



IBM eServerJ iSeriesJ

Session: 409113
25TC

iSeries NetServer: What's New!

<http://www.ibm.com/servers/eserver/series/netserver/>

Charles Emig
emig@us.ibm.com
March, 2003

© Copyright IBM Corporation, 2003. All Rights Reserved.
This publication may refer to products that are not currently available in your country. IBM makes no commitment to make available any products referred to herein.

Agenda

- Available in V5R1
 - ▶ Domain Logon Support
 - ▶ Security Enhancements
 - ▶ Linux Support
- Available in V5R2
 - ▶ Kerberos version 5 authentication
 - ▶ User defined subsystems for file serving jobs
 - ▶ Windows popup messaging
 - ▶ Windows XP Professional support
- Additional References

iSeries NetServer Advanced Support

What was new in V5R1?

- Domain Logon Support
- Security Improvements
- Support for Linux Samba clients via PTFs
- Configuration Wizard in Operations Navigator
- Large File Support (> 2GB)
- Session management enhancements for WTS
- Added support for Windows NT background services
- Printer shares can be published in Directory Services

iSeries NetServer Advanced Support

What's new in V5R2?

- Support for Kerberos version 5 authentication
- Run file server jobs in subsystems other than QSERVER
- Base support for Linux Samba clients
- Windows popup messages
- QUSRTOOL for menu driven use of iSeries NetServer APIs
- Support for Windows XP Professional

V5R1 iSeries NetServer Logon Support

Domain Logon Support

What iSeries NetServer Logon support provides:

- ✓ Domain Master Browser function
- ✓ Domain Controller reporting for domain discovery requests from clients
- ✓ Central location for the storage of home directories, Windows user profiles, Windows system policies, and logon scripts
- ✓ Domain/Workgroup logon authentication. The following can occur through the logon process:
 - ▶ Automatic retrieval of Windows user profiles if configured to be roaming
 - ▶ Automatic retrieval and application of Windows system policies
 - ▶ Automatic retrieval and execution of a logon script
 - ▶ Automatic drive mapping to the user's home directory for Windows NT/2000/XP

Domain Logon Support

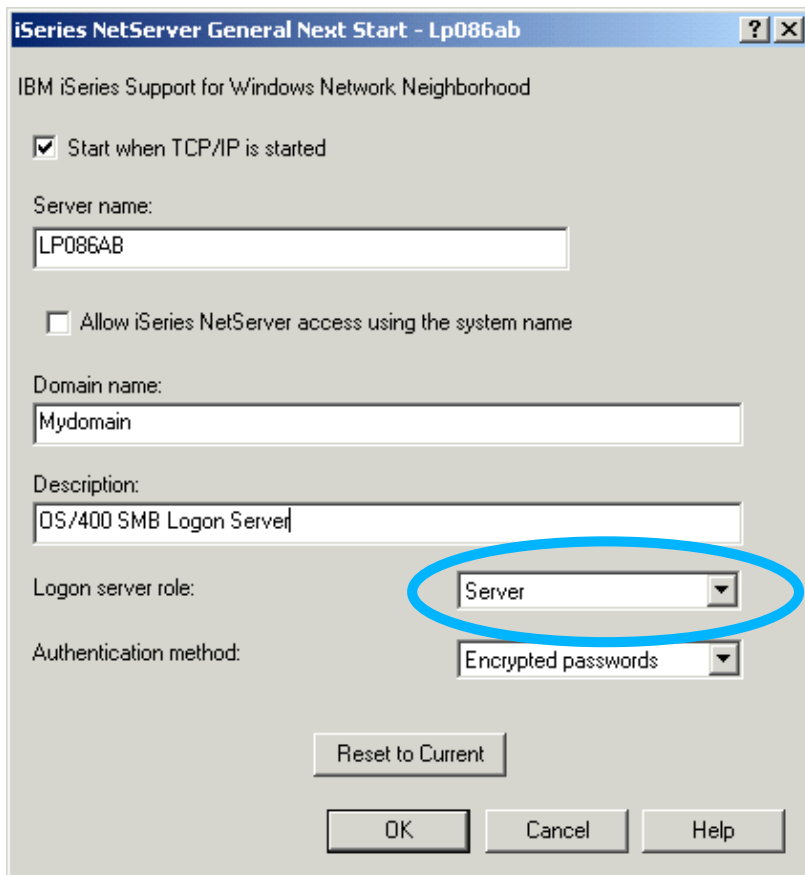
What iSeries NetServer Logon support does NOT provide:

- ✘ Single point of authentication for domain (users still need to authenticate with other servers when accessing their shares)
- ✘ Automatic Backup Domain Controller (BDC) function including replication and failover
- ✘ WINS Server (but iSeries NetServer participates in WINS)
- ✘ Network password change support
- ✘ Server Manager and Computer Accounts Database
- ✘ Domain User Accounts Database (i.e. No User Manager to centrally administer and store domain-specific user info such as restricted logon times).

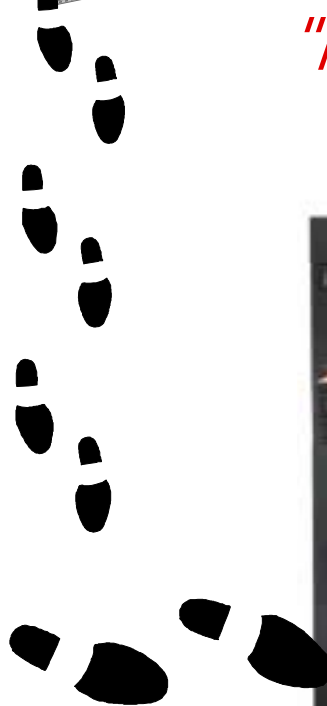
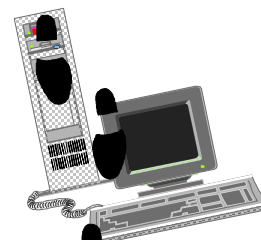
✎ If any of these functions are needed, then a Windows NT Server or SAMBA Server is still required.

Domain Logon Support

Configuring your iSeries as a Logon Server



General tab of iSeries NetServer properties



*"Move over,
NT!"*



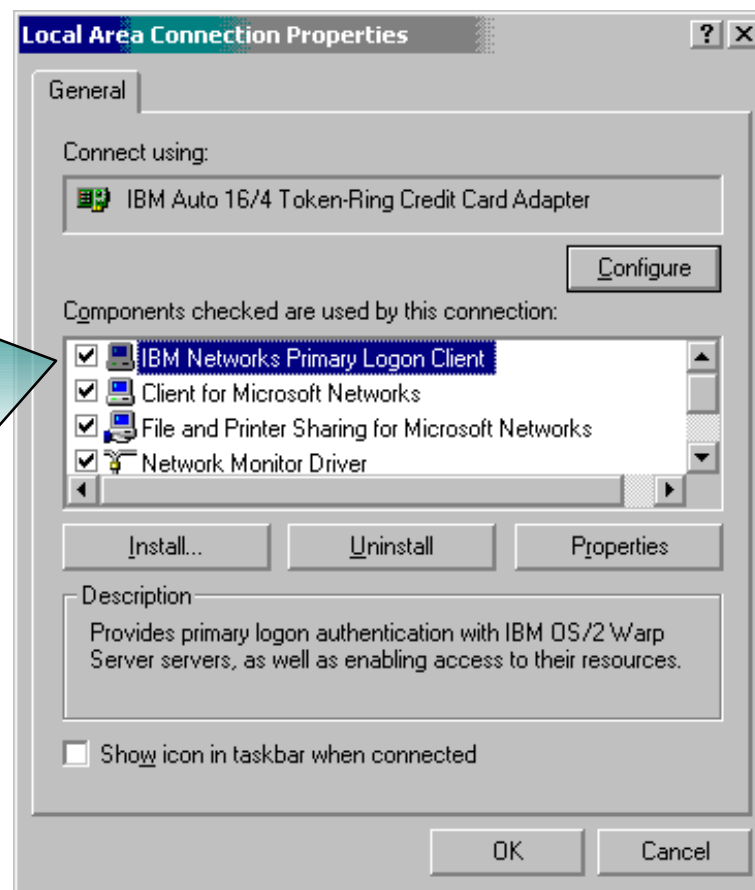
Domain Logon Support

Windows 95/98

- No additional software needed

Windows NT/2000/XP

- Requires "IBM Networks Primary Logon Client for Windows NT/2000/XP"
- Free download for iSeries customers
- "Some restrictions apply"



V5R1 Security Enhancements

V5R1 Security Enhancements - Password Levels

Password Level System Value: QPWDLVL

Moving to QPWDLVL 1

- ▶ Passwords remain 10 characters maximum and case-insensitive
- ▶ LANMAN user passwords no longer supported and deleted
- ▶ Windows 9x clients must be configured for NTLMv2 to access iSeries NetServer

Moving to QPWDLVL 2

- ▶ iSeries allows mixed case 128 character passwords (same as Windows 2000)
- ▶ LANMAN user passwords are supported, but Windows 9x clients will not work with long passwords
- ▶ Potential issues if later move to a lower password level

Moving to QPWDLVL 3

- ▶ iSeries allows up to mixed case 128 character passwords
- ▶ LANMAN user passwords no longer supported and deleted
- ▶ Windows 9x clients must be configured for NTLMv2 to access iSeries NetServer
- ▶ Potential issues if later move to a lower password level

V5R1 Security Enhancements - NTLMv2

NTLMv2 Authentication Support

- ✓ iSeries NetServer now supports clients using NTLMv2 authentication
- ✓ NTLMv2 authentication removes the dependency on the old LANMAN style password encryption
- ✓ Uses more secure MD5 hashing algorithm
- ✓ If passwords don't match, some clients will not allow you enter a new one

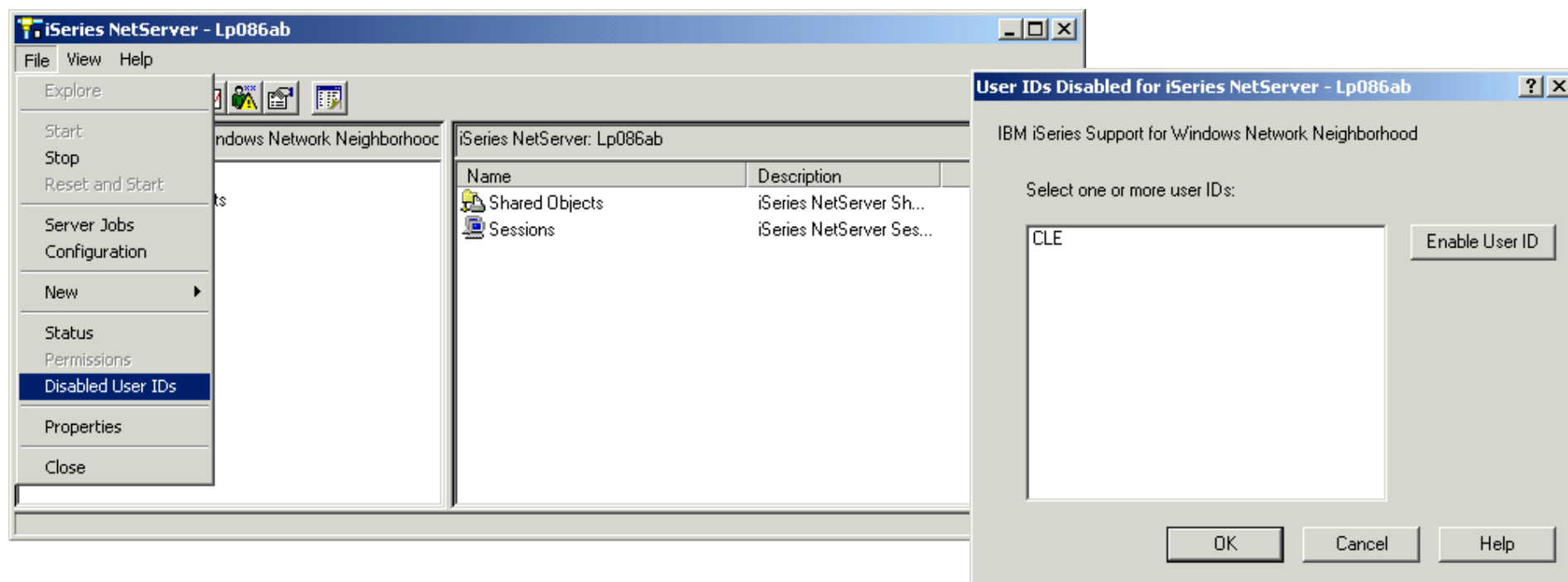
How to enable on Windows 95/98

- Official Microsoft documentation:
<http://support.microsoft.com/support/kb/articles/Q239/8/69.ASP>
- Requires IE 4 or later browser
- Requires Directory Services Client installed (Windows 2000 Server CD)
- Change the following registry key:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
"LMCompatibility"=dword:00000003 (Change to 0 to disable)

V5R1 Security Enhancements - Disabled Users

Disabled Users in iSeries NetServer

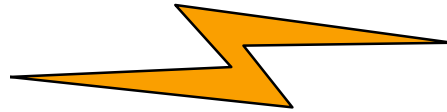
- More "smarts" built in
- Automatic disabling problem diminished
- New GUI Administration of disabled users



iSeries NetServer: **Support for Linux clients**

Linux Support

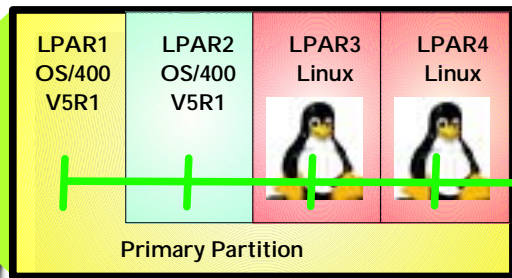
- Stand-alone Linux client



- iSeries NetServer
- iSeries V5R2



- V5R1 LPAR
- Linux Partitions
- Samba is client to local LPAR #1 and remote iSeries NetServer



What is Samba, really?



