry to the MetaFrame server.
5. Install the MetaFrame Win32 Client.
6. Use the ICA Client Remote Application Manager to create a remote TCP/IP network connection entry.

Quick Start Usage

1. Use Dial-up networking from the Windows 95 client machine to dial into an ISP (Internet Service Provider) for TCP connectivity or use your existing TCP/IP network connection.
2. Run the VTCP/SECURE client software from Windows 95, creating a secure communications channel to the MetaFrame server.
3. Run the ICA Win32 Client Remote Application Manager and connect to the MetaFrame server.

The following matrix lists the possible client operating systems and the recommended ICA Clients to use. The VSCLIENT software for Windows works on all of the listed operating systems over TCP/IP remote node dial up or network TCP/IP client connections only. Direct ICA dialin and other network protocols are not supported by VTCP/SECURE software.

Client operating system	ICA Client
Windows 3.1 (with WinSock 1.1 or higher)	ICA 16-bit client for Windows
Windows for Workgroups (with WinSock 1.1 or higher)	ICA 16-bit client for Windows
Windows 95	ICA 32-bit client for Windows

Client operating system	ICA Client
Windows NT 3.51 or 4.0	ICA 32-bit client for Windows

Installation

VSGATE Software

1. Log on to the MetaFrame server as an administrator.
2. At a command prompt, type **change user /install**.
3. Install the VSGATE software.
4. During the VSGATE software installation, select to install the software as a service and enter the TCP/IP subnet mask of the MetaFrame server.
5. Reboot the MetaFrame server.
6. Log on to the MetaFrame server as an administrator.
7. Run Vsadmin from the VSGATE program group.
8. From the Vsadmin program, select **5** to manage local passwords.
9. Select **1** to add a user.
10. Enter the new username.
11. Select the default settings except for the Access Filter settings.
12. Select **1** for Netops for Access Filter settings.
13. Save the configuration.

VSCLIENT Software

1. On a Windows 95 client, install the VTCP/SECURE software.
2. During the VSCLIENT installation, select **System Wide**.
3. Reboot the Windows 95 client.

Usage

1. From the Windows 95 client machine, dial into the ISP for Internet access using Windows 95 Dial-up Networking or if avaible use an existing TCP/IP network connection.
2. Select the VSCLIENT application from the VSCLIENT program group.
3. Click **Connect**.
4. Enter the name or IP address of the MetaFrame server and click **OK**. (Leave the port address empty.)
5. Once communication to the VSGATE server is established, you are prompted for the VTCP/SECURE *username* and *password* you created in Vsadmin. With proper authentication, a “Smart Tunnel” or virtual private network is created between the remote client and the MetaFrame server.

6. Run the ICA Win32 Client Remote Application Manager and create an entry to connect over TCP/IP to the MetaFrame server.
7. Double-click the new entry to establish a secure TCP/IP network connection to the MetaFrame server.

CHAPTER 5

Connecting to the Web

If you are publishing applications for end-users who connect to your Citrix servers over the Internet or your organization's Intranet, the next phase of deploying your solution is to set up Citrix Web Computing. This chapter provides the following information to assist you:

- An introduction to Citrix Web Computing
- Requirements for supported Web browsers for Citrix Web Computing
- Requirements for supported Web servers for Citrix Web Computing
- A sample procedure for setting up Citrix Web Computing

An Introduction to Citrix Web Computing

Citrix Web Computing consists of four components:

- **Web server**. The Web server software can run on the Citrix server or on a separate computer. The only step needed to enable the Web server for Citrix Web Computing is to register ICA as an application MIME type. Any Web server that supports application MIME types can be used.

  One important distinction that sets Citrix Web Computing apart from the CGI and Microsoft Active Server Pages models is that the Web server does not execute any additional software to support Citrix Web Computing. The Web server contains ICA files that are downloaded to the Web browser for processing by the ICA Web Client.

- **Citrix server**. To the Citrix server, an ICA connection from a Web client is no different than a connection from any other ICA Client. The same security and user configuration guidelines used for published applications apply to Web Computing.

  By default, the ICA connections created during Setup support an unlimited number of connections. See your Terminal Server documentation for instructions on limiting the number of concurrent users.

Fifteen anonymous user accounts are created automatically during installation. There must be sufficient user accounts to support the expected number of concurrent users. If necessary, use User Manager for Domains to manually create additional user accounts.

- **Citrix ICA Web Client**. The ICA Windows Web Clients work with any Web browser that supports configurable MIME types. The Citrix ActiveX control for Internet Explorer and Plug-in for Netscape Navigator and Netscape Communicator allow these Web browsers to display ICA sessions embedded in Web pages.

  When a user clicks a hyperlink to an ICA file or loads an HTML page containing an embedded ICA session, the Web browser passes the ICA file to the ICA Web Client, which then initiates a session on the Citrix server using the information contained in the ICA file and the application definition. Video, keyboard, and mouse data are passed between the session on the Citrix server and the ICA Web Client using the Citrix ICA protocol.

- **ICA file**. ICA files are text files containing a series of command tags. These tags define the attributes of the session to be launched on a Citrix server. The Web browser downloads the ICA file and passes it to the ICA Web Client, which then initiates the ICA session on the Citrix server.

  You can use either Published Application Manager or the ICA File Editor to create ICA files.

  For more information about Citrix Web Computing and the ICA Windows Web Clients, see the *Citrix ICA Client Administrator's Guide* for the Windows Web Clients.

Web Browsers for Citrix Web Computing

Microsoft Internet Explorer Version 3.02 for Windows NT

Microsoft Internet Explorer Version 3.02 is a World Wide Web browser for HTML documents on the Internet and on Intranets. Internet Explorer combines Web exploration and FTP capabilities into one integrated package.

Requirements

Hardware Requirements

- Internet connection (modem, Ethernet card, ISDN, etc.)

Software Requirements

- Microsoft Internet Explorer Version 3.02 for Windows NT
- MetaFrame Version 1.0 or higher with TCP/IP support installed

▶ **To install Microsoft Internet Explorer Version 3.02 on a MetaFrame server**

Note Do not install both Internet Explorer 3.x and Internet Explorer 4.0 on the MetaFrame server. Because Internet Explorer 3.x and 4.0 share DLLs, you can run only one version on the server.

1. Log on to the MetaFrame server as an administrator.
2. At a command prompt, type **change user /install**. This places the user session in install mode.
3. Install Internet Explorer following the directions in the *Microsoft Internet Explorer Installation Guide*.
4. When installation is complete, at a command prompt, type **change user /execute**. This changes the user session back to execute mode.

Configuration

To run Internet Explorer on a MetaFrame server, you must install TCP/IP support. To install TCP/IP support:

1. In Control Panel, double-click **Network**.

   The **Network Settings** dialog box appears.
2. Select the **Protocols** tab and click **Add**.
3. Choose **TCP/IP Protocol** from the pull-down list and click **OK**.

   The DHCP Configuration dialog box appears. If there is a Dynamic Host Configuration Protocol (DHCP) server on your internetwork, click **OK** to enable automatic DHCP configuration.
4. Reboot the MetaFrame server to start TCP/IP support.

Multiuser Configuration

By default, Internet Explorer 3.x stores the user’s History, Cookies, and temporary Internet files in the %SystemRoot% directory. Because this directory is read-only for normal users, they cannot run Internet Explorer.

To customize Internet Explorer for any user, run the %SystemRoot%\Application Compatibility Scripts\Install\MSIE30.cmd script and installing Internet Explorer.

Microsoft Internet Explorer Version 4.0 for Windows NT

Microsoft Internet Explorer Version 4.0 is a World Wide Web browser with an integrated set of tools for every type of user, from basic services like e-mail to conferencing, broadcasting, and Web-authoring capabilities.

Requirements

Hardware Requirements

- Internet connection (modem, Ethernet card, ISDN, etc.)

Software Requirements

- Microsoft Internet Explorer Version 4.0 for Windows NT
- MetaFrame Version 1.0 or higher with TCP/IP support installed

▶ **To install Microsoft Internet Explorer Version 4.0 on a MetaFrame server**

Note Do not install both Internet Explorer 3.x and Internet Explorer 4.0 on the MetaFrame server. Because Internet Explorer 3.x and 4.0 share DLLs, you can run only one version on the server.

Active Desktop is currently not supported.

1. Log on to the MetaFrame server as an administrator.
2. At a command prompt, type **change user /install**. This places the user session in install mode.
3. Install Internet Explorer selecting the browser-only or standard installation. The full installation is currently not supported.
4. When installation is complete, at a command prompt, type **change user /execute**. This changes the user session back to execute mode.

Configuration

To run Microsoft Internet Explorer 4.0 on a MetaFrame server, you must install TCP/IP support. See the *Microsoft Terminal Server Installation Guide* for additional information.

Multiuser Configuration

After installing Internet Explorer, run the %SystemRoot%\Application Compatibility Scripts\Install\MSIE40.cmd script. This script moves the ActiveMovie shortcut into the all-users Accessories folder and ensures that each user has a unique download directory.

Netscape Navigator Version 3.04, 32-bit Version

Netscape Navigator Version 3.04 is a multimedia World Wide Web browser for HTML documents on the Internet and on Intranets. Navigator integrates Web exploration, e-mail, news groups, chat, and FTP capabilities. There is platform support for live on-line applications. Navigator supports Live Objects, frames, Java applets, and Netscape inline plug-ins.

Requirements

Hardware Requirements

- Internet connection (modem, Ethernet card, ISDN)

Software Requirements

- Netscape Navigator Version 3.04, 32-bit Version
- MetaFrame Version 1.0 or higher with TCP/IP support installed

Installation

1. At a command prompt, type **change user /install** and press ENTER.
2. Install Netscape Navigator following the directions in the Netscape documentation.
3. At a command prompt, type **change user /execute** and press ENTER.

Configuration

To run Netscape Navigator on a MetaFrame server, you must install TCP/IP support. See the Microsoft Terminal Server documentation for details.

