IBM eServer J iSeries J

Session: 409113
41GC

iSeries NetServer: What's New!

http://www.ibm.com/servers/eserver/iseries/netserver/

Vern Yetzer
yetzer@us.ibm.com
September, 2003

Session Objectives

- Awareness of NetServer enhancements in V5R1 and V5R2.
- Understand new authentication support.
- Be able to configure NetServer in a kerberos realm.

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?

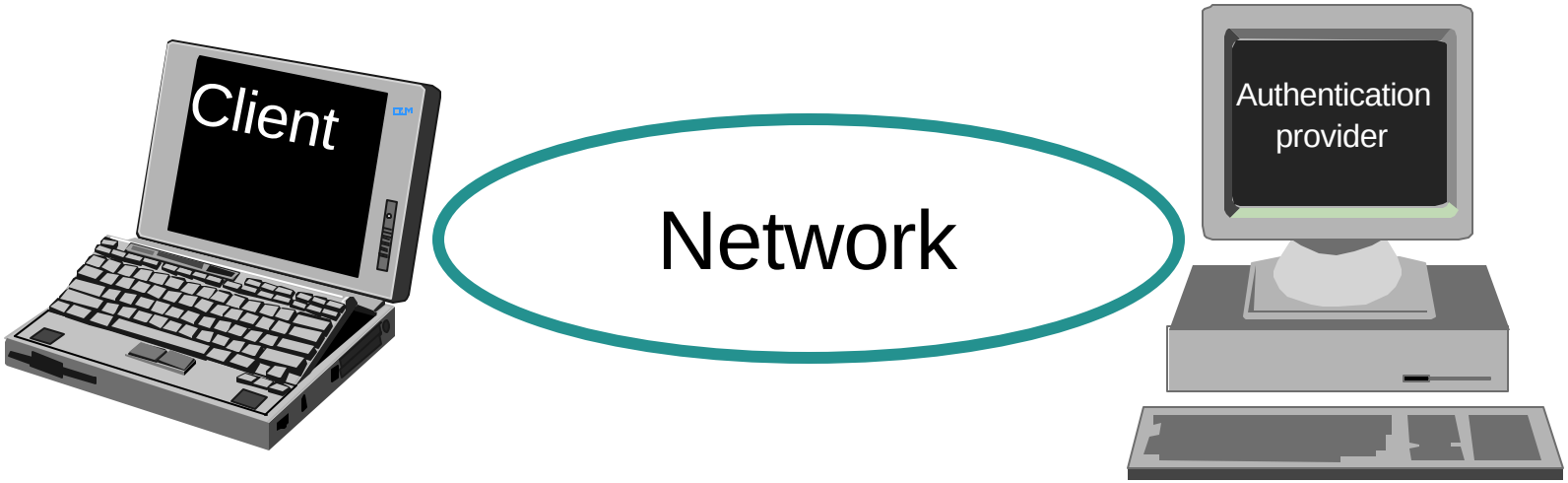
- Support for Kerberos version 5 authentication
- Run file server jobs in subsystems other than QSERVER
- Base support for Linux Samba clients
- Windows popup messages
- QUSRTOOL for menu driven use of iSeries NetServer APIs
- Support for Windows XP Professional

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

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 or 2003 server is required
      - Windows 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