Briefly

- ▶ Samba is an Open Source file server and client compatible with Microsoft Networking, that comes with many current distributions of Linux.
- ▶ SaMBa - Unix implementation of the SMB protocol (CIFS)

Samba is...

- ▶ Free
- ▶ Popular
- ▶ Licensed under the GPL
- ▶ Andrew Tridgell's brainchild
- ▶ Highly configurable
- ▶ Constantly enhanced/changing
- ▶ Relatively mature (server)
- ▶ Vendor independent
- ▶ Essential to the value proposition of Linux on iSeries

Samba client utilities

- smbclient
- smbmount
- smbmount
- smbprint
- nmblookup



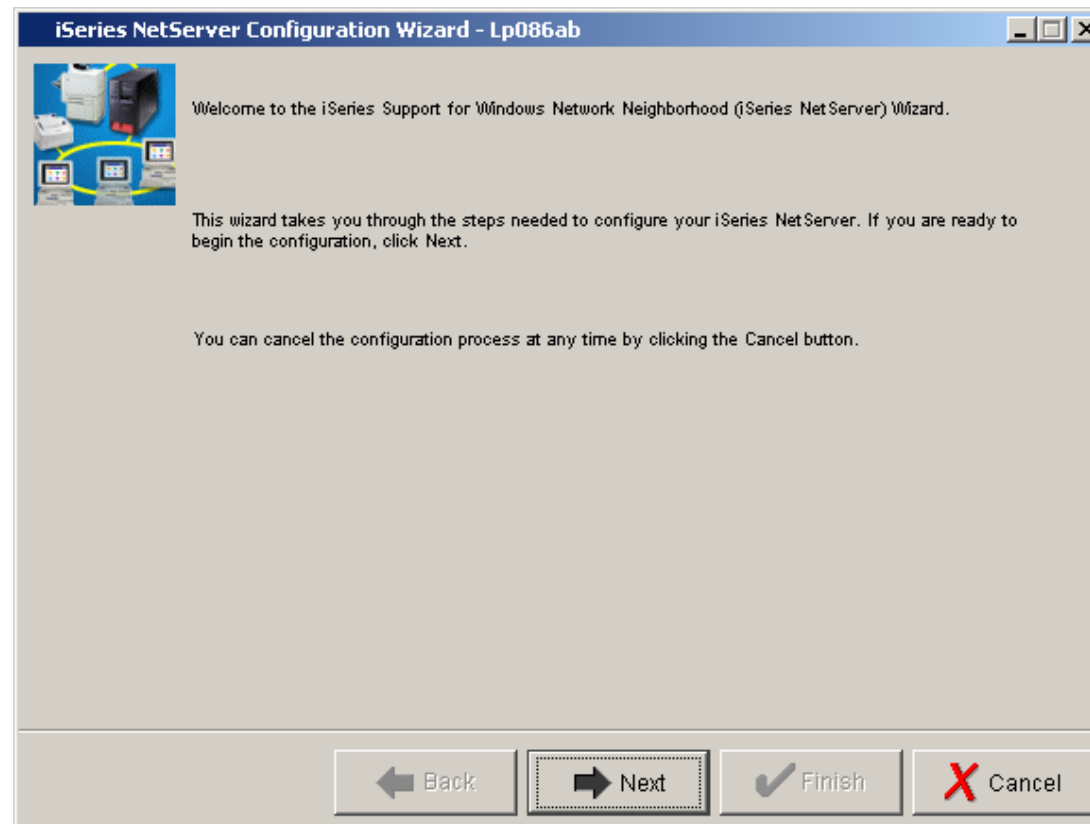
⚡ **Note:** Although *smb.conf* is primarily a Samba server configuration file, these client utilities scan it and make use of some options such as 'wins server'

V5R1 Miscellaneous Enhancements

Configuration Wizard

- Easily Setup iSeries NetServer the first time
- Choose menu option **File > Configuration** from the iSeries NetServer window.

**First
screen
from
wizard**



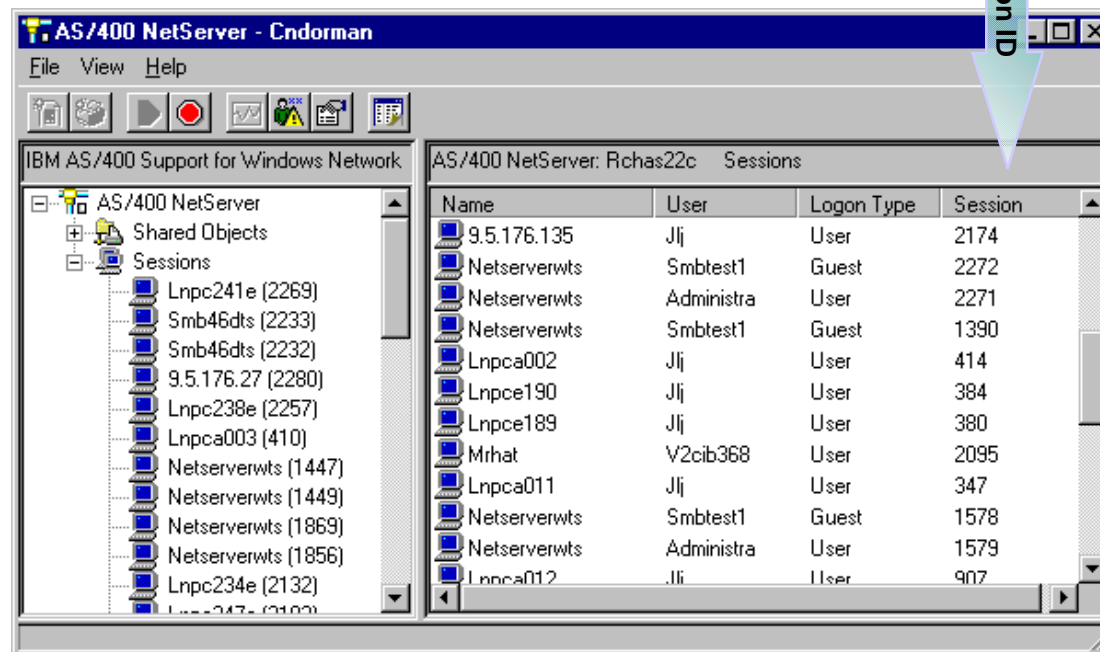
Large File Support & Scalability

- **iSeries NetServer now supports file sizes greater than 2 Gigabytes**
 - ▶ Use is contingent upon the file system being served out of
 - ▶ Currently these file systems support large files: Root, QOpenSys, QSYS.LIB, UDFS, and NFS

- **Improved Scalability for Network Connections**
 - ▶ Asynchronous I/O completion ports
 - ▶ Support for Direct TCP/IP Hosting added
 - Windows 2000 SMB connections to port 445

Session Improvements

- Unique Session Identifier
 - ▶ Can view properties share usage for individual WTS sessions
 - ▶ Can stop individual WTS sessions



- Support for Windows Background Services
 - ▶ Piggybacking virtual users

Publishing Printer Shares

Publishing with Directory Services

Works only in conjunction with these services in the network

- ▶ Need Windows 2000 server configured for Active Directory
- ▶ Need Directory Services (LDAP) configured to the Windows 2000 Active Directory

Select this to publish

The screenshot shows the 'iSeries NetServer Print Share - Lp086ab' dialog box. The 'General' tab is selected. The dialog is titled 'IBM iSeries Support for Windows Network Neighborhood'. It contains the following fields and options:

- Share name: PRINTER
- Description: iSeries NetServer shared printer
- Output queue: Print
- Library: Qgpl
- Printer driver: Apple LaserWriter II NT
- Spooled file type: Auto-select
- Printer file: (empty)
- Library: (empty)
- Publish on LDAP directory server

There are two 'Browse...' buttons on the right side of the dialog, one next to the 'Output queue' field and one next to the 'Printer file' field. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

V5R2 Kerberos Authentication Support

Kerberos Authentication Support

Requirements

- iSeries Requirements
 - ▶ V5R2 OS/400
 - ▶ 5722AC3 - Cryptographic Access Provider 128-bit
 - ▶ Network Authentication Service configured
 - ▶ Enterprise Identity Mapping (EIM) configured
- Other Requirements
 - ▶ A separate machine to act as the Key Distribution Center (KDC)
 - Windows 2000 server is recommended
 - Windows 2000 Support Tools must be installed
 - ▶ A client base of only Kerberos enabled clients
 - Windows 2000 or Windows XP are supported
 - Windows 9x/Me/NT clients cannot connect when Kerberos authentication support is enabled
 - Samba clients do not currently support Kerberos authentication

Kerberos Authentication Support

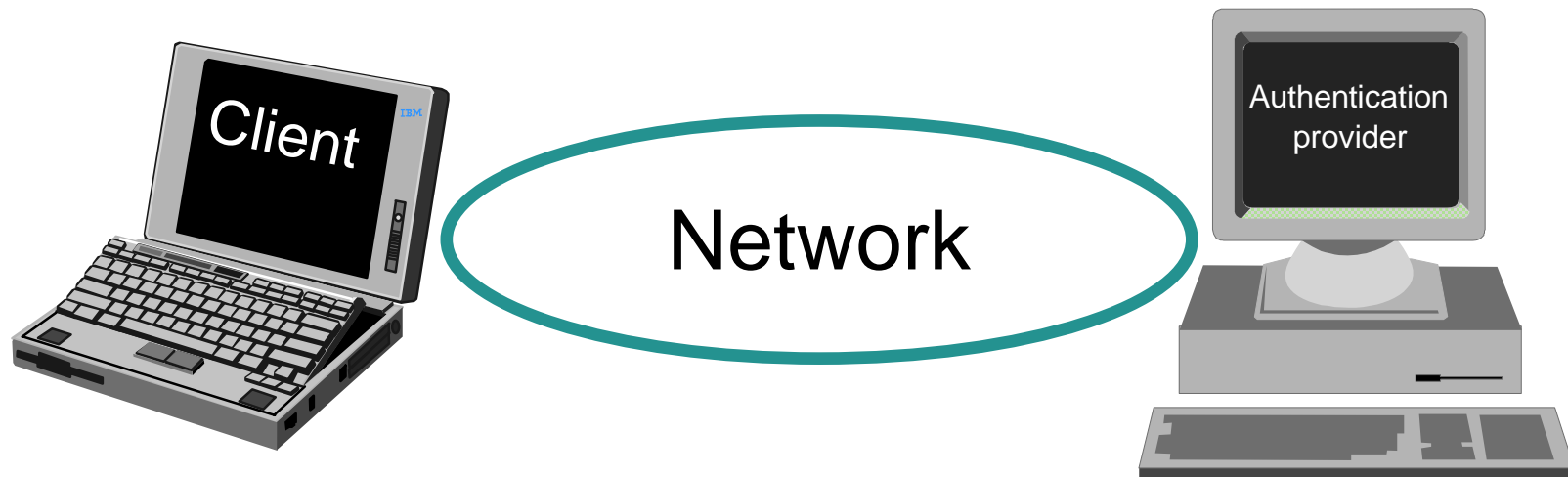
Benefits / Limitations

- Benefits
 - ✓ **No need to match Windows and iSeries profile names or passwords**
 - ✓ Single network signon
 - ✓ Increased authentication security
- Limitations
 - × A separate machine must act as the Key Distribution Center (KDC)
 - × Additional configuration is required
 - × Not compatible with iSeries NetServer logon support
 - × Windows 9x/Me/NT clients do not support Kerberos authentication
 - × Supported Samba clients do not currently include Kerberos authentication support

Kerberos Authentication Support

Network Authentication

- What is Network Authentication?
 - ▶ Act of using a network provider to verify the identity of a user attempting to establish a connection to a network resource