Multiuser Configuration

By default, Navigator creates the Start menu shortcuts in the current user's Start menu instead of the All Users Start menu. Also, the Bookmark file, Cache, Cookies, History, News and Security directories are stored in %SystemRoot%. Because this directory is read-only for normal users, they cannot run Navigator.

To customize Navigator for any user, run the %SystemRoot%\Application Compatibility Scripts\Install\NetNav30.cmd script after installing Navigator.

Netscape Communicator Version 4.05, 32-bit Version

Netscape Communicator Version 4.05 is a World Wide Web browser designed for corporate users with support for calendars, mainframe access, and centralized management of Communicator. It combines Netscape Navigator with a suite of Internet tools for mail, news and discussion group access, online conferencing, Web page creation, and instant messaging.

Requirements

Hardware Requirements

- Internet connection (modem, Ethernet card, ISDN)

Software Requirements

- Netscape Communicator Version 4.05, 32-bit Version
- MetaFrame Version 1.0 or higher with TCP/IP support installed

Installation

1. At a command prompt, type **change user /install** and press ENTER.
2. Install Netscape Communicator following the directions in the Netscape documentation.
3. At a command prompt, type **change user /execute** and press ENTER.

Configuration

To run Netscape Communicator on a MetaFrame server, you must install TCP/IP support. See the Microsoft Terminal Server documentation for details.

Multiuser Configuration

Netscape Communicator supports multiple user configurations, However, it does not provide a method to automatically install these user configurations. It is recommended that you create a single “default” configuration targeting the user’s home drive. This prevents Communicator from presenting users with a list of configurations and eliminates the need for users to configure their own setting.

After installing Communicator, run the Netscape User Profile Manager. Create a single profile named Default. When prompted for the profile path, use %rootdrive%:NS40. Leave all name and e-mail name entries blank. If any other profiles exist, delete them.

After you complete these steps, run the %SystemRoot%\Application Compatibility Scripts\Install\NetCom40.cmd script. This script ensures that the default profile is copied to each user’s directory the first time the user logs on.

Web Servers for Citrix Web Computing

MetaFrame supports any Web server that supports application MIME types. Procedures for doing this vary by Web server. The Web server software can run on the same computer as MetaFrame or on a separate server. The following Web servers are several of those supported by MetaFrame.

Microsoft Internet Information Server Version 3.0

Microsoft Internet Information Server (IIS) Version 3.0 is an integrated Web server with Windows NT Server, Terminal Server Edition. It is a complete solution for creating and managing Web sites on the Internet or an Intranet. IIS uses the same directory, security model, and file permissions as all other Windows NT server network services.

Software Requirements

- Microsoft Internet Information Server Version 3.0
- MetaFrame Version 1.0 or higher with TCP/IP support installed

▶ **To install Microsoft Internet Information Server on a MetaFrame server**

1. Log on to the MetaFrame server as an administrator.
2. At a command prompt, type **change user /install**. This places the user session in install mode.
3. Install the Internet Information Server following the directions in the Microsoft documentation.
4. When installation is complete, at a command prompt, type **change user /execute**. This changes the user session back to execute mode.

Configuration

To run Internet Information Server on a MetaFrame server, you must install TCP/IP support. To install TCP/IP support:

1. In Control Panel, double-click **Network**.

   The **Network Settings** dialog box appears.
2. Select the **Protocols** tab and click **Add**.
3. Choose **TCP/IP Protocol** from the pull-down list and click **OK**.

   The **DHCP Configuration** dialog box appears. If there is a Dynamic Host Configuration Protocol server on your internetwork, click OK to enable automatic DHCP configuration.
4. Reboot the MetaFrame server to start TCP/IP support.

\

Registering the ICA MIME Type

1. Stop IIS if it is currently running.
   A. Click **Start** and point to **Programs**.
   B. Point to the Microsoft Internet Server folder and then click Internet Service Manager. The Internet Service Manager starts.
   C. Right click the icon for the WWW service and then click **Stop**. Repeat for the FTP and Gopher services.
2. From the **Start** menu, click **Run**.
3. Type **regedt32** and click **OK**.
4. In the Registry Editor, select the following key:

   \\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\InetInfo\Parameters\MIMEMap
5. On the **Edit** menu, click **Add Value**.
6. Enter the following values:

   ```
   Value Name      application/x-ica,ica,,5
   Data Type       REG_SZ
   ```

   Click **OK** when finished.

   Note The commas in the Value Name are important and must be entered exactly as shown. REG_SZ is the default data type and can be left alone. You do not need to specify a value for the string; the presence of the registry variable is the relevant information.
7. Exit Registry Editor. Restart IIS.

Netscape FastTrack Server Version 3.01 for Windows NT

Netscape FastTrack Server Version 3.01 is an entry level Web server that lets users create and manage a Web site. It is a complete solution for creating and managing Web sites on the Internet or an Intranet. The FastTrack Server includes the Netscape Communicator client software for creating, editing, and publishing documents.

▶ **To install the Netscape FastTrack Server on a MetaFrame server**

1. Log on to the MetaFrame server as an administrator.
2. At a command prompt, type **change user /install**. This places the user session in install mode.
3. Install Netscape FastTrack Server following the directions in the readme file.

4. When installation is complete, at a command prompt, type **change user /execute**. This changes the user session back to execute mode.

Configuration

To use the Netscape FastTrack on a MetaFrame server, you must install TCP/IP support. To install TCP/IP support:

1. In Control Panel, double-click **Network**.

   The **Network Settings** dialog box appears.
2. Select the **Protocols** tab and click **Add**.
3. Choose **TCP/IP Protocol** from the pull-down list and click **OK**.

   The DHCP configuration dialog box appears. If there is a Dynamic Host Configuration Protocol server on your internetwork, click **OK** to enable automatic DHCP configuration.
4. Reboot the MetaFrame server to start TCP/IP support.

Registering the ICA MIME Type

1. Edit the following four files:
   - *path*\bin\admserve\cfgstuff\MIME.types
   - *path*\bin\httpd\install\misc\MIME.types
   - *path*\admserve\httpd-*servername*\MIME.types
   - *path*\httpd-*servername*\MIME.types

   where *path* is the directory containing the Netscape FastTrack Server and *servername* is the name of the FastTrack Server.
2. Add the following line to the end of each file:

```
type=application/x-ica exts=ica
```

Sample Procedure for Setting Up Web Computing

Here is a sample procedure for setting up a seamless connection to a MetaFrame server, using:

- MetaFrame Version 1.8
- Microsoft's Internet Explorer 3.x or 4.x Web Browser

For more detailed instructions on setting up Citrix Web Computing, see the *Citrix ICA Client Administrator's Guide* for the ICA Windows Web Clients.

▶ To publish an application

The first step in this procedure is to publish an application. Publishing an application allows you to start an application without knowing any details of the application's location, executable name, or server name.

1. Open Published Application Manager.
2. From the **Application** menu, click **New**.
3. Enter the application name and a detailed description; click **Next**.
4. Select whether the application will be started explicitly or anonymously and then click **Next**.
5. Click **Browse** to locate the executable file for the application and click **Next**.
6. Specify the Window properties for the application and click **Next**.
7. Specify the default settings for Program Neighborhood clients when users connect to this application. Click **Next**.
8. Select how the application will appear on Citrix clients that have Program Neighborhood user interface and click **Next**.
9. Highlight the groups and users that are allowed to run the application and click **Add**. When they are selected, click **Next**.
10. Highlight the server(s) that will be configured to run the application and click **Add**. When finished, click **Next**.
11. Click **Finish**.

▶ To create an ICA file

The next step in this procedure is to create an ICA file. An ICA file is a plain text file that contains the parameters necessary to define an ICA session.

1. Open Published Application Manager.
2. Highlight the Published Application you just created and from the **Application** menu, click **Write ICA File**.
3. Select the level of assistance you require and click **Next**.
4. Select the size and color attributes you want displayed when connecting to the application by the ICA file and click **Next**.
5. Select the desired encryption level for the ICA session. For anything other than Basic, the client and the server must have SecureICA installed. Click **Next**.
6. Click **Browse** to specify the path and a name for the ICA file and click **Save**. The file name and path should automatically be entered into the **File Name** dialog box. Click **Next**.
7. Specify **no** when asked to Create an HTML template for this application.
8. Click **Finish**.

The following sample .ica file runs an application maya-notepad residing on machine MAYA after establishing a RAS connection.

```
[WFClient]
Version=2
TcpBrowserAddress=128.1.1.11
TcpBrowserAddress2=128.1.1.81

[ApplicationServers]
maya-notepad=

[maya-notepad]
Address=maya-notepad
InitialProgram=#maya-notepad
DesiredHRES=640DesiredVRES=480DesiredColor=2
TransportDriver=TCP/IP
WinStationDriver=ICA 3.0
The first section is the WFClient connection.
```

```
[WFClient]Version=2TcpBrowserAddress=128.1.1.11TcpBrowserAddress2=128.1.
1.81
```

The TcpBrowserAddress is the IP address of a server on the network where access to the application is available. This could also include an IPX address or NetBIOS address if those protocols are used instead of IP.

The second section is the Application Servers section

```
[ApplicationServers]maya-notepad=
```

The Application Servers section indicates the published application to which you will be connected.

The section that describes the application appears as follows. The address is the published application name or the specific address of the server. If a specific address is used, load balancing is not employed. Think of it in the way that an asynchronous connection differs from a RAS connection. This comes into play when moving a connection across the Internet and the proper firewall ports are not opened on the routers in between. The initial program name is the published application to which you will be connecting; if this is left blank, a desktop is defaulted. The transport driver indicates the transport protocol you will be using. The desired resolution is indicated; if a screen percent is present, it overrides the resolution indicated. The desired color refers to the number of colors, 16 colors=1, 256 colors=2.

```
[maya-notepad]Address=maya-notepad
InitialProgram=#maya-notepad
TransportDriver=TCP/IP
WinStationDriver=ICA 3.0
```

```
DesiredHRES=640DesiredVRES=480DesiredColor=2
```

▶ To enable the client

Now that everything is prepared on the server side, you must copy the files you will need from the MetaFrame CD to a folder on the client's hard drive.