Kerberos Authentication Support

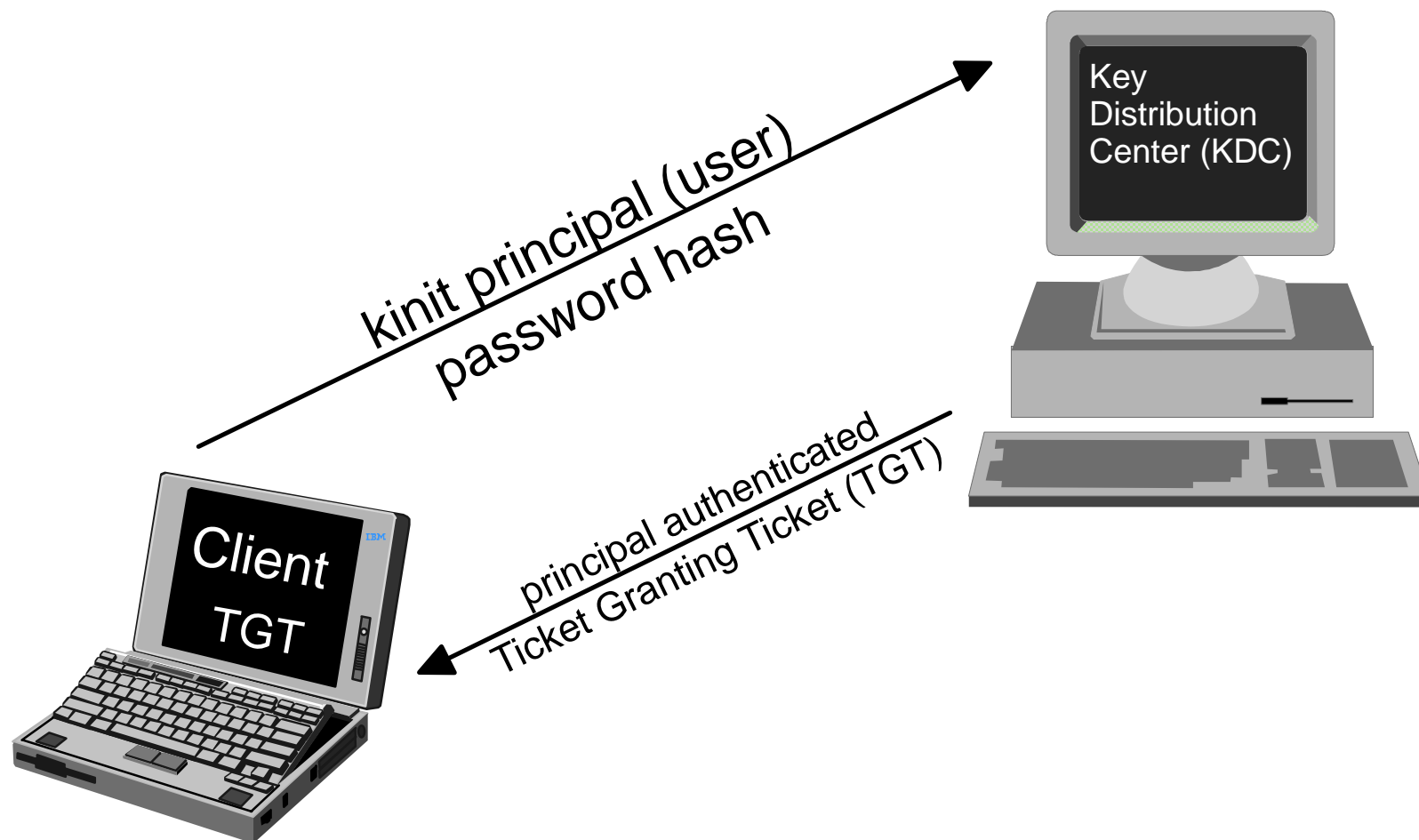
Kerberos

What is Kerberos:

- ▶ Kerberos is an network authentication protocol that:
 - Provides strong **authentication** for client/server applications
 - Uses secret-key cryptography
 - Allows mutual authentication between a client and server
- ▶ Kerberos does **NOT**:
 - Encrypt transaction data once a session is established

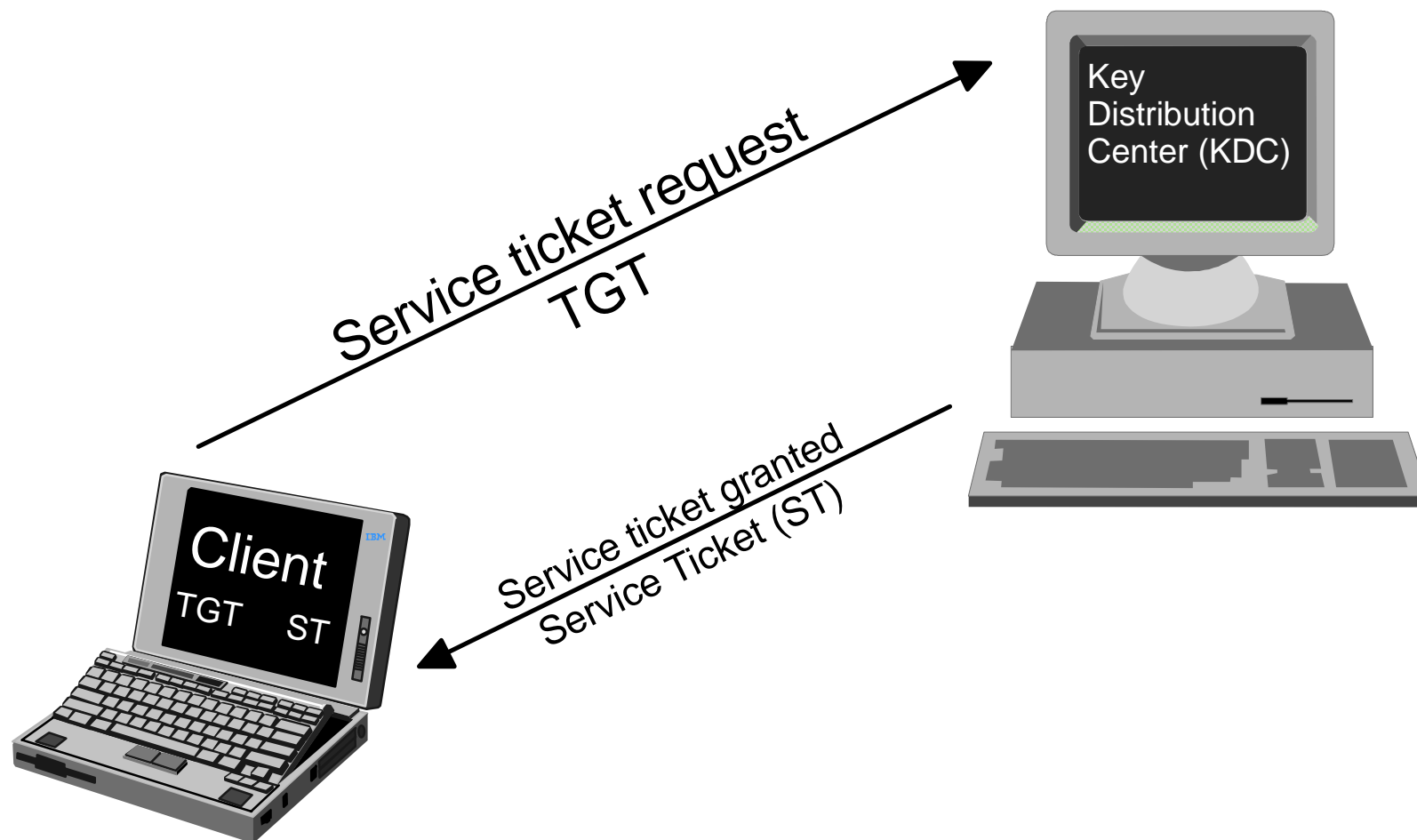
Kerberos Authentication Support

Kerberos Flows - Initial Logon



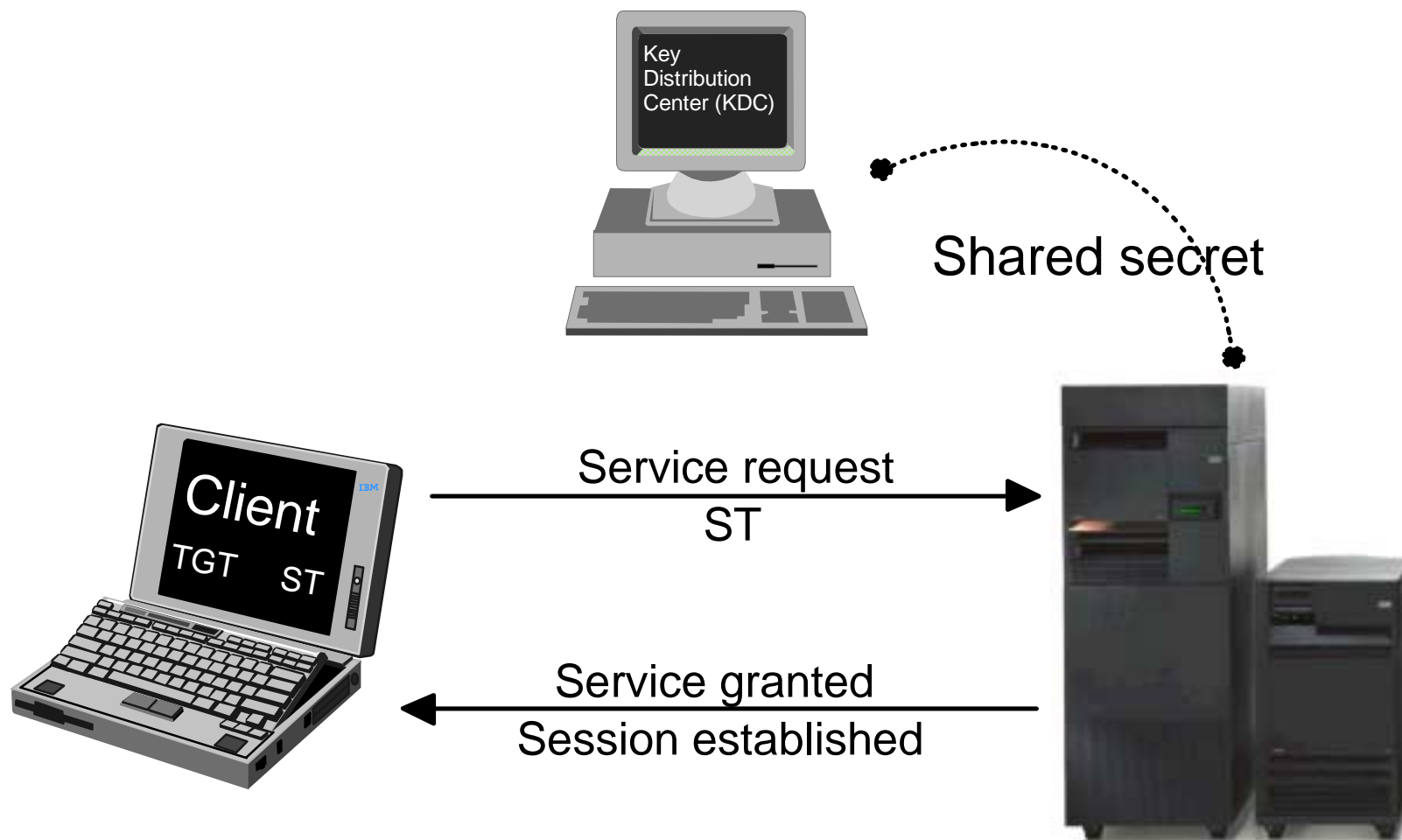
Kerberos Authentication Support

Kerberos Flows - Service Ticket Request



Kerberos Authentication Support

Kerberos Flows - Service Request



Kerberos Authentication Support

Enterprise Identity Mapping (EIM)

What is EIM:

- ▶ EIM is an eServer (i.e. cross platform) function used to map user identities between systems. EIM allows you to:
 - Create and maintain list of people/servers within enterprise.
 - Keep track of IDs (registry user names) associated with a person/server on systems (registries) in a network.
 - Find local identity based off of a source identity.
- ▶ EIM does **NOT**:
 - Store passwords.
 - Perform user authentication.
 - Perform object or resource authorizations.

Kerberos Authentication Support

Understanding EIM

Employee: Jane S Doe

Company's network

| | | | |
|--------------------------|--------------------------|---------------------|--|
| iSeries: machine1 | zSeries: machine2 | pSeries: mc3 | Kerberos realm: MYCOMPANY.COM |
| ID: JANEDOE | ID: JSDOE | ID: JANED | Principal: janedoe@mycompany.com |

Given Jane's situation, the following EIM associations could be established:

| List Of EIM Associations For Jane Susan Doe | | | |
|---|---------------|-----------------------|------------------|
| EIM Identifier | Registry Name | Registry User Name | Association Type |
| Jane S. Doe | MYCOMPANY.COM | janedoe@mycompany.com | Source |
| Jane S. Doe | machine1 | JANEDOE | Target |
| Jane S. Doe | machine2 | JSDOE | Target |
| Jane S. Doe | mc3 | JANED | Target |

Kerberos Authentication Support

Central Concept Behind Kerberos Authentication and EIM

| List Of EIM Associations For Jane Susan Doe | | | |
|---|---------------|-----------------------|------------------|
| EIM Identifier | Registry Name | Registry User Name | Association Type |
| Jane S. Doe | MYCOMPANY.COM | janedoe@mycompany.com | Source |
| Jane S. Doe | machine1 | JANEDOE | Target |
| Jane S. Doe | machine2 | JSDOE | Target |
| Jane S. Doe | mc3 | JANED | Target |

- User authenticates on source machine with **Kerberos** principal/pwd.
- Server on target machine receives **Kerberos Service Ticket (ST)**.
- Target server validates the ST and extracts the source **registry user name** and **registry name** from it.
- Source **registry user name**, the source **registry name**, and the local **registry name** are passed to an EIM API.
- EIM API returns the appropriate local **registry user name** which the server can use any way it wants.

Kerberos Authentication Support

Configuring Network Authentication Service

- ▶ Access the Network Authentication configuration wizard through iSeries Navigator
 - Security | Network Authentication Service
 - Right click and choose **Configure...**



Kerberos Authentication Support

Configuring Network Authentication Service

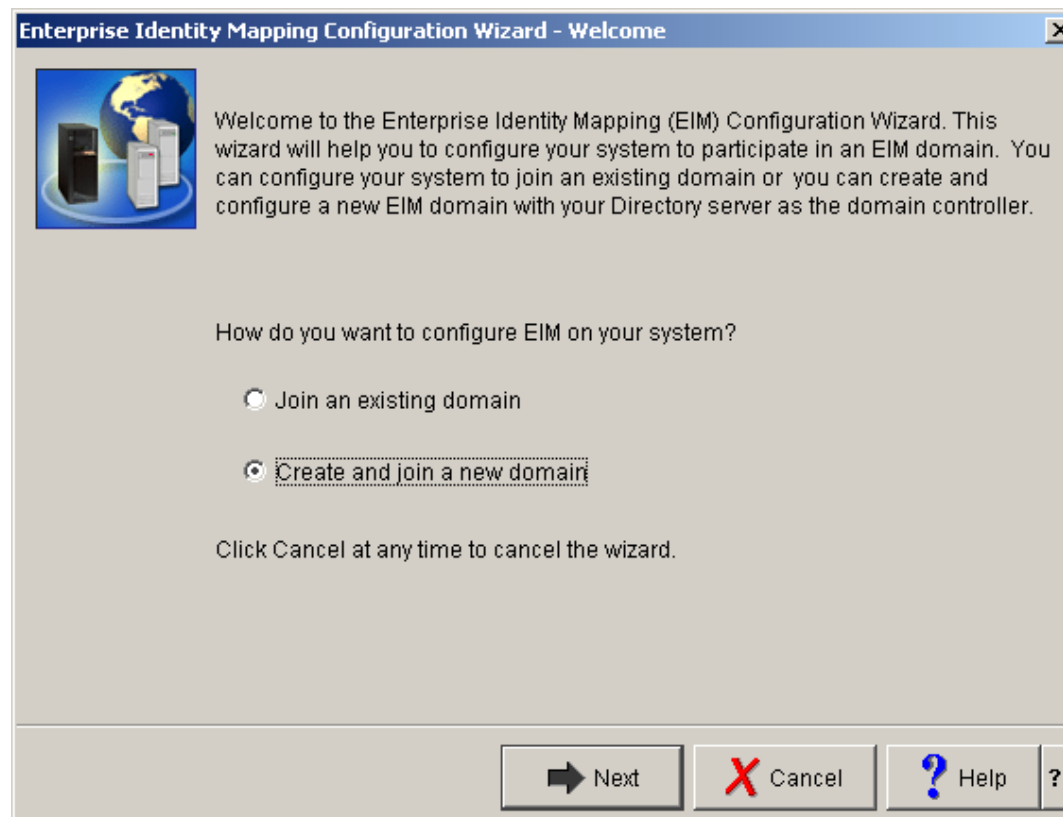
- ▶ During configuration be sure to choose to add the service principal names required by iSeries NetServer
- ▶ Remember the password used for the iSeries NetServer principals for later



Kerberos Authentication Support

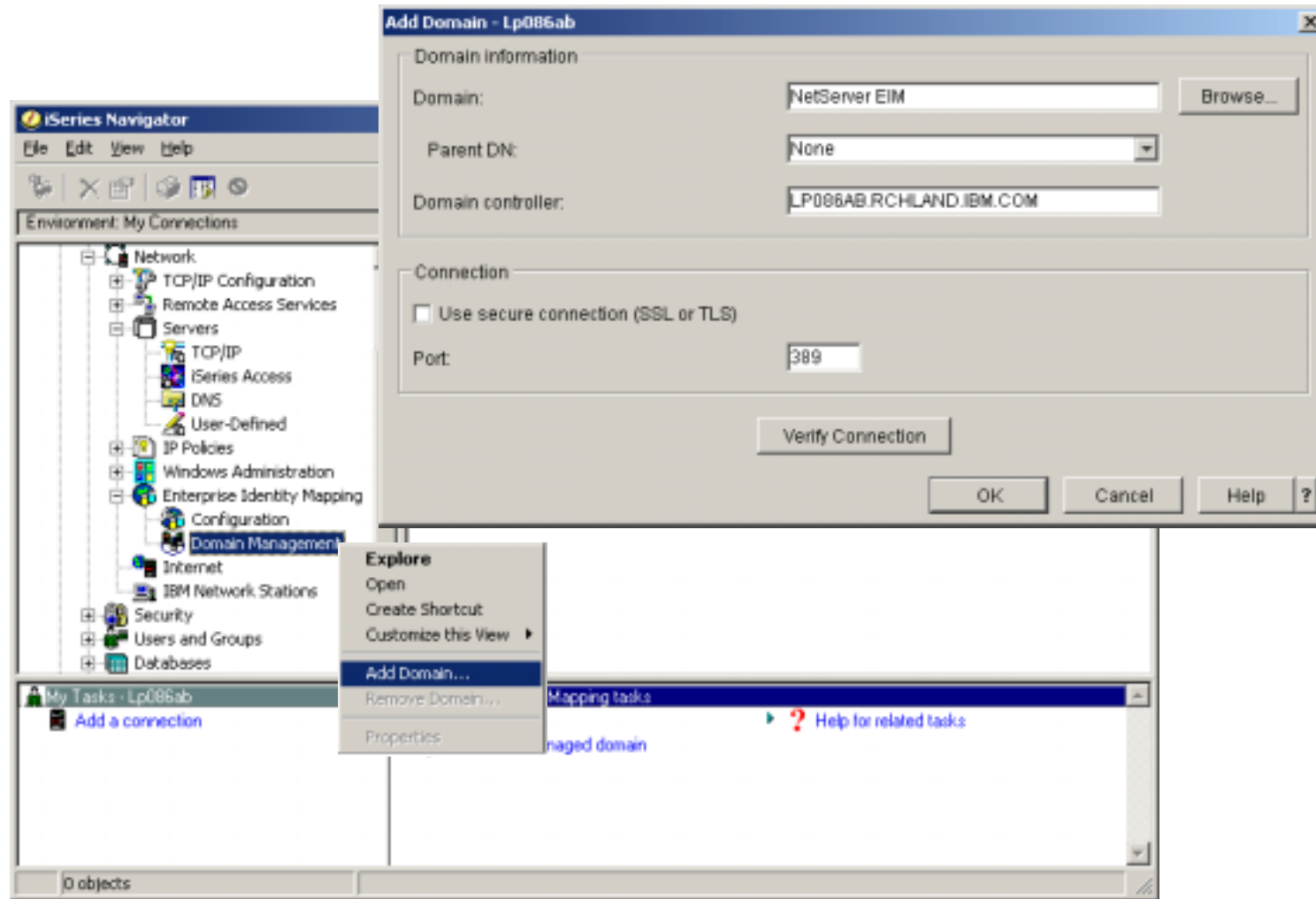
Configuring EIM

- ▶ Access the EIM configuration wizard through iSeries Navigator
 - Network | Enterprise Identity Mapping | Configuration
 - Right click and choose **Configure...**