1. Search the contents of the MetaFrame CD for the WFICA32.exe file.
2. Copy the file to the local hard drive.

From the user desktop, create a new shortcut to reflect the WFICA32.exe file appended with the name of the ICA file that you created; for example, c:\wfica32 maya-notepad.ica.

▶ To enable the browser

The final step is to enable the browser to act as your dialer without actually invoking the browser.

1. From the user's desktop, right click on the Internet Explorer icon and select **Properties**.
2. Select the **Connections** tab. In Internet Explorer 4.x, select **Connect to Internet Using a Modem**. Click **Settings**. Choose the **DUN** connection you use to establish your connection to your ISP and deselect **Disconnect if Idle for More than xx Minutes**. Click **OK** twice to close Internet Properties.

   For Internet Explorer 3.x, select the **Connection** tab. Select **Connect to Internet as Needed**. Select the **DUN** connection you use to establish your connection to your ISP and deselect **Disconnect if Idle for More than xx Minutes**. Click **OK** twice to close Internet Properties.

▶ To test the connection

To test your connection, double-click the WFICA32 icon. This invokes the dial-up connection and prompts you to enter your password. When you enter your password, your connection is established to the Citrix system and your published application starts.

CHAPTER 6

Maintaining MetaFrame

Once you have deployed and configured your MetaFrame servers and ICA Clients, you have to maintain your systems. This chapter includes information to assist you with:

- Monitoring network activity and performance
- Applying service packs and hotfixes

Monitoring Network Activity and Performance

This section discusses tools that track network activity and performance. These tools: Event Viewer, Network Monitor, and Performance Monitor, display three types of information, respectively:

- Event logs that record errors, security audits, and other significant events for problem diagnosis
- Network traffic statistics that indicate such things as network utilization, total frames received per second, and broadcast frames received per second
- Performance statistics that indicate such things as queue activity, processor utilization, memory usage, and server throughput

Event Viewer

Terminal Server keeps a record of errors, logon activities, and other significant events that happen on computers. These records are stored in event logs that can be examined with the Event Viewer. Typical log entries include such items as the failure of a device driver, a data error from a network card, or an unsuccessful logon.

Every Terminal Server computer has three logs in which events are recorded: system, security, and application.

The following table describes each event log.

Event log	Description	Event selection process
System	Errors, warnings, or information generated by the MetaFrame server.	Selection of events is preset by the operating system.
Security	Valid and invalid logon attempts and events related to resource use such as creating, opening, or deleting files or other objects.	Control of security event auditing is set in the Policies menu of User Manager. Control of file and directory access audits is set through Windows NT Explorer.
Application	Errors, warnings, or information generated by application software, such as an electronic mail or database program.	Application developers decide which events to monitor.

System and application logs are available to be viewed by all users, while security logs are accessible only to system administrators. With appropriate administrative rights, you can also view logs on other computers.

Using Event Logs to Troubleshoot

Each entry in an event log can include the following information: Date, Time, Source, Type, Category, Event ID, User, and Computer name. In addition, most events generate a text description and sometimes binary data, which are available by double-clicking on a single entry or choosing **Details** in the **View** menu. The binary data is generated by the application that was the source of the event record. Because the data appears in hexadecimal format, interpreting it may require consulting someone who is familiar with the source application. Binary data is displayed in words or in bytes.

Careful monitoring of event logs can help you predict and identify the sources of system problems. For example, if log warnings show that a disk driver can only read or write to a sector after several retries, it indicates that the sector will eventually become corrupt. Log files can also confirm problems with application software. If an application crashes, an application event log provides a record of activity leading up to the event for support personnel to analyze.

Here are some suggestions to help you diagnose problems using event logs:

- Archive logs in log format. The binary data associated with an event is discarded if you archive data in text or comma-delimited format.
- If you suspect a hardware component is the origin of system problems, filter the system log to show events generated only by that component.

- If a particular event seems related to system problems, try searching the event log for other instances of the same event or to judge the frequency of an error.
- Note Event IDs. These are unique numbers that match a text description in a source message file. This number are used by product support representatives to understand what occurred in the system.

Using Event Logs to Analyze Activity

Using spreadsheet or word-processing programs, you can manipulate event log data saved as text to produce graphs, charts, and reports. Graphs generated from event logs are used to show the times when logon activity is highest, the average time between network failures, and so on.

Reading event logs into other applications requires saving them in text or comma-delimited text format. This type of archive discards binary data associated with an event but saves all other log details.

Network Monitor

Network Monitor can be used to capture and display frames (also called *packets*) to detect and troubleshoot problems on the network. The Network Monitor is not installed by default when Terminal Server is installed.

To install Network Monitor and the Network Monitor Agent:

1. In Control Panel, double-click **Network**.
2. From the **Network** dialog box, select the **Services** tab.
3. Select **Network Monitor Tools** and **Agent**.

You can now start Network Monitor from Administrative Tools or from a command prompt.

ICA packets use TCP port 0x5D6 or 1494 using decimal notation. It can be recognized in Network Monitor by looking for the 5D6 in either the **Source Port** or **Destination Port** address. A display filter can be set on the **Source and Destination** port to show only 0x5D6 packets in Network Monitor.

Note Network Monitor is not the only place to get information about ICA traffic. If you have connection problems, use MetaFrame Administration to monitor the ICA connection status while a user attempts to log on.

ICA packets are encrypted. If an analysis of a trace is necessary to troubleshoot a problem between the MetaFrame server and an ICA Client, save the capture data to a file. Send this capture data to support personnel if the problem cannot be resolved.

Performance Monitor

The hardware and software configuration used with a MetaFrame server has a large effect on system performance as measured by user response time. The most useful tool in tuning a MetaFrame server is Performance Monitor. Performance Monitor is a graphical tool that collects and examines data concerned with system activity. The overall performance of a MetaFrame server can be examined by monitoring the following areas:

- Processor(s)
- Memory
- Hard Disk(s)
- Network

System throughput problems usually occur when demand for one of these resources exceeds the supply. The available resources in this case are the microprocessor(s), memory, hard disk(s), and networking hardware and software. Finding out how user applications interact with each of these resources is a logical first step when you start monitoring.

When monitoring a system, you are really monitoring the behavior of its objects. In MetaFrame, an object is a standard mechanism for identifying and using a system resource. Objects are created to represent individual processes, sections of shared memory, and physical devices. Performance Monitor groups counters by object type. A unique set of counters exists for the processor, memory, cache, hard disk, users, processes, and other object types that produce statistical information. Certain object types and their respective counters are present on all systems. However, other counters, such as transport-protocol counters, only appear if the computer is running the associated software.

Each object type can have several instances. For example, the Processor object type will have multiple instances if a system has multiple processors. The PhysicalDisk object type has two instances if a system has two disks. Some object types, such as Memory and Server, do not have instances. If an object type has multiple instances, each instance produces the same set of statistics (counter information).

Solving Performance Problems

The following sections describe potential bottlenecks that can affect system performance and discuss how to use Performance Monitor to determine if any of these areas are adversely affecting system performance.

Processor(s)

The processor-related factors that can affect performance on a MetaFrame server include:

- Processor utilization
- Interrupts
- Context switches
- Screen savers

Processor Utilization

If processor utilization is over 90% on a regular basis, consider upgrading the processors in the MetaFrame server. You could install a faster processor if this is a single-processor system, or install additional processors or faster processors in a multiprocessor system. Many server-class systems are designed to allow the inclusion of additional processors or processor boards. MetaFrame scales linearly as processors are added, subject to performance constraints from other system resources such as memory. To determine CPU utilization, monitor the %Processor Time counter under the Processor object. The %Processor Time shows the percentage of elapsed time that a processor is busy executing non-idle threads. If the %Processor Time counter consistently registers at or near 100%, the processors might be slowing the system response time down. If 100% processor utilization is consistent, check the processor queue length for excessiveness.

Interrupts

A defective device adapter can cause an excessive number of interrupts. This severely degrades the performance of the system because most of the processor time is spent handling interrupts. A moderately busy server (32-bit hard disk adapter, network card, and about 12 users) will experience an average of about 100 interrupts per second. If the number of interrupts per second increases dramatically without a corresponding increase in system activity, it could indicate a hardware problem. To determine if there is excessive interrupt activity, monitor the Interrupts/sec counter under the Processor object.

Context Switches

Device drivers perform context switches to switch between user and system level processing. A poorly-written device driver can cause the system to make a large amount of context switches. A typical value for context switches is 500 per second or fewer. If the number of context switches per second is greater than 500, a device driver may have built-in critical sections that are too long. If the number of context switches is not too high, the server can be taken off-line and a DOS-based diagnostic program such as CheckIt or QA Plus can be run to pinpoint the malfunctioning driver. To check the server for poorly written device drivers, monitor the Context Switches/Second counter under the System object.

Screen Savers

Screen savers, especially “busy” ones, can use a large amount of processor resources and, in the case of an ICA connection, network bandwidth. If you plan to use a screen saver, use a generic one and test it on the system before you implement it.

To determine if a screen saver is using too much processing time, run the screen saver on the console. Log on to an ICA Client and run Performance Monitor. Monitor the %Processor Time counter under the Processor object. Note the demand that the screen saver puts on the processor.

Memory

The factors related to system memory that can affect performance on a MetaFrame server include:

- Memory load
- The system page file, PAGEFILE.SYS
- Memory paging

Memory Load

To determine how much memory is present on the MetaFrame server, use Windows NT Diagnostics. To use Windows NT Diagnostics to determine system memory:

1. In the Administrative Tools group, click the **Windows NT Diagnostics** icon. The **Windows NT Diagnostics** menu appears.
2. Select **Memory**. The window that appears contains information about system memory. The **Memory Load Index** field at the bottom of this dialog box shows current memory load. If this value is consistently high, increase the amount of system memory.