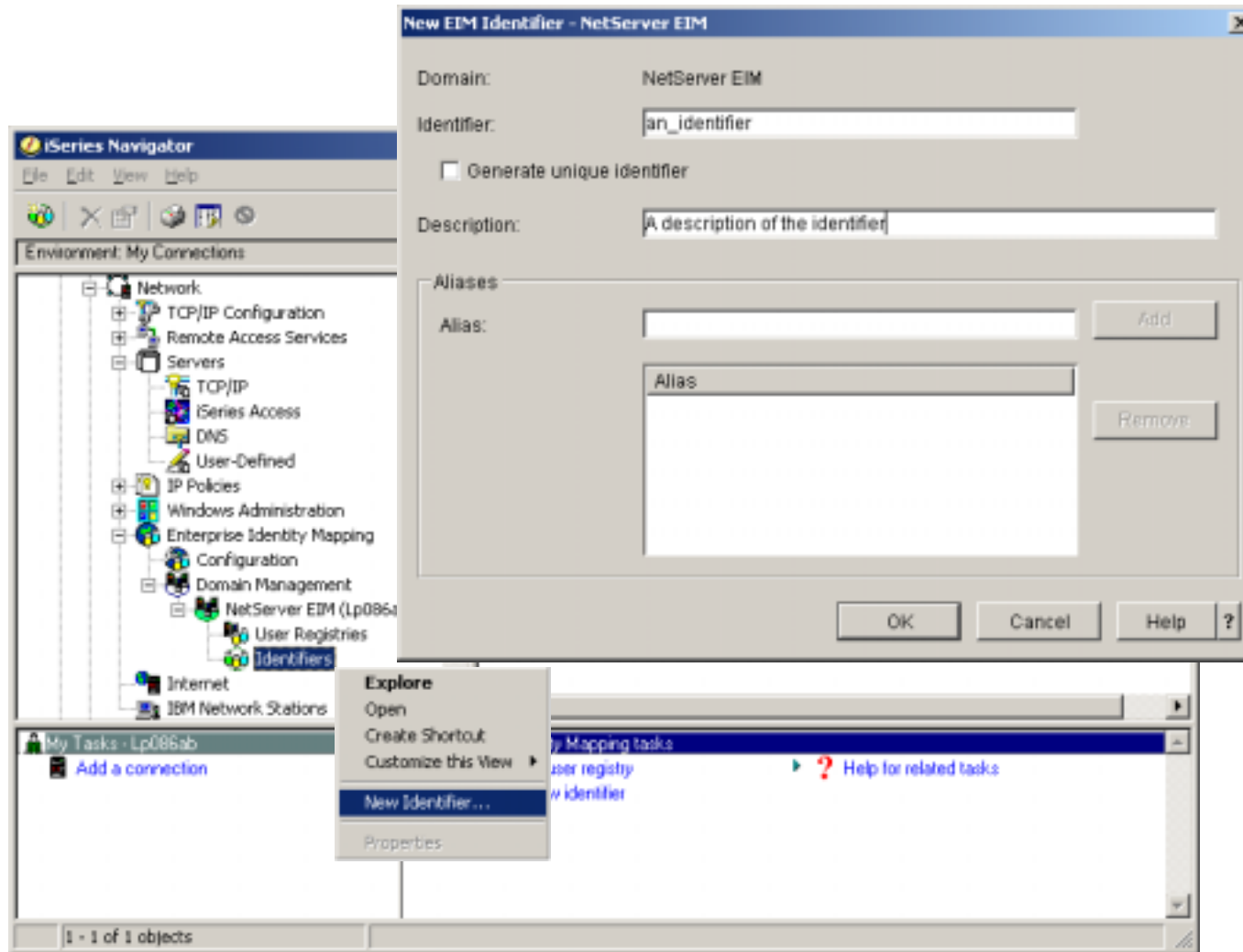
Kerberos Authentication Support

Configuring EIM - Adding the New Domain



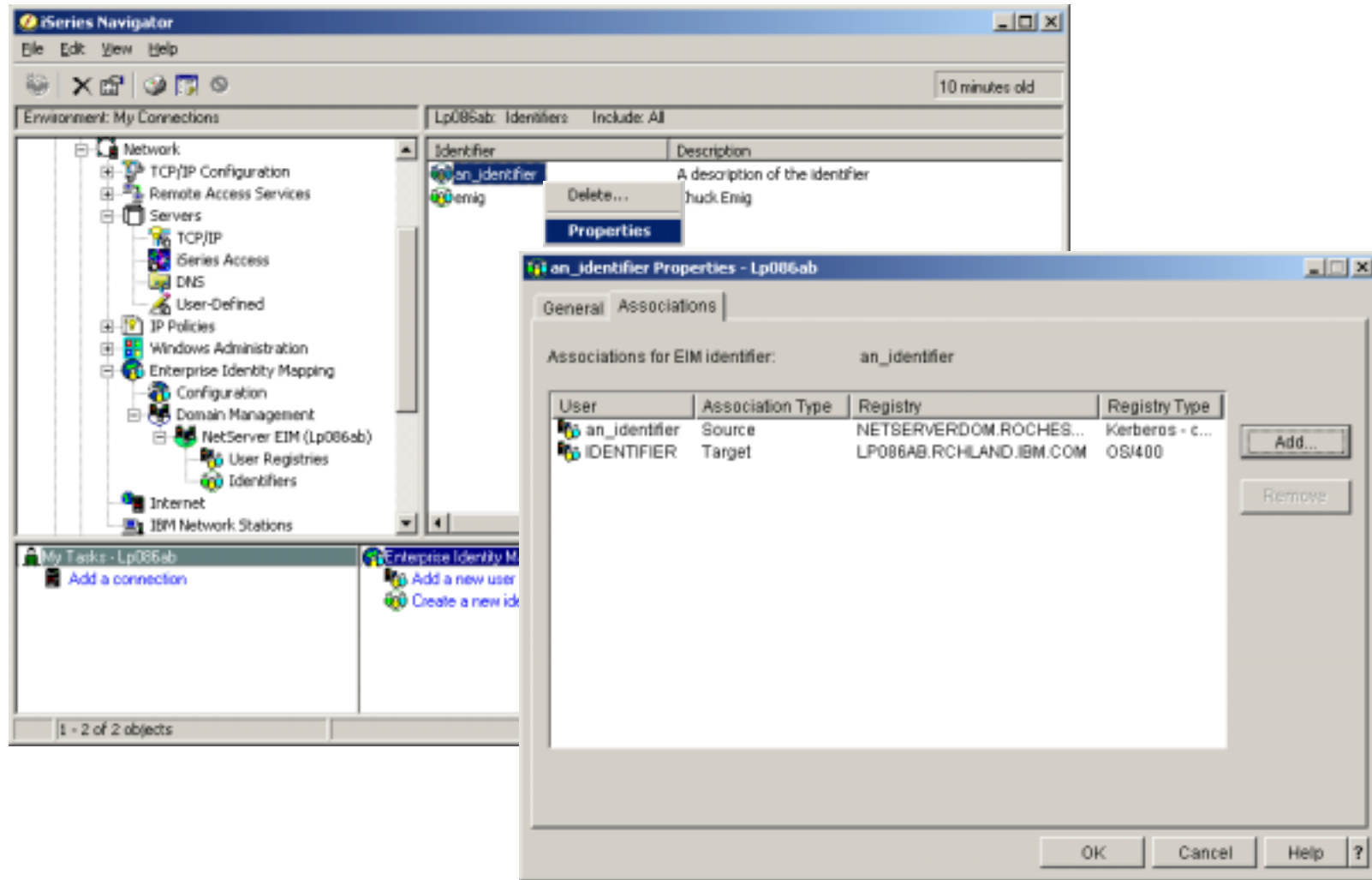
Kerberos Authentication Support

Configuring EIM - Adding Identifiers



Kerberos Authentication Support

Configuring EIM - Adding Associations



Kerberos Authentication Support

Configuring a Windows Domain Controller

- ▶ Add a new user to the Active directory
 - Start | Programs | Administrative Tools | Active Directory Users and Computers
 - Action | New | User

- ▶ Map the new user to an iSeries NetServer service principal name

- From a command prompt, issue one of the following commands:

ktpass -princ HOST/<name>@<REALM> -mapuser <user> -pass *

ktpass -princ cifs/<name>@<REALM> -mapuser <user> -pass *

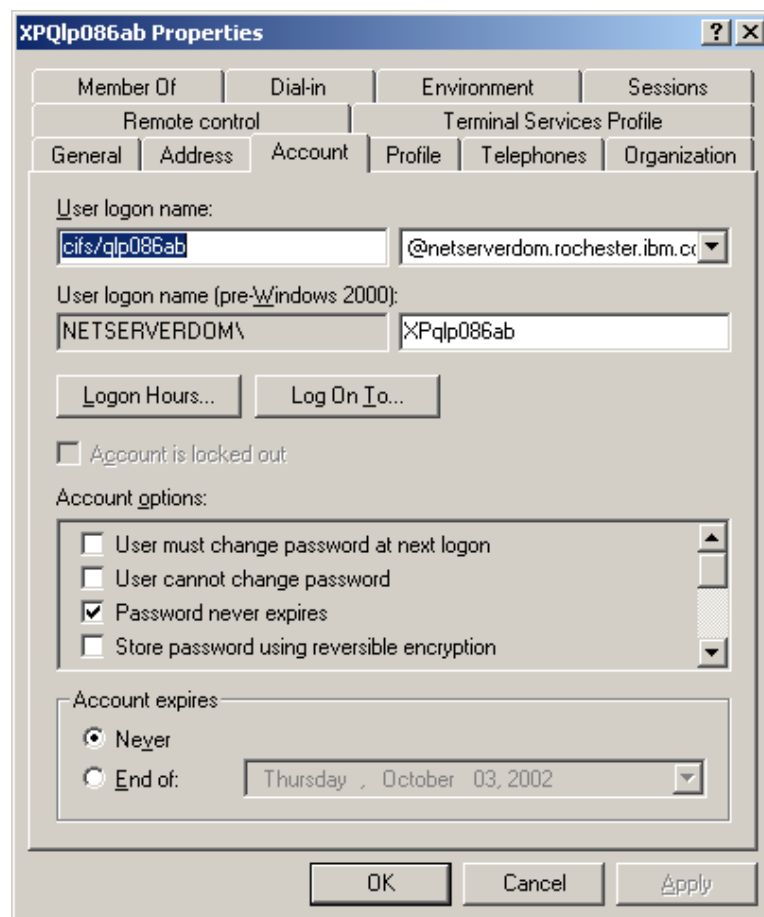
In the above commands,

- <name> = The DNS name of your iSeries, the NetServer name, or the IP address of your iSeries
 - <REALM> = The name of your Kerberos realm
 - <user> = The name of the Active directory user created above
 - Specifying * for the password cause the command to prompt for the password
 - The password used here should match the one used in the Network Authentication wizard
 - HOST should be used if Windows 2000 clients exist in the network
 - cifs should be used if Windows XP clients exist in the network
- Repeat the steps for each name that will be used to access iSeries NetServer
 - Networks with both Windows 2000 and Windows XP clients will need to add both forms of the principal names

Kerberos Authentication Support

Verifying that the Windows Principals are Correctly Configured

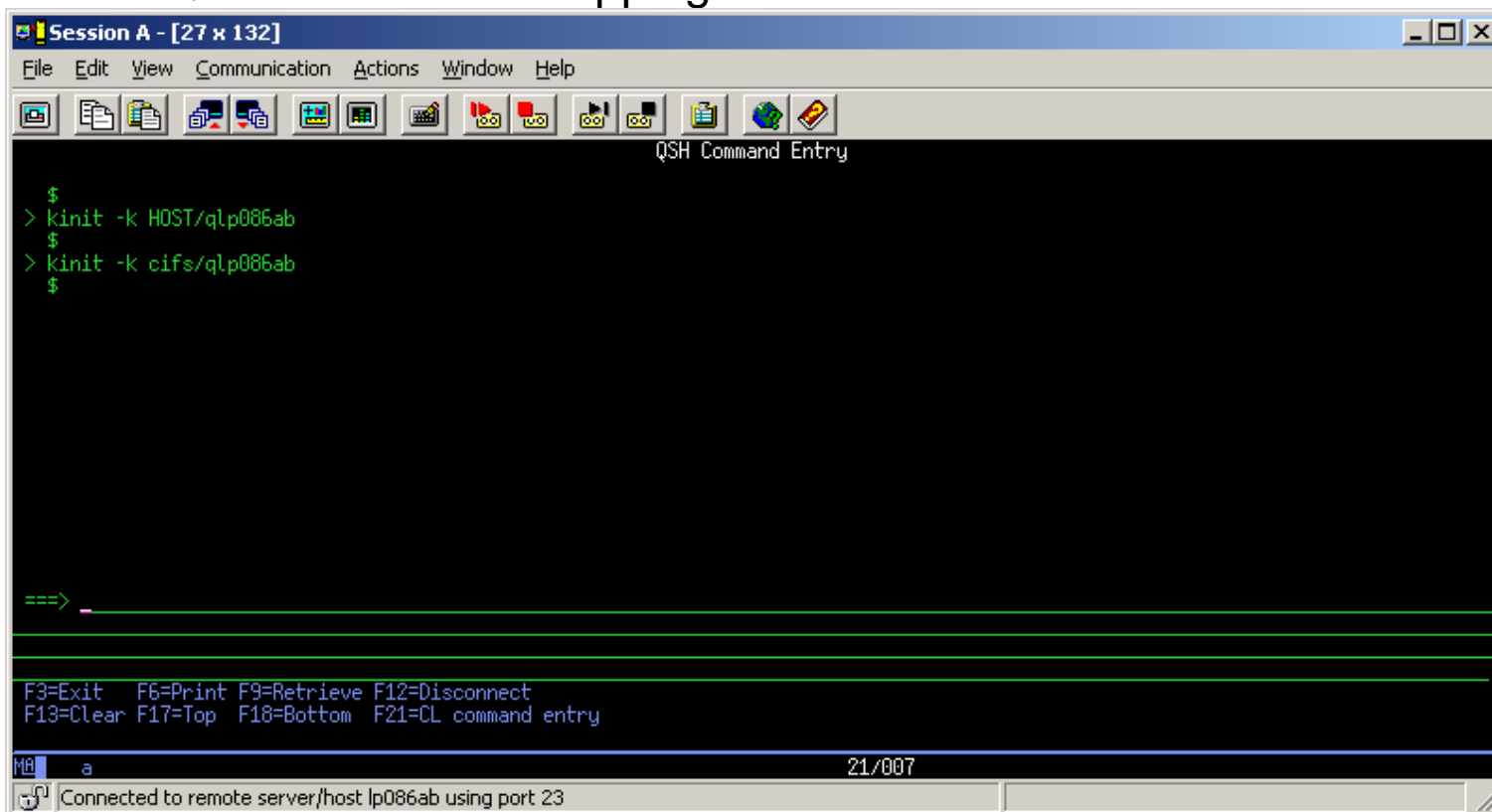
- View the Account tab in the user properties



Kerberos Authentication Support

Verifying that the Windows Principals are Correctly Configured

- Use Qshell to test the mappings



The screenshot shows a Qshell terminal window titled "Session A - [27 x 132]". The window has a menu bar with "File", "Edit", "View", "Communication", "Actions", "Window", and "Help". Below the menu bar is a toolbar with various icons. The main area is a black terminal with green text. The text shows the following commands and their outputs:

```
$  
> kinit -k HOST/qlp086ab  
$  
> kinit -k cifs/qlp086ab  
$
```

Below the terminal area, there is a status bar with the text "====>". At the bottom of the window, there is a footer with the text "F3=Exit F6=Print F9=Retrieve F12=Disconnect F13=Clear F17=Top F18=Bottom F21=CL command entry" and "21/007". The status bar at the very bottom shows "MA a" and "Connected to remote server/host lp086ab using port 23".

- ✈ If Qshell is not available, use the following command structure:
CALL QKRBKINIT PARM('-k' 'HOST/<name>')

Kerberos Authentication Support

The image displays two overlapping windows from the IBM iSeries NetServer configuration utility. The background window, titled "iSeries NetServer General Next Start - Lp086ab", shows the "General" tab with the following settings: "Start when TCP/IP is started" is checked; "Server name" is "QLP086AB"; "Allow iSeries NetServer access using the system name" is checked; "Domain name" is "NETSERVERDOM"; "Description" is "iSeries"; "Logon server role" is set to "None"; and "Authentication method" is set to "Kerberos v5". A "Reset to Current" button and "OK", "Cancel", and "Help" buttons are at the bottom.

The foreground window, titled "iSeries NetServer Configuration Wizard - Lp086ab", shows the "Authentication" step. It features an icon of a server and a question: "Which authentication method would you like to use?". Two radio buttons are present: "Encrypted passwords" (unselected) and "Kerberos v5" (selected). A note below reads: "Note: Kerberos authentication should be used with networks containing only Windows 2000 or newer iSeries NetServer clients. Windows 95/98/ME/NT clients will not be able to connect to iSeries NetServer if Kerberos authentication is enabled." At the bottom of this window are "Back", "Next", "Finish", and "Cancel" buttons. A large green double-headed arrow points from the "Kerberos v5" radio button in the foreground window to the "Kerberos v5" dropdown menu in the background window.