Pagefile.sys

Terminal Server preallocates hard disk space for virtual memory. This area is marked as a file called Pagefile.sys. In Terminal Server, the default pagefile size is 1.5 times the amount of physical memory. This value is determined during system installation. The MetaFrame server can exceed the default size space if it is determined that more memory is needed. However, this is time consuming and can slow down the system.

Use Performance Monitor to monitor the demands on the pagefile. Check the Commit Limit and the Committed Bytes counters under the Memory object to determine how the pagefile is performing. When the Committed Bytes counter exceeds the Commit Limit, increase the size of the pagefile as follows:

1. In Control Panel, double-click **System**.

2. Click the **Performance** tab and click **Change** in the **Virtual Memory** section.
3. In the **Paging File Size for Selected Drive** section, enter new Initial and Maximum sizes. Click **Set** and then click **OK**.
4. Click **OK** to exit.

Determine the optimum pagefile size by logging Committed Bytes over a period of two weeks with Performance Monitor. Record the maximum value over the two week period. Increase this number by 10 to 20% to determine the system's minimum pagefile size.

Memory Paging

Terminal Server keeps the most used data in physical memory and pages the least accessed data out to the pagefile. When a system is heavily loaded, memory is paged in and out at a rapid rate. This affects system performance if the hardware is unable to keep up with the server. The number of pages per second being paged in and out of memory is a valuable indicator of hardware performance. The pages per second should consistently average five or less per hard drive. If the pages per second is constantly above five, the system is paging in and out of virtual memory too much. Either use faster hard disks so the system can access virtual memory quicker or add more RAM to the machine.

Note All configured connections consume system memory, whether active or inactive. To avoid allocating memory for connections that will never be used, be sure to configure only the type and number of connections required for your configuration.

Hard Disk(s)

Citrix does not recommend installing MetaFrame on a RAID drive or using a RAID drive for the MetaFrame swap file. RAID drives have additional overhead that enhances data reliability but can adversely affect operating system performance.

The factors related to hard disk(s) that can affect performance on a MetaFrame server include:

- Percentage of disk time
- Disk queue length

Percentage of Disk Time

The %Disk Time counter measures the percentage of time that a hard disk is active. If the %Disk Time counter value is high, the hard disk is not adequate for the system. Take one or more of the following steps:

1. Use a 32-bit PCI bus mastering SCSI controller or a higher-performance (for example, Wide SCSI or Fast Wide SCSI) subsystem in the MetaFrame server. This speeds up data transfer to and from the drive.
2. Spread the pagefile across multiple drives.
3. Install a separate hard drive and assign only the pagefile to the drive.
4. Install a separate SCSI controller and hard drive and assign only the pagefile to that drive and controller.
5. Offload some of the more frequently accessed data to a less utilized server.
6. Install another server to help handle the user load.

Disk Queue Length

Another item to monitor is the Disk Queue Length counter. This measures the number of I/O requests outstanding for the hard disk. If data has to wait in a long queue before it is written or read from the disk, it can affect the MetaFrame server performance. The Disk Queue Length values should be sustained at no more than 1.5 to 2 times the number of spindles making up the physical disk. Most disks have only one spindle. RAID disks usually have more but appear as only one physical disk to Performance Monitor.

Network

When monitoring network performance, examine the total bytes per second passing to and from the server. Compare this with the speed of the network being used to transfer the data; for example, 10Mbps or 100Mbps Ethernet, or 4Mbps or 16Mbps Token Ring. (Because these values are in bits per second, divide by 8 to get the number of bytes per second; for example 10Mbps Ethernet is actually 1.25MBps.) If the server's total network throughput is close to the network's transfer speed, the network is saturated. Possible solutions are listed below.

Upgrading the Network

- Add a faster network backbone
- Add a router between network segments
- Connect the servers directly to the backbone

Upgrading the Server

- Add a faster network adapter
- Use the latest drivers for the network adapter
- Assign a lower interrupt for the network adapter to give it higher system priority

Monitoring Users and ICA Sessions

MetaFrame supports multiple simultaneous users on a MetaFrame server, logged on to the MetaFrame server from a variety of connections. You can use the Event Viewer to examine events such as user logon and logoff and connection activity. You can use Performance Monitor to track resource consumption by user or connection or diagnose connection problems by examining statistics gathered on a per-user or per-connection basis.

For example, you can monitor the amount of processor time being used to identify potential performance problems. Statistics can be used to find and diagnose connection problems, such as a defective modem or WAN link, by finding connections with excessive error counts.

Virtual Memory

In a multiuser environment like MetaFrame, the demand for memory is higher than in single-user environments. It is, therefore, recommended that the system's pagefile size be increased.

1. In Control Panel, double-click **System**.

   The System Properties dialog box appears.
2. Select the **Performance** tab.
3. Click the **Change** button.

   This opens the **Virtual Memory** dialog box.
4. Set the **Initial Size** and the **Maximum Size** to correspond to the calculated value, which is 2.5 times the size of the system RAM. For example, if you have 256MB of RAM, set the Initial and Maximum Sizes to 640MB.

Note Setting both the Initial Size and the Maximum Size to the same size provides the best performance because the MetaFrame server does not take extra time increasing the paging file.

Spreading the pagefile across all available drives improves the performance of your MetaFrame server because the MetaFrame server can perform Read and Write operations to more than one disk simultaneously.

Third-Party Technologies for Prioritizing ICA Traffic

In busy network environments, here are two solutions for ensuring that ICA packets are prioritized and routed properly:

- Cisco Queuing Technologies
- Packeteer (PacketShaper)

Cisco Queuing Technologies in a Citrix Environment

For organizations using Cisco routers, a method exists for prioritizing the ICA protocol when routing over low bandwidth links such as a serial connection. Cisco offers two methodologies for prioritizing the ICA protocol. These methodologies, Priority Queuing and Custom Queuing, relate to ICA traffic prioritization over ports 1494 and 1604.

Note Routing is critical for large enterprise networks to function properly. Only qualified personnel who are well versed with Cisco technologies should perform router configuration.

Requirements

Software Requirements

- MetaFrame Version 1.0 or later

  - Or -

- *WINFRAME* Version 1.7 with Service Pack 5B or later

Hardware Requirements

- MetaFrame and/or *WINFRAME* servers
- Cisco Router

Usage

Using Cisco routers, ICA traffic can be prioritized by two distinct methods: Priority Queuing and Custom Queuing. The following sections define and describe these methods in detail. They also provide the necessary commands required as input at the router command interpreter. These sections assume that the user is knowledgeable in using Cisco routers and has the proper authorization to make such changes. All commands in these sections are given to the router from the privileged level of the EXEC command interpreter.

Priority Queuing

Priority Queuing allows the administrator to set up a priority on a particular protocol or port number. Anytime a buffer of that protocol or port number is transmitted, it is given high, medium, or low priority.

However, by using this method other protocols can be limited if there is significant priority traffic running through the router. For example, during periods of intense prioritized ICA traffic, there would not be sufficient network bandwidth for an FTP session or non-ICA print job.

The steps required to set up a priority queue are listed below:

1. At the Router # command prompt, type **config terminal**. This places the system in configuration mode.
2. Configure a priority list (1-16) and name the IP protocol as the one to prioritize. Specify the transport layer protocol and port number (TCP 1494) to be prioritized. At the Router#(config) prompt, type:

   priority-list 1 protocol ip high tcp 1494
3. Assign a default level of prioritization. At the Router#(config) prompt, type:

   priority-list 1 default low

   In this case, protocols that do not fall into category 1 default to low priority.
4. Specify the queue sizes. This step is optional. See the Cisco documentation for additional information.
5. Assign the priority list to an interface. This step applies to serial ports, so the command refers to the serial interface (s0). To assign priority 1 to the interface s0, from the Router#(config) prompt, type:

   int s0
   priority-group 1

   To determine if the changes have taken effect, use the show interface s0 or the show queuing command.

Custom Queuing

Custom Queuing provides the ability to set up 16 different queues that act in a round robin format. This is similar to division multiplexing. The router scans process packets through all of the sequences in a round robin format. You set the byte length for a specific queue so that multiple packets from the same protocol are transmitted as opposed to one packet of another protocol. This is considered a better alternative than Priority Queuing. Similar to token ring, everyone gets a chance to transmit data. Only some protocols can transmit more data than the rest.

The steps required to set up Custom Queuing are as follows:

1. At the Router # command prompt, type **config terminal**. This places the system in configuration mode.
2. Set custom queuing filters for protocols or interfaces. At the Router#(config) prompt, type:

   queue-list 1 protocol ip high tcp 1494

   This configures queue list 1 for the IP protocol and the TCP port 1494, which is what ICA uses to initiate a session.

3. Assign a default queue. This specifies the default queue for all unnamed protocols and ports that are not explicitly defined. At the Router#(config) prompt, type:

   queue-list 1 default 2

4. Change queue capacity. This step is optional. See the Cisco documentation for additional information.

5. Configure the transfer rate per queue. This sets the byte count for a particular queue. This allows multiple packets to be sent for one queue while sending one packet for another queue. At the Router#(config) prompt type:

   queue-list 1 queue 1 byte-count 4500

   Queue 1 in queue-list 1 has a byte-count of 4500, which is three times that of a regular Ethernet packet, thereby sending three packets of this queue-list member as opposed to one packet of the default queue.

6. Assign the custom queue list to an interface. This step applies to serial ports so the command refers to the serial interface (s0). The first entry designates the serial interface, while the second assigns custom queue 1 to the interface (s0). From the Router#(config) prompt, type:

   int s0
   custom-queue-list 1

   To determine if the changes have taken effect, use the show interface s0 or the show queuing command.