V5R2 User Defined Subsystem Support

User Defined Subsystem Support

Why?

- Ability to separate connections from different clients into separate subsystems

- ▶ Example:

An IT Manager can control which subsystem each group of users will run in. The manager can create separate subsystems for each division of the company. Then using iSeries Navigator the manager configures each division's PC's to connect to a different subsystem. Then he can find a particular user's file server job easier, because he will only have to look in the subsystem for that division.

When the manager needs to restrict access to the system due to a problem or maintenance, he can end that subsystem without impacting the other divisions' operations. Other clients could continue to work without any errors.

- Ability to separate iSeries NetServer jobs from other protocols
 - ▶ PTFs can be applied for a single protocol without affecting others
 - iSeries NetServer
 - File server
 - Database server

User Defined Subsystem Support

Setup

- ▶ **Create the subsystem description to be used by the iSeries NetServer QZLSFILE jobs**
 - CRTSBSD SBSD(QSYS/NETSVR01) POOLS((1 *BASE))
TEXT('NetServer Subsystem')
- ▶ **Add the required prestart jobs to the subsystem description**
 - ADDPJE SBSD(QSYS/NETSVR01)
PGM(QSYS/QZLSFILE) CLS(QSYS/QPWFSEVER)
- ▶ **Start the subsystem**
 - STRSBS SBSD(QSYS/NETSVR01)

User Defined Subsystem Support

Enabling the Support

The screenshot shows the iSeries Navigator interface with the 'iSeries NetServer' service selected in the 'Servers' tree. A context menu is open over the service, with 'Properties' highlighted. The 'iSeries NetServer Properties - Lp086ab' dialog box is open, showing the 'Subsystems' tab. The 'All clients' radio button is selected, and the 'Subsystem' dropdown is set to 'NETSVR01'. The 'Alternate action' dropdown is set to 'Start in current subsystem'. Below these options is a table for defining client-specific subsystems.

| Client | Description | Subnet Mask | Subsystem |
|--------|-------------|-------------|-----------|
| | | | |

Buttons for 'Add', 'Edit', and 'Remove' are located to the right of the table. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

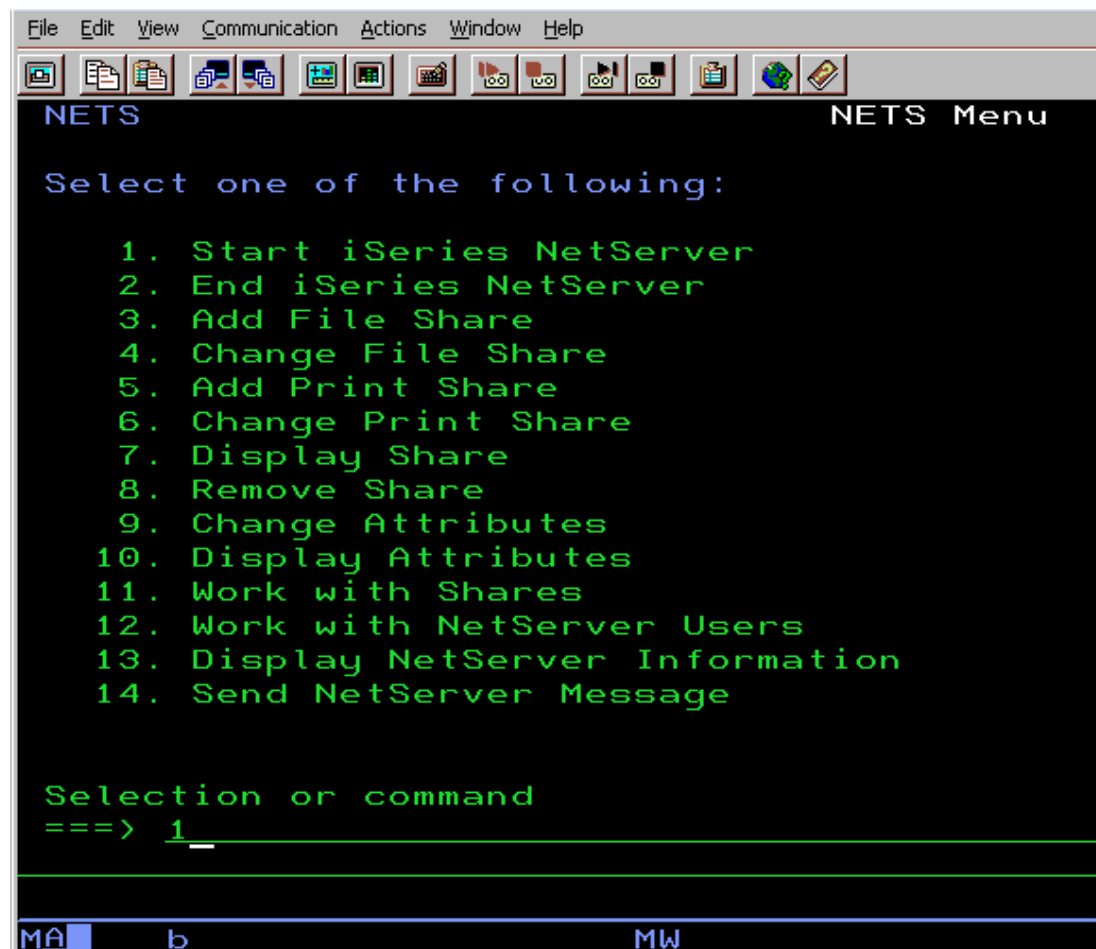
Displays the properties of the selected items.

V5R2 GO NETS

GO NETS

Administration Power on a Green Screen

- Provides menu driven use of iSeries NetServer APIs
- Shipped in the QUSRTOOL library in V5R2



The screenshot shows a green screen interface for the NETS menu. At the top, there is a menu bar with options: File, Edit, View, Communication, Actions, Window, and Help. Below the menu bar is a toolbar with various icons. The main area of the screen displays the following text:

```
NETS                                     NETS Menu

Select one of the following:

  1. Start iSeries NetServer
  2. End iSeries NetServer
  3. Add File Share
  4. Change File Share
  5. Add Print Share
  6. Change Print Share
  7. Display Share
  8. Remove Share
  9. Change Attributes
 10. Display Attributes
 11. Work with Shares
 12. Work with NetServer Users
 13. Display NetServer Information
 14. Send NetServer Message

Selection or command
===> 1_
```

At the bottom of the screen, there is a status bar with the text "MA b MW".

GO NETS

Setting up GO NETS

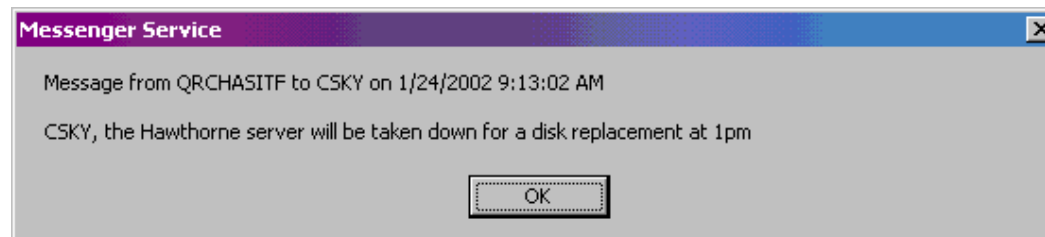
- Follow these example steps to build the GO NETS command tool into library NETSRVCMD.
 1. Create the target library. NETSRVCMD may be replaced with the library name of your choice.
 - CRTLIB LIB(NETSRVCMD) TEXT('iSeries NetServer menu and commands')
 2. Expand the necessary files:
 - CALL QUSRTOOL/UNPACKAGE PARM('*ALL ' 1)
 3. Create the installation program:
 - CRTCLPGM NETSRVCMD/TZLSINST QUSRTOOL/QATTCL
 4. Call the installer to create the GO NETS tool:
 - CALL NETSRVCMD/TZLSINST NETSRVCMD
 5. Add the new library to the library list:
 - ADDLIBLE NETSRVCMD
 6. Run the tool's menu interface. From now on, you need only type this command to bring up GO NETS function.
 - GO NETS

V5R2 Windows Popup Messaging Support

Windows Popup Messaging

Why?

- ▶ iSeries NetServer clients do not usually report meaningful error messages for the following problems:
 - The user profile does not exist
 - The user profile is disabled
 - The user is disabled for iSeries NetServer access
 - The password is expired
 - The user profile does not have a password
 - There was a Kerberos authentication failure
- ▶ Can be used to send administrative alerts
 - **Example:** SNDNSVMSG MSG('&1, the Hawthorne server will be taken down for a disk replacement at 1pm') TONETID((*ALLNSVCNN))
 - ★ This command is part of the QUSRTOOL support
 - The command will send popup messages to all active iSeries NetServer users
 - The &1 can be used to indicate the user name for replacement text in the message



Windows Popup Messaging

Popup Messages

- ▶ **CPIB68A** (Severity 40)
 - CPIB68A: No user profile found for user &1.
- ▶ **CPIB68B** (Severity 40)
 - CPIB68B: The profile for user &1 is disabled.
- ▶ **CPIB68C** (Severity 40)
 - CPIB68C: The password for user &1 is expired.
- ▶ **CPIB68D** (Severity 40)
 - CPIB68D: No password exists for user &1.
- ▶ **CPIB68E** (Severity 40)
 - CPIB68E: User &1 is disabled for iSeries NetServer access.
- ▶ **CPIB68F** (Severity 20)
 - CPIB68F: User &1 was enabled for iSeries NetServer access.
- ▶ **CPIB690** (Severity 20)
 - CPIB690: Password for user &1 will expire in &2 day(s).
- ▶ **CPIB691** (Severity 10)
 - CPIB691: User &1 has successfully connected.
- ▶ **CPIB692** (Severity 40)
 - CPIB692: User &1 encountered Kerberos error &2 connecting through iSeries NetServer.

Windows Popup Messaging

Client Setup

- On Windows NT/2000/XP:
 1. Open Services from Administrative Tools. This is found off the Control Panel in Windows 2000/XP.
 2. Scroll down to find Messenger. Ensure that the status is Started and the Startup type is Automatic.
- On Windows 9x/Me:
 - ▶ You must have Winpopup.exe installed. If it is not installed, follow these instructions to install it:
 1. In Control Panel, double-click Add/Remove Programs.
 2. On the Windows Setup tab, click Accessories, and then click Details.
 3. Click the WinPopup check box to select it, and then click OK.
 4. Click OK.
 - ▶ Once the program is installed, follow these steps to start it:
 1. Open the Start Menu
 2. Select Run
 3. Enter the program name, winpopup.exe, and click OK.

Windows Popup Messaging

Client Setup

■ On Linux:

1. You need to enable Samba's messenger support. Edit the smb.conf file so that it contains a "message command" directive. The following is an example line:
message command = /bin/bash -c 'echo -e "WinPopup Message from %f on \$(date): \n" >> /tmp/msg.txt; cat %s >> /tmp/msg.txt; echo -e "\n\n" >> /tmp/msg.txt; rm %s'
2. Restart the Samba server. For example (on Red Hat): /etc/rc.d/init.d/samba restart
3. Create a shell script that can read the /tmp/msg.txt file and pop the messages into a window in the background. The following is an example bash script:

```
#!/bin/bash
```

```
# Run this script in the background to display a message window where WinPopup  
# messages are displayed in sequence. Samba must be started and smb.conf must  
# be configured to append messages to /tmp/msg.txt
```

```
# remove old messages  
rm /tmp/msg.txt  
touch /tmp/msg.txt  
chmod 666 /tmp/msg.txt
```

```
rxvt -fb -sb -fn lucidasanstypewriter-bold-14 -sl 2048 -bg red -fg white -title "SMB Network Messages" -geometry 80x10+150+280  
-e tail -f /tmp/msg.txt
```

Note: This script creates an rxvt window. If you don't have rxvt installed or would rather use an xterm window, substitute xterm instead.

4. Save the script as tailmsg.sh, make it executable, and run it in the background: ./tailmsg.sh &

iSeries Setup and Use

- Change the message logging severity of the QZLSSERVER job
 - ▶ CHGJOB JOB(QZLSSERVER) LOG(4 20 *NOLIST)
- Displaying a Log of the Message Send Attempts
 - ▶ You may use the iSeries NetServer maintenance program at your own risk to display a log of network messages that the server attempted to send. The log contains a maximum of the last 500 messages (by default), and when the log is dumped, those messages are purged. This means that you will only see the network messages since the last time that they were dumped. Here is how you call the maintenance utility:
 - CALL PGM(QZLSMAINT) PARM('32')
 - ▶ The log is dumped into a QPCSMPT spool file for the QSECOFR user profile. Use the Work with Spooled Files (WRKSPLF) command to display the queue:
 - WRKSPLF QSECOFR
 - ▶ Example spool file dump of logged messages:

| TIME | NAME | IP-ADDR | TYPE | RC | MESSAGE |
|------------------|----------|----------|------|----|--|
| 1/23/02 17:39:55 | SMBTEST1 | C0050939 | 2 | 0 | CPIB68B: THE PROFILE FOR USER SMBTEST1 IS DISABLED. |
| 1/23/02 17:40:16 | CSKY | C005095D | 7 | 0 | CPIB690: PASSWORD FOR USER CSKY WILL EXPIRE IN 3 DAY(S). |

👉 Note: If the RC column is not 0, then there was an error delivering the message to the user

For More Information...