Troubleshooting

If a priority or custom queue is not working properly, follow these directions:

Unassign the queue from the ports for which it is configured. In interface setup configuration, type the following:

1. If a priority is set up, from Router(config-if)#, type:

   no priority-group 1

2. If a custom queue is set up, from Router(config-if)#, type:

   no custom-queue-list 1

This immediately removes the policy from that interface until a problem is determined. Repeat the procedure from the (config) mode to actually remove the queues, inserting the word “no” in front of the commands to reverse them. Run show running-config to verify that changes were made. Make sure you copy to startup-config using the copy running-config startup-config when changes are acceptable.

Packeteer (PacketShaper)

PacketShaper comes in three configurations.

- The PacketShaper 1000 manages WAN connections at speeds up to 384Kbps
- The PacketShaper 2000 handles WAN and Internet connections at speeds up to 10Mbps
- The PacketShaper 4000 supports WAN and Internet connections at speeds up to 100Mbps

Typically a PacketShaper is located at the remote side just outside of the CSU/DSU to manage the data flowing in and out of the remote location. You can access PacketShaper through a Web interface, a Telnet command line interface, or a console session. If PacketShaper fails, it becomes a straight-through device passing packets as now. PacketShaper identifies traffic, in this case port 1494, traveling in both directions and prioritizes that traffic in a way that allows ICA traffic to get through on the busiest of WANs. PacketShaper can be easily set up.

Packeteer requires some knowledge to get the full benefit from the device. Packeteer allows the administrator to monitor the traffic traveling across the link and then apply policies to that traffic depending upon mission criticality of the protocols or traffic classes. Included in this note are the directions to set up Packeteer to recognize the ICA protocol and start tracking it. You can toggle packet shaping on and off to see the effect that it has on network traffic.

Requirements

Hardware Requirements

- *WINFRAME* or MetaFrame server
- WAN Setup

Software Requirements

- *WINFRAME* Version 1.7 or later
- MetaFrame Version 1.0 or later
- PacketShaper Version 3.0 or later

Installation

Below are the instructions to set up a PacketShaper running Version 3.0 to recognize and prioritize ICA traffic. For Version 3.1, Packeteer has built in recognition for Citrix *WINFRAME*/MetaFrame, so when traffic autodiscovery is on, PacketShaper detects *WINFRAME*/MetaFrame ICA and server balancing traffic and automatically creates classes for both. To determine what version you are running, log in to PacketShaper using the Web interface. Version information is in the top right corner of the PacketShaper Policy Console home page.

1. Make sure your PacketShaper is correctly configured and is functioning on your network. In your configuration (the Setup option of the PolicyConsole navigation bar), make sure that Traffic Discovery is turned on. If you have any questions about this, please contact Packeteer technical support at support@packeteer.com or (408) 873-4550.
2. Create a class for Inbound Citrix *WINFRAME*/MetaFrame traffic:

   A. Click the **Manage** option of the PolicyConsole navigation bar.

   B. Click **inbound** in the Traffic Tree in the left side of the **Manage** dialog box.

   C. Click **Class...** in the **New** area in the right hand side of the **Manage Traffic Tree** dialog box. This creates a child class on the inbound branch of the traffic tree.

   D. In the **New Class** dialog box, complete the following areas:

Class name	outside_WinFrame/MetaFrame_inbound
Protocol family	IP
Service	TCP
Server location	any
Outside port	1494

   E. Click the **Add Class** button.

3. Create a class for Outbound Citrix *WINFRAME*/MetaFrame traffic:

   A. Click **outbound** in the Traffic Tree in the left side of the **Manage** dialog box.

   B. Click **Class...** in the **New** area in the right hand side of the **Manage Traffic Tree** dialog box.

   C. In the **New Class** dialog box, complete the following areas:

Class name	inside_WinFrame/MetaFrame_outbound
Protocol family	IP
Service	TCP
Server location	any
Outside port	1494

   D. Click the **Add Class** button.

4. Set up PacketShaper so you can monitor *WINFRAME*/MetaFrame traffic:

   Click the **Monitor** option of the PolicyConsole navigation bar.

   Click the **Clear All Statistics...** button so that you can see the *WINFRAME*/MetaFrame traffic more clearly.

5. Create Citrix *WINFRAME*/MetaFrame traffic so that PacketShaper can detect it.

   A. Open the *WINFRAME*/MetaFrame Client Remote Application Manager.

   B. From Remote Application Manager, open the applications to which you have access.

   C. Return to PacketShaper's **PolicyConsole Monitor** dialog box.

   D. Click **Update**.

6. Set Policy to give *WINFRAME*/MetaFrame traffic priority over all other traffic.

   A. Click the **Manage** option of the PolicyConsole navigation bar.

   B. Click class outside_WinFrame/MetaFrame_inbound.

   C. In the **New** column, select **Policy**.

   D. From the **Policy** dialog box, click **Priority**.

   E. When the screen refreshes, set priority to **7** and click **Add Policy**.

7. Repeat these steps for the inside *WINFRAME*/MetaFrame outbound class.

You have now configured PacketShaper to manage network traffic so that ICA traffic has priority over all other network traffic.

Applying Server Hotfixes and Service Packs

What are Hotfixes and Service Packs?

Hotfixes are interim MetaFrame system patches available for download from the Citrix Web site (http://citrix.com/support), the Citrix FTP site (ftp.citrix.com), and the Citrix BBS (954-267-2590). Apply hotfixes only on the advice of Citrix Technical Support. Hotfixes are tested and verified to fix specific problems.

Service packs are collections of patches that are released between major revisions of Windows NT. Service packs are cumulative; that is, they contain the patches included in all prior service packs.

Hotfix Naming Convention

Hotfixes are posted as self-extracting executables and follow a specific naming convention. MetaFrame and *WINFRAME* server hotfixes have a slightly different naming convention than client hotfixes. Hotfix ME100010.EXE is used as a server hotfix in the example for the table.

M	Digit 1 specifies whether the hotfix is applicable to a MetaFrame or *WINFRAME* server. This digit can be one of two values: S = *WINFRAME* server hotfix, M = MetaFrame server hotfix.
E	Digit 2 reflects the applicable language, English in this case. Other values include F = French, G = German, S = Spanish, J = Japanese.
10	Digits 3 and 4 reflect the version of the software for which this hotfix is applicable, MetaFrame Version 1.0 in this case.

0	Digit 5 indicates which service pack should be installed before the hotfix is installed. If this digit is “0,” it indicates that the hotfix can be installed without first installing a service pack.
010	Digits 6 through8: this value is sequential and indicates the hotfix number. This example shows it is the tenth hotfix since the last service pack was released. International hotfix numbers match the domestic version of the hotfix

The table below illustrates the naming convention used for client hotfixes. Hotfix NE200581 is used as the example for this table.

N	Digit 1 specifies to what client the hotfix is applicable. This digit can be one of four values: N = ICA 32-bit Client hotfix, W = ICA 16-bit Client hotfix, D = DOS Client hotfix, B = Web Client hotfix.
E	Digit 2 reflects the applicable language, English in this case. Other values include F = French, G = German, S = Spanish, J = Japanese.
2	Digit 3 reflects the security level of the client. This digit can be one of four values: 0 = No encryption, 1 = 40-bit encryption support, 2 = 56-bit encryption support, 3 = 128-bit encryption support.
00	Not used at this time
581	Digits 6 through 8 reflect the client build number, client build number 581 in this case.

Extracting, Installing, and Removing Hotfixes

Create a directory called \Hotfix to store the self-extracting files that you download. Create subdirectories for each hotfix. Use these subdirectories to store the files that are archived within each self-extracting file. Each hotfix contains an executable file, Hotfix.exe. Because each hotfix executable file has the same name (Hotfix.exe), it is **very important** to store each hotfix in a separate subdirectory. Install hotfixes from the directory where you store the extracted files.

▶ **To install a hotfix**

Note Change drive letters and/or directories to match your system configuration.

1. Download the hotfix to the \Hotfix directory.
2. At a command prompt, change to the system directory; for example **C:**
3. Type **cd \hotfix** to change to the \Hotfix directory.
4. Create a subdirectory for the new hotfix; for example, **md me100010**. Change to this directory.
5. Type **..\me100010** to execute the self-extracting file in the parent directory. The files are extracted to the current directory.

6. Review the Readme.txt file for information about the hotfix, such as special installation instructions.
7. Type **hotfix /i** to install the hotfix.
8. Type **hotfix /v** to verify that the files are correctly installed.
9. Type **shutdown 0 /reboot** to reboot the server.

▶ **To remove a hotfix**

1. At a command prompt, type **C:** to switch to the current directory.
2. Change to the directory containing the hotfix; for example, **cd me100010**.
3. Type **hotfix mf:me100010 /r** to remove the hotfix.
4. Type **shutdown 0 /reboot** to reboot the server.

The Hotfix Utility

Hotfix is a utility that makes installing, tracking, and maintaining hotfixes easier.

Command Syntax

HOTFIX [/H /R /V] [*hotfixname*]
HOTFIX /I [*sourcedir*]
HOTFIX [\\computername] [/L /F] [*hotfixname*]

Parameters

\\computername
The name of a remote computer that is the target of the command. This can be used only with the /LIST option.

hotfixname
The name of the hotfix.

sourcedir
Source directory containing the corrected files and the Hotfix.ini file for the hotfix.

Options

/FULL or /F
Specifies a full listing. Default is brief.

/HELP /H or /?
Displays the syntax for the utility and information about the utility’s options.

/INSTALL or /I
Installs the hotfix identified by the Hotfix.ini file in the source directory or the current directory in the source directory was not specified. The fix is installed on the local machine.

/LIST or /L

Displays a list of all installed hotfixes. If a hotfixname is specified, a detailed listing of the specific hotfix is displayed.

/REMOVE or /R

Removes the specified hotfix from the local machine.

/VERIFY or /V

Verifies that the specified hotfix is correctly installed on the local machine. If no hotfixname is specified, all installed hotfixes are checked.

CHAPTER 7

Troubleshooting the System

This chapter contains information to help you diagnose and solve problems with your MetaFrame systems:

- Troubleshooting User Accounts
- Finding Memory Leaks
- Resolving Driver Conflicts
- Setting Up a MetaFrame Server Kernel Debug Session

Troubleshooting User Accounts

Periodically when using an application, I get an error from the application that the hard disk or some group of files is corrupted or missing. Why is this happening?

Many applications create temporary files as they run. They use these files to store information about the document you are working on or information about your particular settings. Any application temporary files are saved in the users' home directories. If users' home directories exist on a network and your network is unstable, these errors can occur. This can also happen when a network server goes down, cannot be reached, or if the network becomes overloaded. If you are having these problems, work with your network administrator to locate the network problem and stabilize the network. You can also move the home directories to the local MetaFrame hard drive to prevent saving temporary files over the network.

Do not keep users' temporary files on a client drive.

Make sure the paths for the TEMP and TMP environment variables do not point to a user's client computer hard drives. If these variables point to a client drive, applications that store temporary files in the directories specified by the TMP or TEMP environment variables can run very slowly and can experience other problems. The best place for temporary files is on the MetaFrame server itself.

Finding Memory Leaks

When multiple users are running a number of applications on a MetaFrame server, it is not unusual for some of these applications to have some form of memory leak that slowly consumes the available memory of the server. A*memory leak* occurs when a memory pool allocates some of its memory to a process and the process does not return the memory. When this happens repeatedly, the memory pool is depleted. If you monitor paged pool bytes and page file usage in Performance Monitor, you will see that they increase over time.

The most common signs that a system is experiencing a memory leak include but are not limited to:

- Virtual memory errors (displayed at the console only)
- Excessive paging of the system pagefile(s)
- Sluggish performance
- System appears to hang
- Client connection/disconnection problems
- Processes and applications become unresponsive

Identifying Memory Leaks Using Performance Monitor

A memory leak can be caused by a process created by a Service, a program, a device driver, etc. The most common way to find a memory leak is to use Performance Monitor to chart the following:

- Object: Process
- Instance: Process Name
- Counter: Private Bytes

For example, on a system with 128MB RAM, a 384MB Pagefile, and two users, the Spoolss.exe shows 250,000,000 private bytes.

Always select the Memory, Objects, and Processes objects when you are looking for a pool leak. Select all counters under each object. You can also select other object counters to help you identify a specific problem. You then simply view all charted objects until one or more objects show a trend that could be a pool leak.

1. By charting the memory resources, it becomes clear that one or more memory pools are allocating memory and the available memory in one or more memory pools is being continuously depleted. When charted, a memory pool can display a continuously climbing stair-step effect while the process leaking memory is running. However, during times of inactivity, it is common to see the charted line remain flat. The charted line continues the stair-step pattern the next time the process leaking memory is started and run.

2. By charting the object counter Object - Threads it is evident that the thread count grows in a manner similar to the tagged pool memory allocations and bytes listed in Step 1. Depending on the amount of threads that are created, the object counter Object - Threads can jump to a high value immediately.
3. The object Process helps determine which process is causing the leak. Select Object counters Pool Nonpaged Bytes, Pool Paged Bytes, and Thread Count. Chart all instances of these counters. The process leaking memory charts in a manner similar to the pool memory that was charted in Step 1.

Identifying Memory Leaks in NT Services

Although Performance Monitor usually provides the necessary information to determine which process is creating a pool leak, it does not always provide the information necessary to determine the exact cause of a memory leak. A trend that shows a memory leak can often be identified but an exact process is not always identifiable as the cause of the memory leak.

If the process leaking memory is a service, you can identify the process in Performance Monitor or by double-clicking **Services** in Control Panel.

1. If the process has been running long enough to show signs of the memory leak, use Performance Monitor to chart the object counter Objects - Threads. The number of threads running depend on many factors, but the number grows larger as the process leaking memory continues to run.
2. From Control Panel, double-click **Services**.
3. Tile the windows so you can see both Control Panel and Performance Monitor.
4. Using Control Panel, start and stop the services one at a time.

If the process that is leaking memory has been running long enough, there will be a drastic reduction in threads when that process is stopped.

Note The process leaking memory does not have to be a service to use this method. If the process leaking memory is a regular program, closing the program also causes the thread count to drop.

Limiting the Impact of Memory Leaks

While there is no way to prevent memory leaks, rebooting the MetaFrame server whenever possible can prevent memory leaks from compounding. Rebooting the server has the added advantage of preventing system degradation caused by disconnected user sessions, crashed applications, and runaway processes. A regular reboot can be scheduled using the **Shutdown** command at the command prompt. For more information on the **Shutdown** command type **shutdown /?** at a command prompt.

Resolving Driver Conflicts

I just installed the Canon GP200F printer/fax drivers on my MetaFrame server. Now, every time I run Word97 and select the Canon GP200F to print to from an ICA Client, I get an error on the MetaFrame server.

The driver DLLs are disrupting the load process by, perhaps, having conflicting base addresses that cannot be rebased. It could also be that the DLL initializations fail because too many implicitly loaded DLLs need thread local storage.

One way to find out is:

1. Get the listdlls executable from www.sysinternals.com and run it with a command line of the form Listdlls –p fxp when the dialog box appears on the screen. That lists all the DLLs in the address space and where they were loaded.
2. Get the preferred base addresses of the driver DLLs (and kernel32.dll) by running the dllbase utility with the DLL as an argument; for example, Dllbase printdriver.dll.

Setting up a MetaFrame Server Kernel Debug Session

Kernel debugging is a process that uses the built-in debugging features of Terminal Server to gather information for detecting, isolating, and resolving system problems.

Kernel debugging involves two computers:

- The computer being debugged, referred to as the *target computer*
- A second computer that controls the execution of the target computer, called the *host computer*

The host computer runs an application called the *kernel debugger* that is used to examine memory and processor status, single-step through programs, and perform other operations useful in problem determination. The target computer can be allowed to run until an error condition occurs or it can be stopped at any time. For Intel-based systems, the kernel debugger application is I386kd.exe.

To allow symbolic debugging (that is, debugging using descriptive names instead of numbers), *symbols* are loaded onto both target and host computers. These symbols contain information used to present information to technical personnel in a more readable manner; for example, displaying regions of memory in terms of their actual usage instead of as lists of hexadecimal numbers. For the information presented to be meaningful, it is important that the symbols present on the target and host computers be identical.

The host computer controls the target computer through a serial communications port. The host can be connected to a local target computer by a serial communications null-modem cable (*local debugging*), or the host can be at a remote location (such as Citrix headquarters) and connected to the target computer by modem (*remote debugging*). The modem used can be any standard Hayes-compatible PC modem; however, Citrix recommends using a U.S. Robotics Sportster series 33.6Kbps modem for best results.

This section describes how to configure a target computer and a host computer for local or remote debugging.

The Kernel Debugger (I386kd.exe)

Using the kernel debugger program, I386kd.exe, a support engineer can use the host computer to control program execution on the target computer. The target computer can be allowed to run until an error condition occurs or it can be manually stopped at any time. The action of stopping the target computer is called *breaking in*. The support engineer breaks into the target computer by pressing CTRL+C in the kernel debugger session on the host computer. If a trap or fault occurs on the target computer, the target machine halts and displays system information. At this point, the operator on the host computer can interactively examine the status of the target computer or allow execution to resume. Press **G** in the kernel debugger session on the host computer to allow execution on the target computer to resume.

The kernel debugger can be used to set execution and memory access breakpoints, examine and modify memory contents, check the state of CPU registers, disassemble code, and other operations.

Symbols and Symbol Trees

To allow symbolic debugging (that is, debugging using descriptive text instead of hex numbers), *symbols* are loaded onto both the target and host computers. These symbols contain information used to present data to technical personnel in a more readable manner; for example, displaying regions of memory in terms of their actual usage, instead of as lists of hexadecimal numbers.

For the information presented to be meaningful, it is important that the symbols installed on the target and host computers be identical and that they match the executable files on the target computer. The symbol files for the base MetaFrame system are located on the MetaFrame CD-ROM in the \Support\Debug\I386 \Symbols directory. The Symbols directory contains directories corresponding to each type of file. You must use **xcopy** to copy the Symbols directory and all its subdirectories to the %SystemRoot% directory on the target computer. These symbols are also copied to a directory on the host computer; this can be any directory and does not have to be the %SystemRoot% directory. These directory structures are referred to as the *symbol tree*.

If the MetaFrame server has hotfixes installed, the symbol files must be installed in the proper order: first the base MetaFrame symbols, then the hotfix symbols. This ensures that the symbols match the executable code.

Kernel Debug Configurations

There are two basic kernel debug configurations - local debug and remote debug. A third type of debug configuration, the ICA debug, is a variation of local debug. Each configuration is discussed below.

In a *local debug* configuration, the host and target computers are in close proximity and are connected by a null-modem cable. While this is the simplest debug configuration, it can only be used for on-site debugging.

In a *remote debugging* configuration, the host and target computers are connected through dial-up modems. This configuration allows a support representative to dial into the target computer located at a remote customer site from a host computer located at Citrix headquarters.

In some cases, the support representative may be unable to directly access the target computer. If two MetaFrame servers are at the remote site, the support representative can perform an *ICA debug* configuration.

Much like the local debug, the host and target computers are in the same location connected by a null-modem cable. In addition, the host computer is configured to accept an ICA dial-in connection. The remote support representative dials in to the host computer and runs the kernel debugger in a remote session. This method combines the simplicity and reliability of a local debug with the ability to remotely debug a customer's target computer.

Requirements for Debugging

To perform kernel debugging, you need the following equipment:

- Target system: MetaFrame server with any hotfixes installed
- Host system (local and ICA debug sessions): MetaFrame server with any hotfixes installed

Note The symbols for the MetaFrame server and hotfixes must be installed in the proper order so that the symbols match the executable files. The host system must have the same MetaFrame server and hotfix symbols installed, but it does not require the same software configuration.