Visit the iSeries NetServer home page for the latest Logon Server help along with iSeries NetServer documentation, usage articles, Info APARs, and PTF information

- ▶ <http://www.ibm.com/servers/eserver/series/netserver/>

Documentation including iSeries NetServer can be found on InfoCenter

- ▶ <http://www.ibm.com/eserver/series/infocenter>

Network Client Information

- ▶ <http://www.neoware.com>
- ▶ <http://www.citrix.com>

Microsoft articles


- ▶ Logon scripts:
 - <http://www.microsoft.com/technet/winnt/winntas/tips/techrep/logscrpt.asp>
- ▶ Profiles and Policies:
 - http://www.microsoft.com/TechNet/winnt/Winntas/technote/Planning/prof_pol.asp
- ▶ Enabling NTLM 2 Authentication for Windows 95/98/2000 and NT:
 - <http://support.microsoft.com/support/kb/articles/Q239/8/69.ASP>

Trademarks and Disclaimers

© IBM Corporation 1994-2003. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

| | | |
|---|------------|-------------------|
| AS/400 | IBM | e (logo) business |
| AS/400e | IBM (logo) | |
| eServer | iSeries | |
|  | OS/400 | |

Lotus and SmartSuite are trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both.

MMX, Pentium, and ProShare are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.

C-bus is a trademark of Corollary, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Kerberos is a trademark of Massachusetts Institute of Technology.

Other company, product or service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information in this presentation concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Contact your local IBM office or IBM authorized reseller for the full text of the specific Statement of Direction.

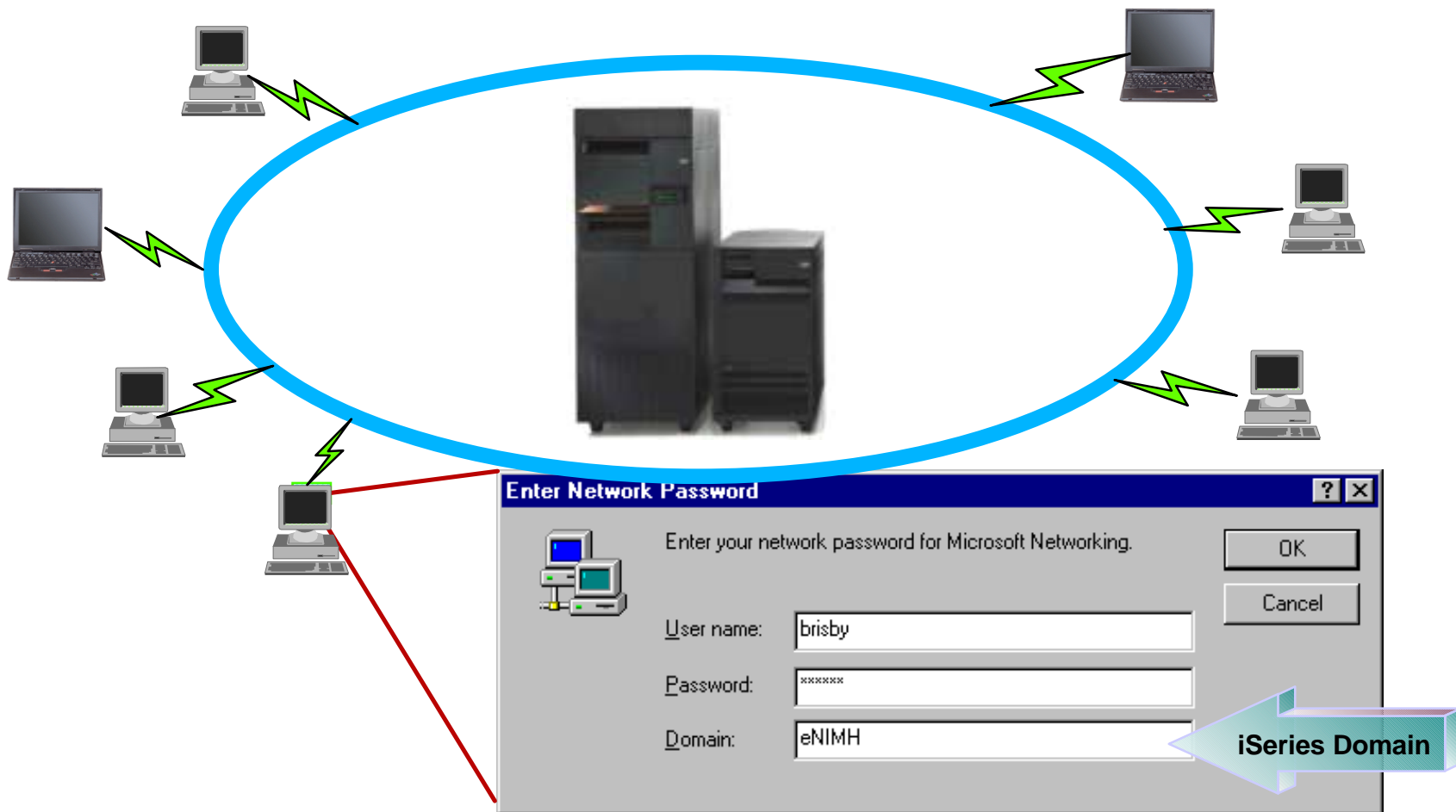
Some information in this presentation addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Photographs shown are of engineering prototypes. Changes may be incorporated in production models.

Domain Logon Support

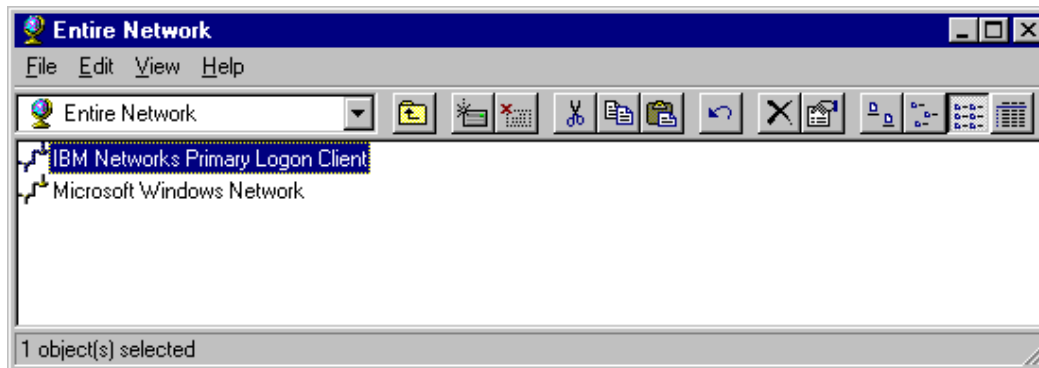
Logon services for Windows 95/98/NT/2000/XP



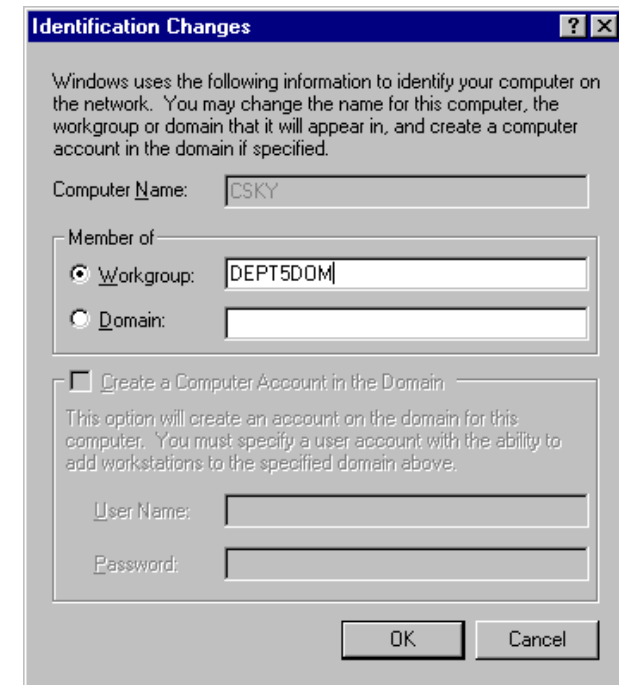
Domain Logon Support

IBM Networks Primary Logon Client

- When installing or configuring properties, it is OK to take the default settings
- You can specify domain name choices that will be available on the logon screen
- IBM Networks Primary Logon Client in Entire Network is only a place-holder
- Typically, the computer will be a member of a workgroup



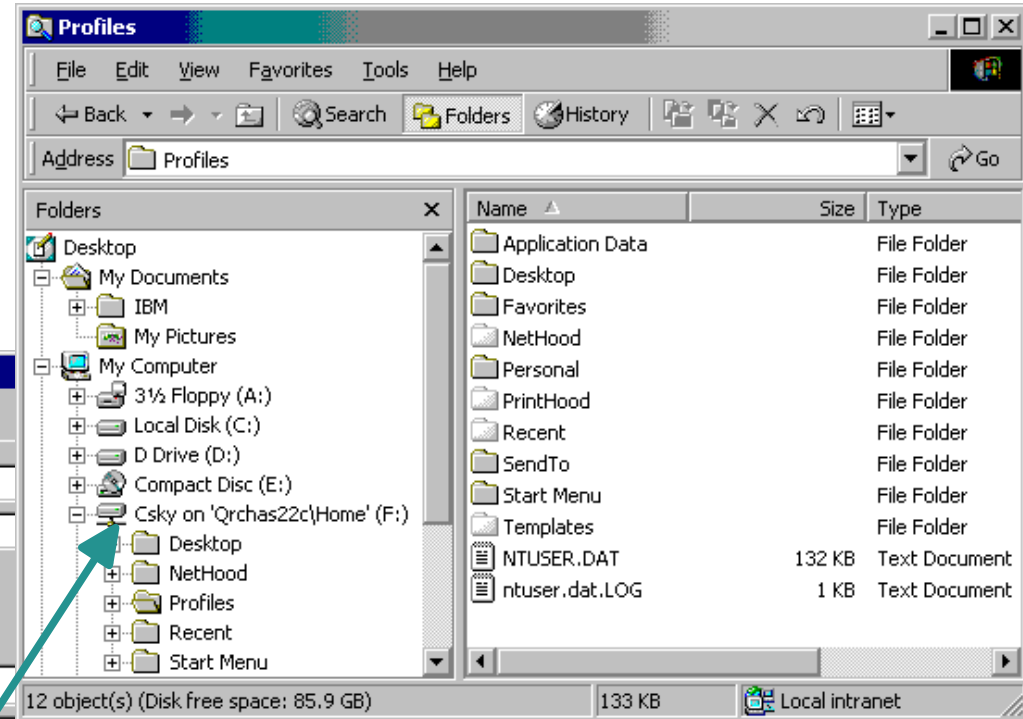
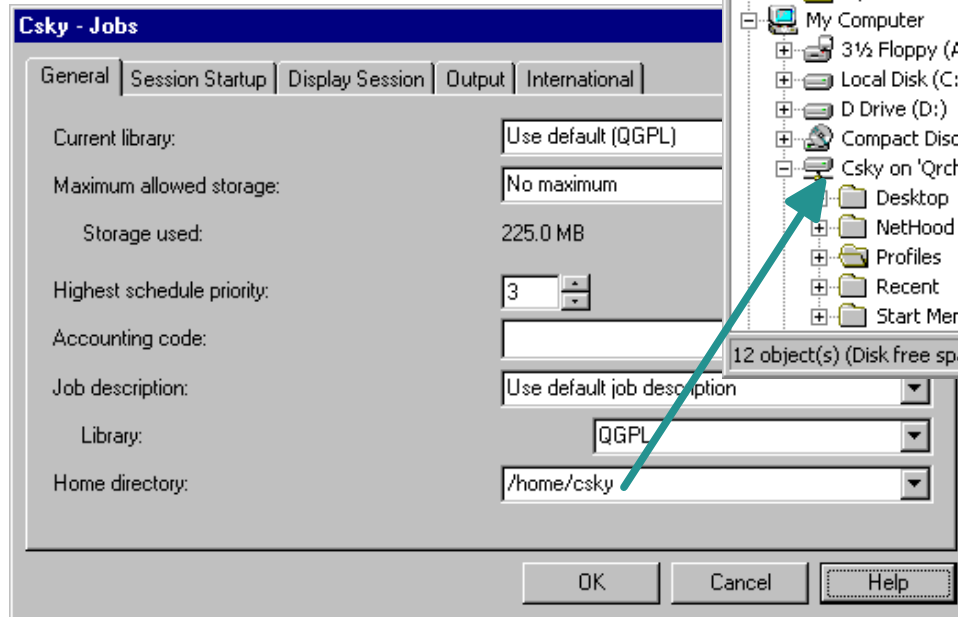
✦ The **IBM Networks Primary Logon Client for Windows NT/2000/XP** can be obtained from the iSeries NetServer homepage. Click [Domain logon support](#), click [IBM Networks Primary Logon Client](#), and scroll to bottom for the registration link.