Hardware Requirements

Local Debug Session

- Null-modem cable between host and target computers

Remote Debug Session

- Modems and modem cables for host and target computers. The host computer is usually preconfigured and is at the support provider's site. The target computer requires a modem configured to allow dial-in access to the target system. Citrix recommends using the U.S. Robotics Sportster series 33.6 modem.

ICA Debug Session

- Null-modem cable between host and target computers
- Modems and modem cables for host and remote client computers. The host computer must have a connection configured in Terminal Server Connection Configuration

Configuring the Target Computer for Debugging

The procedure for configuring the target computer is similar for both local and remote debugging. The only difference is that remote debugging requires you to place the modem attached to the debugging port into auto-answer mode.

There are four steps to the setup process:

- Installing hotfixes
- Installing symbols
- Preparing the modem and/or COM port
- Modifying the Boot.ini to enable kernel debugging

Installing Hotfixes on the Target Computer

See "Extracting, Installing, and Removing Hotfixes" earlier in this section.

Installing Symbols on the Target Computer

The correct symbols must be installed on the target computer before kernel debugging can occur.

▶ **To install the debugging symbols on the target computer**

1. Create a Symbols directory in the %SystemRoot% directory; for example,**md %systemroot%\symbols**.

2. Insert the MetaFrame CD-ROM into a CD-ROM drive that can be accessed by the target computer. Use **xcopy** to copy the \Support\Debug\I386\Symbols directory and its subdirectories from the MetaFrame CD-ROM to the Symbols directory; for example: **xcopy /v /s *x*:\support\debug\i386 \symbols %systemroot%\symbols**, where *x* is the CD-ROM drive.
3. If you are installing hotfixes, copy the symbol files corresponding to the new binaries in the hotfix to the %SystemRoot%\Symbols directory on the target computer.
4. When you are done installing the symbols, configure the target system modem and COM port.

Preparing the Target Computer Modem and COM Port

The next step is to configure the COM port and the optional modem (remote debug only) on the target computer. Local and ICA debug configurations use a null-modem connection between the target and host computers and do not need modem configuration. Remote debug configurations require modem configuration.

▶ **To configure the target system COM port for debugging**

For both local and remote debugging, you must select the serial port that will be used by the host system. This must be the highest numbered planar COM port; for example, if your motherboard contains COM1 and COM2 ports, the debugger must use COM2. Select the highest-numbered planar COM port from the pull-down list.

Note **Do not** configure the COM port used for debugging as a connection. Use Terminal Server Connection Configuration to make sure no connection is configured for that port.

Modifying the Boot.ini File to Enable Kernel Debugging

Boot.ini is a system text file that lists the operating systems that can be started, the default operating system to start, and a timeout value specifying how long to wait before automatically starting the default operating system.

When you first start a MetaFrame server, the system loader (NTLDR) reads the Boot.ini file in the system partition. Boot.ini defines what items will be listed in the boot menu and how NTLDR will start each item. Here is a sample Boot.ini file:

```
[boot loader]

timeout=30

default=multi(0)disk(0)rdisk(0)partition(2)\WTSRV
```

```
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WTSRV="Windows Terminal Server
Version 4.00"
multi(0)disk(0)rdisk(0)partition(2)\WTSRV=" Windows Terminal Server
Version 4.00 [VGA mode]" /basevideo /sos
C:\="MS-DOS"
```

The line immediately following the [operating systems] section describes the path NTLDR uses to boot this particular installation of Terminal Server. For the purpose of this document, this line is referred to as the *boot line*. The boot line in this example shows that Terminal Server is installed in the \Wtsrv directory on the second partition (partition 2) of the first disk (disk 0). The next line down starts the same installation of Terminal Server but it uses two switches, /basevideo and /sos, which instruct NTLDR to start the server in a special way. The /basevideo switch starts the system using the standard VGA video driver. The /sos switch displays device driver names as they are loaded.

The target computer is placed in debug mode by setting one or more of the following switches in the boot line in Boot.ini.

Boot.ini Debugger Switches

The following Boot.ini switches are used to enable the kernel debugger on the target computer:

/Debug — Causes the kernel debugger to be loaded during boot and kept in memory at all times. This allows a support engineer to break into the target computer at any time, even if the system is not suspended at a kernel STOP (blue) screen.

/Crashdebug — Causes the kernel debugger to be loaded during boot but swapped out to the pagefile after boot. In this mode, a support engineer can break into the debugger only if the target computer is suspended at a kernel STOP (blue) screen.

/Baudrate=*value* — Determines the speed at which the target computer communicates with the host computer. The default value is 19200 bps. For a remote debug configuration, set the value for 9600 bps. This switch also forces /Debug mode.

/Debugport=COM*x* — Specifies the serial port used for the kernel debugger on the target computer, where *x* is the communications port to use. If no serial port is specified, the kernel debugger defaults to COM2. Like /Baudrate, this switch also forces /Debug mode.

Boot.ini Changes

Because the Boot.ini file usually has the Hidden, System, and Read-only file attributes set, these attributes must be manually unset and then reset after editing.

▶ To modify Boot.ini

1. Right click on Boot.ini and select **Properties**. Uncheck the Read-only check box on the properties dialog box. Boot.ini can now be edited using Notepad. A sample Boot.ini follows:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(2)\WTSRV
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WTSRV="Windows Terminal Server
Version 4.00"
multi(0)disk(0)rdisk(0)partition(2)\WTSRV="Windows Terminal Server
Version 4.00 [VGA mode]" /basevideo /sos
C:\="MS-DOS"
```

2. The best way to modify Boot.ini is to create a new boot entry for debugging. This gives you the ability to boot your MetaFrame server for normal use or for debug use. Copy the desired boot line and append the /Debug switch to the end of the boot line. This switch is sufficient for local and ICA debug configurations. For remote debug configurations, you must also append the /Baudrate=9600 switch to the end of the boot line. If the debug modem or null-modem cable is connected to a communications port other than COM2, make sure you append the /Debugport=COM*x* switch. A sample modified Boot.ini follows:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(2)\WTSRV
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WTSRV="Windows Terminal Server
Version 4.00"
multi(0)disk(0)rdisk(0)partition(2)\WTSRV="Windows Terminal Server
Version 4.00(debug)" /debug /baudrate=9600 debugport=com1
multi(0)disk(0)rdisk(0)partition(2)\WTSRV="Windows Terminal Server
Version 4.00 [VGA mode]" /basevideo /sos
C:\="MS-DOS"
```

Note **Do not** configure the COM port used for debugging as a connection. Use Terminal Server Connection Configuration to make sure no connection is configured for that COM port.

After making the required changes, choose **Save** from the **File** pull-down menu to save the changes.

3. Exit Notepad.
4. Right click on Boot.ini and select **Properties** to restore the Read-only attribute of Boot.ini.
5. Reboot the system. The MetaFrame server is now ready for debugging by a remote host.

Configuring the Host Computer for Debugging

The host computer set up is similar whether the host computer is used in a local, remote, or ICA debug configuration. There are four steps to the set up process:

- Installing symbols
- Preparing the COM port and optional modem
- Installing and configuring the kernel debugger
- Executing the kernel debugger

Installing Symbols on the Host Computer

To effectively debug the target computer, the host computer must have access to a set of symbol files that exactly correspond to the files installed on the target computer. Because the system files installed on the host may not match the system files installed on the target (and are not required to), the symbol tree on the host must be in a directory other than the host's %SystemRoot% directory. Citrix recommends creating a \Debug directory on the host computer with subdirectories for each version of the symbol tree; for example the tree containing the symbols for MetaFrame Version 1.0 might be named \Debug\MF10\Symbols. Follow the same procedures used to install the symbol files on the target computer to install symbols on the host computer, except that where the procedure refers to the %SystemRoot% directory on the target computer, use the \Debug directory on the host computer instead.

▶ **To install the debugging symbols on the host computer**

1. Create a \Debug directory on the host computer. Create a subdirectory for each version of the symbol tree; for example \Debug\MF10\Symbols.
2. Insert the MetaFrame CD-ROM into a CD-ROM drive that can be accessed by the target computer. Use **xcopy** to copy the \Support\Debug\I386\Symbols directory and its subdirectories from the MetaFrame CD-ROM to the directory created in Step 1; for example: **xcopy /v /s *x*:\support \debug\i386\symbols d:\debug\mf10\symbols**, where *x* is the CD-ROM drive.
3. If you are installing hotfixes, copy the symbol files corresponding to the new binaries in the hotfix to the symbols directory created in Step 1 of the target computer.

4. When you are done installing the symbols, configure the target system for debugging.

If the target computer is a multiprocessor system or uses a special hardware abstraction layer (HAL), you must rename some of the symbol files.

For multiprocessor systems, rename NTkrnlmp.dbg to NToskrnl.dbg. These files are located in the Exe subdirectory of the symbol tree.

In File Manager, click **Properties** to examine the internal name of the Hal.dll file on the target computer. This file is located in the %SystemRoot%\System32 subdirectory. Based on this information, rename the corresponding Dbg file to Hal.dbg in the DLL subdirectory of the symbol tree.

Preparing the Host Computer Modem and COM Port

As with the target computer, the next step is to configure the COM port and the optional modem (remote debug only) on the host computer. Local and ICA debug configurations use a null-modem connection between the target and host computers and do not need modem configuration. Remote debug configurations require modem configuration.

Local Debug

For local debugging, very little configuration is required. Connect a null-modem cable between the serial ports of the host and target computers.

Remote Debug

In a remote debug configuration, a modem is connected to the host computer. This modem must be set to communicate at 9600 bps. It may also be necessary to disable flow control, error correction, and compression. See "Executing the Kernel Debugger" later in this section for directions on resetting the modem.

ICA Debug

Like local debug configurations, ICA debug configurations require a null-modem connection between the host and target computers. In addition, an async dial-in connection must be configured on the host computer and a modem connected to the dial-in connection port. Use Terminal Server Connection Configuration or the Dial-In Setup Wizard to create the dial-in connection.

Installing and Configuring the Kernel Debugger Application

To install the kernel debugger application, insert the Terminal Server CD-ROM in the host computer. Copy the files located in the \Support\Debug\I386 directory on the Terminal Server CD-ROM to the \Debug directory on the host that was created to hold the symbol files.

The following environment variables control the behavior of the kernel debug application, I386kd.exe.

Variable	Purpose
_NT_DEBUG_PORT	COM port used by the host computer for debugging. Default = COM1.
_NT_DEBUG_BAUD_RATE	The maximum baud rate for the debug port. Use 9600 or 19200 for modem connections, 19200 for null-modem serial connections. Default = 19200.
_NT_SYMBOL_PATH	The path to the symbols directory.
_NT_DEBUG_LOG_FILE_APPEND	The name of the log file to which debugger appends output.
_NT_LOG_FILE_OPEN	Optional; the name of the file to which to write a log of the debug session.

I386kd.exe supports the following command-line switches:

-b Causes the debugger to stop execution on the target computer as soon as possible, by causing a debug breakpoint (INT 3).

-m Causes the debugger to monitor modem control lines. The debugger is only active when the data carrier detect (DCD) modem signal is asserted; otherwise, the debugger is in terminal mode and all commands are sent to the modem. This option can be used only with a remote debug configuration.

-r Toggle output register flag

-v Verbose mode; displays more information about such things as when symbols are loaded.

-x Causes the debugger to stop execution on the target computer and break to a command prompt when an exception first occurs, rather than letting the application or module that caused the exception handle it.

Citrix recommends that a batch file be used to configure the environment prior to executing I386kd.exe. For example, assume the following host configuration:

- Remote debug configuration
- Host modem is connected to COM2
- The baud rate is 9600
- The host’s symbol tree is located in C:\Debug\MF10\Symbols
- A log file is created in C:\Debug\MF10\Symbols

Here is a sample batch file using the assumptions listed above:

```
REM Sample Debug Batch File: SETDEBUG.BAT
REM Set Remote Debug Configuration: COM2, 9600 baud
set _NT_DEBUG_PORT=com2
set _NT_DEBUG_BAUD_RATE=9600
REM Set path to debug symbols
set _NT_SYMBOL_PATH=c:\debug\mf10\symbols
REM Enable logging and set log path
set _NT_LOG_FILE_OPEN=c:\debug\mf10\symbols\debug.log
REM Start kernel debugger: Verbose mode, Monitor DCD
i386kd -v -m
```

Running the Kernel Debugger

The actual debugging process is outside the scope of this document. This section describes only how to verify that the debugger is installed and configured properly. Once this is verified, the system is ready for a support engineer to debug the system.

Local and ICA Debugs

When I386kd is executed on the host computer, the following text is displayed:

```
Microsoft(R) Windows NT Kernel Debugger
Version 4.00
Copyright (C) Microsoft Corp. 1981-1996
Symbol search path is:
KD: waiting to connect...
```

At this point, the kernel debugger is waiting for user input. You can press CTRL+C to break into the target computer if it is still running. If the target is currently stopped at a blue screen, break in occurs automatically. If you have any problems at this point, press CTRL+R to force a resynchronization between the host and target computers.

Remote Debug

If you are using a remote debug configuration, I386kd must be executed with the**-m** option. The following text is displayed:

```
Microsoft(R) Windows NT Kernel Debugger
Version 3.51
(C) 1991-1995 Microsoft Corp.
Symbol search path is:
KD: waiting to connect...
KD: No carrier detect - in terminal mode
```

In this case, the debugger is in terminal mode, so you can directly send standard**at** commands to the host modem. Begin by sending commands to disable hardware compression, flow control, and error correction. These commands vary from modem to modem, so consult your modem documentation. The following modem initialization string is recommended for U.S. Robotics modems:

```
AT&H0&I0&K0&M0&N6
```

Once the modem is initialized properly, it must be instructed to dial the phone number of the target modem. This is accomplished by sending the **ATD** command to the modem. For tone dialing phone systems, type **ATDT*phonenumber***, where *phonenumber* is the telephone number of the modem connected to the target system.

Some telephone systems use pulse dialing systems. For pulse dialing systems, type **ATDP*phonenumber***, where *phonenumber* is the telephone number of the target modem.

Assuming the modem connected to the target system is properly configured, the host modem and target modem establish a connection and assert the data carrier detect (DCD) signal. Once DCD is detected, terminal mode is disabled and you are connected to the debugger on the remote target computer.

At this point, the kernel debugger is waiting for user input. You can press CTRL+C to break into the target computer, if it is still running. If the target is currently stopped at a blue screen, break in occurs automatically. If you have any problems at this point, press CTRL+R to force a resynchronization between the host and target computers.

With some remote debug configurations, it can be difficult to break into the debugger. See “Troubleshooting” below for additional tips.

Troubleshooting a Debug Session

Typically, few problems are encountered with local and ICA debugs. Most problems occur when doing a remote debug and they are generally modem related. The most common problems encountered are:

- Inability to break into the debugger
- Failure of the target modem to auto-answer
- [Parity Error] message

Each problem is discussed separately below.

Inability to Break into the Debugger

This is the most common problem experienced. The symptom is that the target computer fails to respond to the CTRL+C and CTRL+R commands from the host computer. The target and host modems appear to be connected and functioning normally but the host operator is unable to stop the target computer.

It is not clear why this condition occurs. Because this problem can be difficult to resolve, Citrix recommends using an ICA debug instead of a remote debug if the problem occurs. If an ICA debug configuration is not possible, follow the steps below to resolve this problem:

1. Make sure the target computer is started in debug mode. When the target computer is rebooted in debug mode, the initial blue startup screen displays text showing the kernel debugger enabled on a particular COM port. If this text is not displayed, the debug options were not added correctly to the Boot.ini file. Make sure the COM port displayed is the one to which the modem is connected.
2. Change the modem make and model on the target computer. If possible, use the same make and model modem as the Citrix representative. Similar modems appear to have a higher remote debug success rate compared with modems from different manufacturers. Citrix recommends using the U.S. Robotics Sportster series 33.6 modem.
3. Force the baud rate of both modems to 9600 bps. Consult your modem documentation for the initialization strings that set the DTE and DCE rates to 9600 bps. For U.S. Robotics modems, this command is AT&N6.
4. Add the /baudrate=9600 option to Boot.ini. This forces the baud rate on the debug COM port to 9600 bps. Always set remote debug configurations for this option.
5. Press the PrintScreen key on the target computer console. While in debug mode, the PrintScreen key will cause the host computer to break in.
6. Make sure both modems are set to transmit break signals. For some modems, a break signal (CTRL+C) received from the computer may cause the modem to perform a specific task without actually transmitting the break to the remote system. For instance, the default behavior of U.S. Robotics modems is to flush the data buffer before sending the break signal to the remote modem. Make sure both modems are set to pass the CTRL+C character. Consult your modem documentation for the necessary commands. For example, to disable destructive breaks on U.S. Robotics modems, the command is AT&Y2.
7. With the modems connected and data carrier detect present, reboot the target computer. If the target modem is set to ignore the state of DTR, the modems will stay connected even if the target computer is rebooted. When the kernel loads on the target computer, it outputs information to the debug port. If the host computer is connected at that time, this can cause the systems to synchronize.

Failure of the Target Modem to Auto-Answer

For all Hayes-compatible modems, ATS0=1 is the command that instructs the modem to auto-answer on one ring. The target modem must be configured with this setting. If the target modem does not auto-answer, follow the procedure below:

1. Move the target modem to a COM port other than the port currently being used by the kernel debugger. If only one COM port is available on the target computer, connect the modem to a different computer or reboot the target with the debugger disabled.
2. Use the Terminal application (or another communications program such as Hyperterminal) to send the ATS0=1 command to the modem. Make sure you receive an OK response from the modem.
3. If possible, dial the number for the modem from a telephone handset to check that it now auto-answers.
4. Save the current modem configuration in non-volatile RAM so the modem is in auto-answer mode when it is powered up. For example, the command AT&W saves the current modem configuration to non-volatile RAM (NVRAM) for U.S. Robotics modems. When the debug process is finished, restore the factory defaults by sending the AT&F command (or equivalent) to the modem. Use the AT&W command (or equivalent) to save the factory defaults to NVRAM.
5. Reconnect the target modem to the debug port on the target computer (or restart the target computer in debug mode).
6. Use the host computer to dial into the target modem.

[Parity Error] Message

This message is displayed on the host computer if the baud rates are too high to sustain a reliable connection. The following steps resolve this problem:

1. Force the baud rate of both modems to 9600 bps. Consult your modem documentation for the initialization string(s) that sets the DTE and DCE rates to 9600 bps. For U.S. Robotics modems, this command is AT&N6.
2. Add the /baudrate=9600 option to Boot.ini. This sets the baud rate on the debug COM port to 9600 bps. Always set remote debug configurations for this option.
3. Change the modem make and model on the target computer. If possible, use the same make and model modem as the Citrix representative. Identical modems appear to have a higher remote debug success rate versus modems from different manufacturers.
4. Conduct a loopback test to isolate the network. Install the ICA Win32 Client on the MetaFrame server and make an IPX connection back to the MetaFrame server. If the loopback test passes, verify that ICA connections on the same network segment as the MetaFrame server can connect. If clients on the same network segment can connect but clients on other segments cannot connect, there is a problem with the router configuration or cabling.
5. Install the most current ICA Client.

6. Install the most current network interface card (NIC) drivers on the client and server machines.
7. Remove and reinstall the NWlink IPX service.
8. Use Event Viewer to check for connection-related error messages.
9. If the problem persists, create a debug trace for the ICA Client connection.

Index