Domain Logon Support

Home Directories & Windows User Profiles

- The home directory for the Windows user is specified in the iSeries user's profile by default.
- From iSeries Navigator user properties, click the Jobs button to see it.



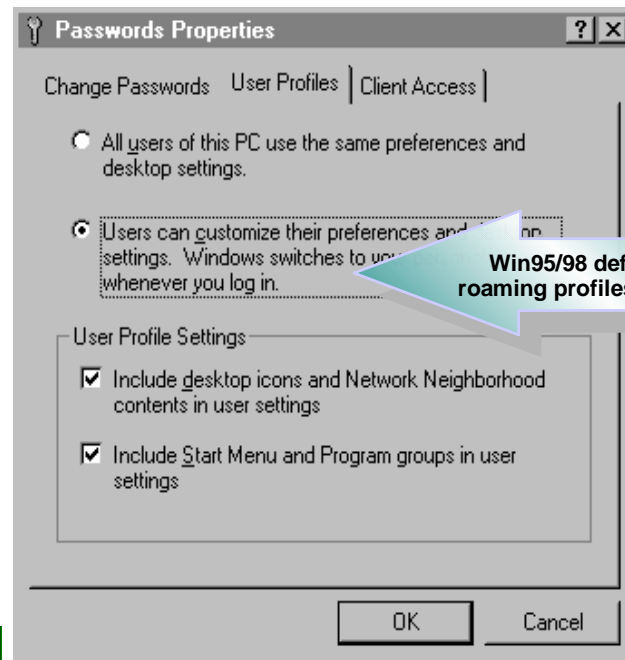
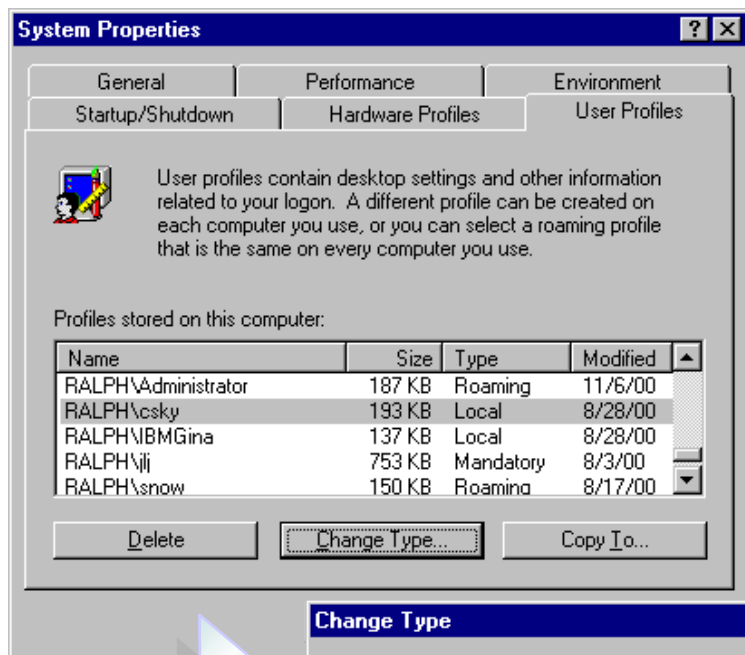
- Windows NT/2000/XP can connect a drive to the home directory automatically during log on.
- By default, roaming user profiles are stored here.

Home directories

- Determined by the logon server
- Must be shared
- Win NT/2000/XP automatically try to connect, Win 9x does not
- Share another directory as HOME (for example) to keep the Windows and iSeries home directories separate
- Win 9x clients can "see" other's home directories
- A share name that is the same name as the user becomes that user's home directory share (override)

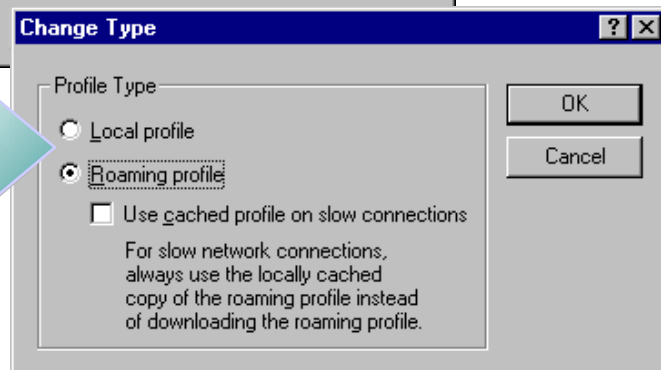
Domain Logon Support

Roaming Profiles



Win95/98 default to use roaming profiles with this set

In Windows NT/2000/XP, must be logged onto domain as administrator to change



Disabling Roaming Users in Windows 95/98 from REGEDIT:

1. Go to HKEY_LOCAL_MACHINE\Network\Logon
2. Choose Edit-->New-->DWORD value
3. Enter the value name of UseHomeDirectory and a data value of 0.

Domain Logon Support

Logon Scripts

What are they?

- ▶ DOS batch files (.bat) that are downloaded and executed by the PC client when a user logs on

Where do they go?

- ▶ They are placed in the NETLOGON share of the Logon Server

Naming conventions?

- ▶ USER.BAT, GROUP.BAT, and QZLSDEFT.BAT

```
REM QZLSDEFT.BAT
REM Sample Logon Script (Win NT/2000/XP)

echo Hello!
echo Welcome to the iSeries NetServer domain.

pause
```

Simple logon script.

Domain Logon Support

Windows System Policy Serving

What are they?

- ▶ Policies are a batch of settings applied to a PC's registry. They are contained in a file called config.POL or NTconfig.POL

How are they created?

- ▶ Use the POLEDIT.EXE utility

Where do they go?

- ▶ Policy files are also placed in the NETLOGON share for Automatic Remote Update

Why use them?

- ▶ To restrict users from certain functions in the OS or applications

Domain Logon Support

iSeries as the Domain Master Browser (DMB)

- iSeries NetServer announces itself to the network as the DMB and PDC
- Maintains the master list of computers sharing resources for the domain
- Maintains a list of reachable domains and can proxy requests to them
- Can merge lists from Master Browsers in other logical subnets

NetBIOS Names example

```

__MSBROWSE__<01>
  IDOM<1B>
  IDOM<1C>
  IDOM<1D>
  IDOM<1E>
  IDOM<00>
CNDORMAN<00>
CNDORMAN<20>

```

BROWSTAT Utility

```

C:\NTRESKIT>browstat status idom

Status for domain idom on transport \Device\NetBT_IBMTRP3
  Browsing is active on domain.
  Master browser name is: CNDORMAN
  Could not connect to registry, error = 53      Unable to determine build of br
  owser master: 53
  \\\CNDORMAN . Version:05.01  Flags: c030b MASTER CONTROLLER
  1 backup servers retrieved from master CNDORMAN
  \CNDORMAN
  There are 1 servers in domain idom on transport \Device\NetBT_IBMTRP3
  There are 3 domains in domain idom on transport \Device\NetBT_IBMTRP3

C:\NTRESKIT>browstat getpdc \Device\NetBT_IBMTRP3 idom
PDC: CNDORMAN

C:\NTRESKIT>

```

Domain Logon Support

Troubleshooting

Most common error messages:

- ✗ "No domain server was available to validate your password..."
- ✗ "The system could not log you on now because the domain X is not available."

What they mean:

- ▶ iSeries NetServer is not configured as a Logon Server for the domain
- ▶ iSeries NetServer conflicts with another Domain Controller
- ★ [The client cannot resolve to the Logon Server](#)
- ▶ The client can resolve to the Logon Server, but future processing confuses it into a resolution failure

What can you do:

- ▶ If datagrams are not being forwarded, keep the clients and the Logon Server in the same subnet if possible
- ▶ Use **WINS** or a compatible name service across your network
- ▶ Change the workgroup of the client PC to a name different from the domain being logged into.

Domain Logon Support

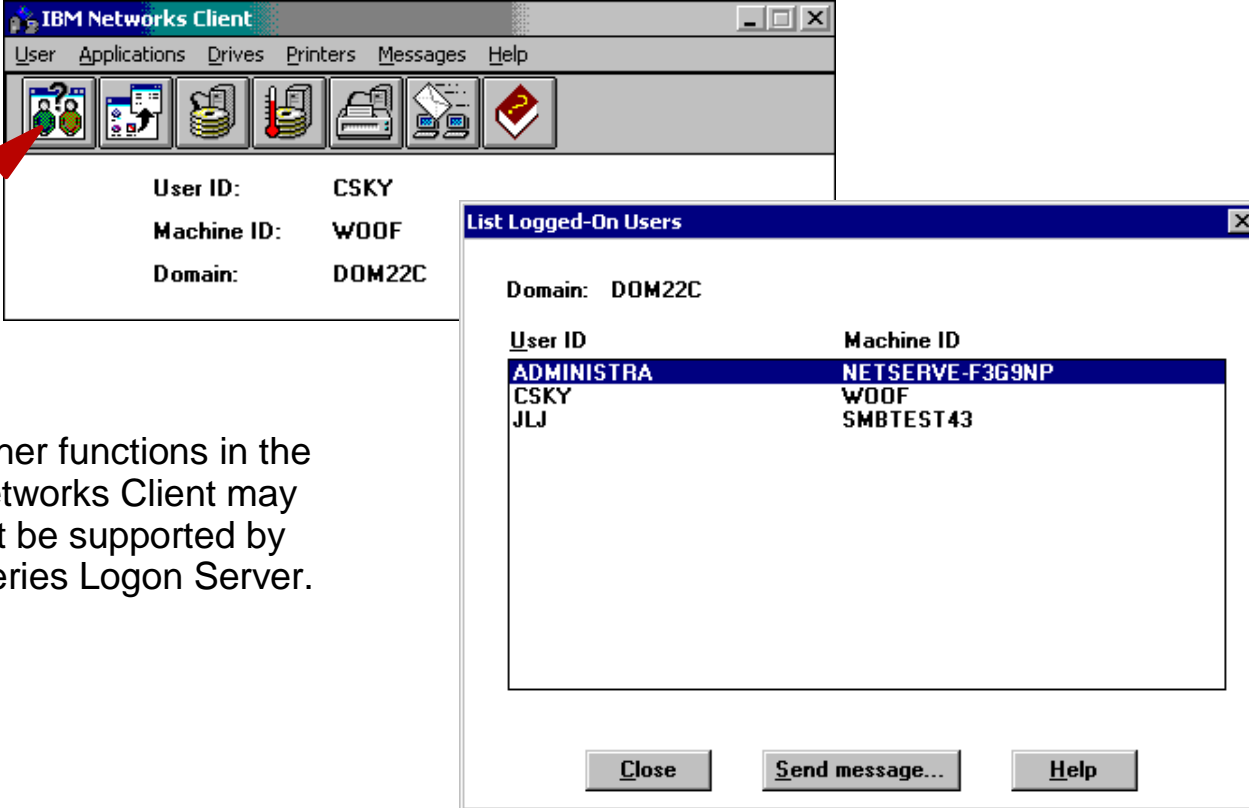
New Informational Messages

- **CPIB687**
 - ▶ An error or conflict occurred with iSeries NetServer. Several reasons are related to Logon support that indicate another machine in the network is in conflict. Informational since Logon Server may still function in most respects. Look at the recovery actions to resolve.

- **CPIB688**
 - ▶ A logon client has requested that a home directory be shared on behalf of a user.

Domain Logon Support

Finding out who logged on



The screenshot shows the IBM Networks Client interface. A red arrow points to the user icon in the top toolbar. Below the toolbar, the following information is displayed:

User ID: CSKY
Machine ID: WOOF
Domain: DOM22C

To the right, a 'List Logged-On Users' dialog box is open, showing the following table:

| User ID | Machine ID |
|------------|-----------------|
| ADMINISTRA | NETSERVE-F3G9NP |
| CSKY | WOOF |
| JLJ | SMBTEST43 |

Below the table are buttons for 'Close', 'Send message...', and 'Help'.

⚡ Other functions in the Networks Client may not be supported by iSeries Logon Server.

👉 Guest users cannot 'log on'