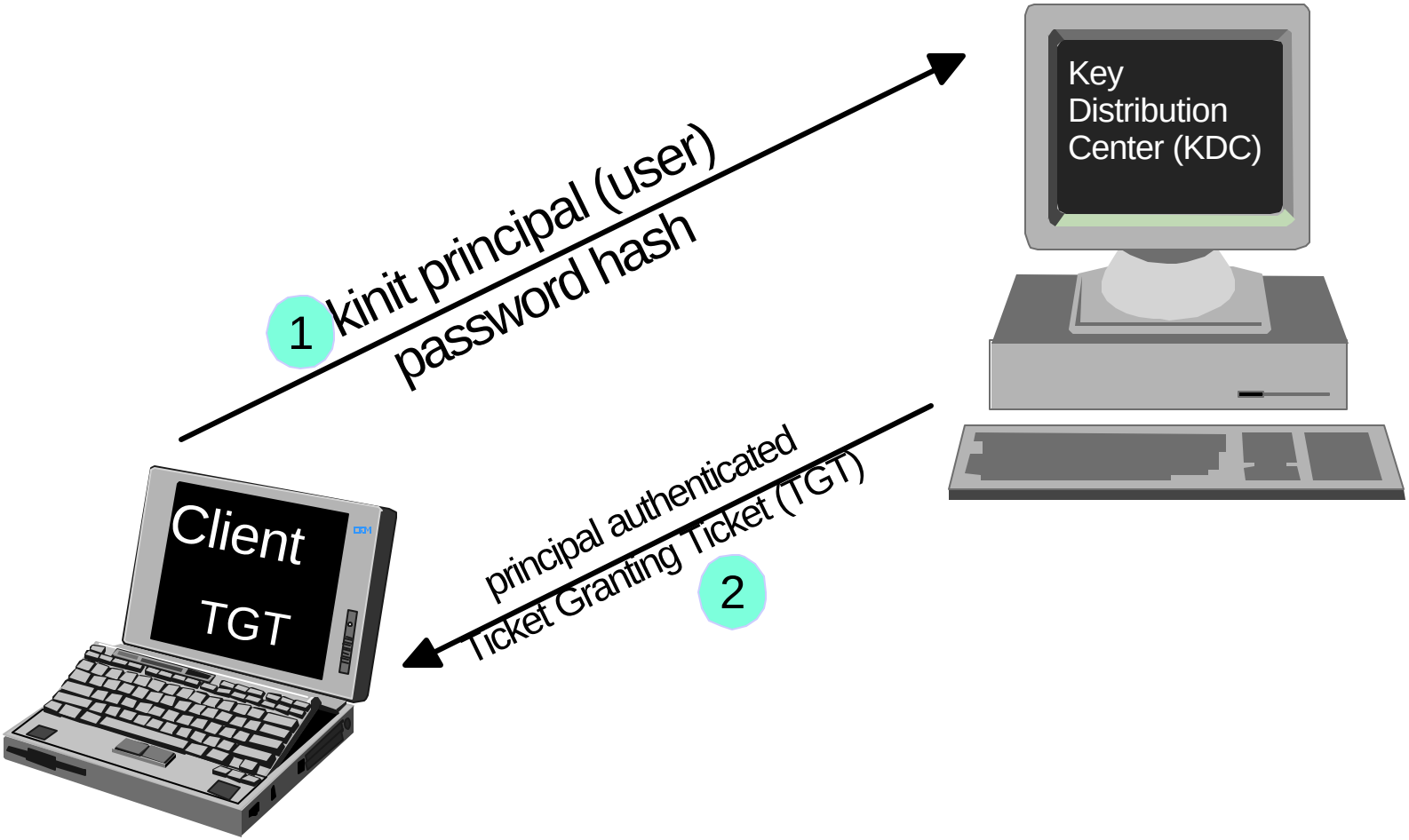
Benefits / Limitations

- 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
  - ✗ Windows 9x/Me/NT clients do not support Kerberos authentication
  - ✗ Supported Samba clients do not currently include Kerberos authentication support

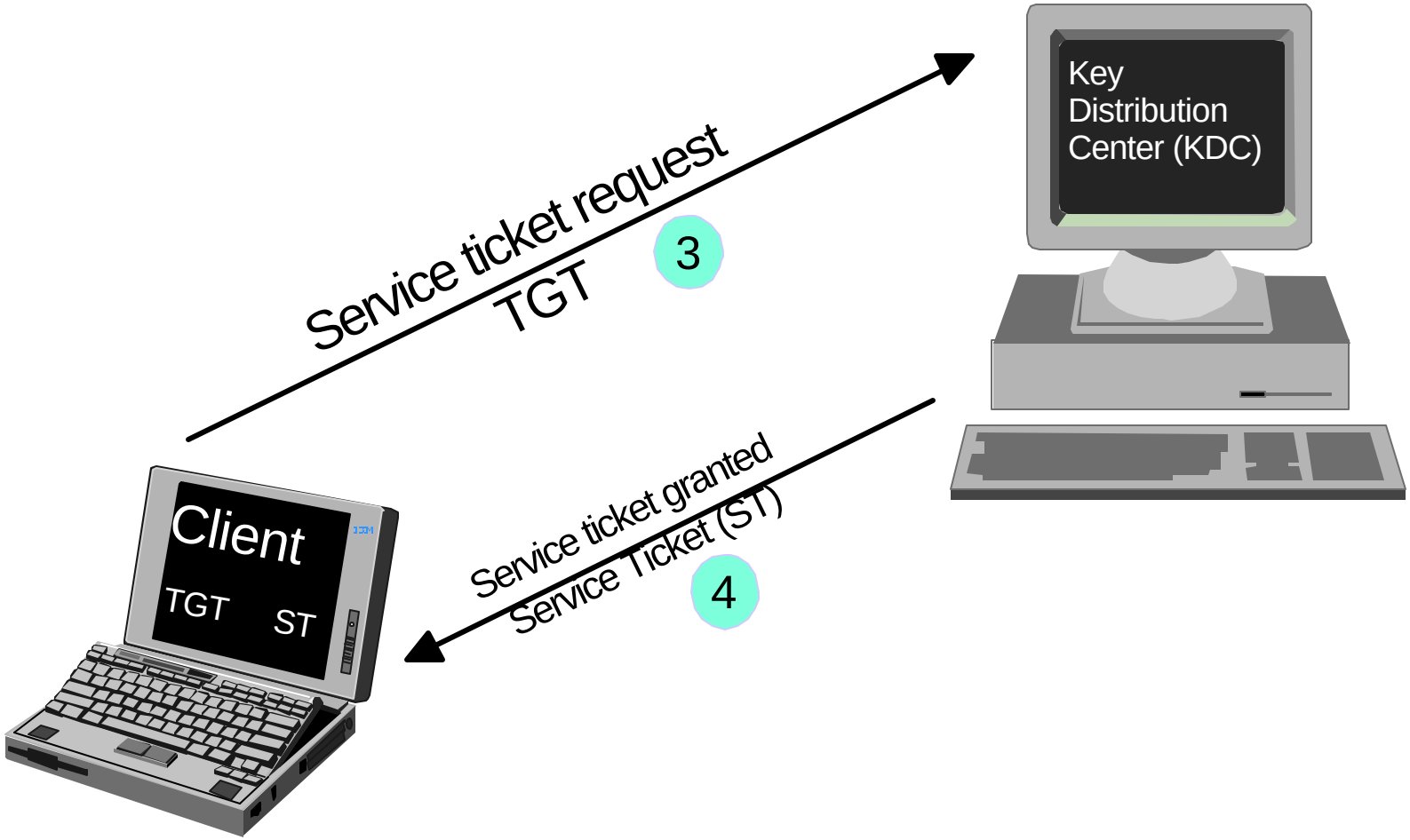
Kerberos Authentication Support

Kerberos Flows - Initial Logon



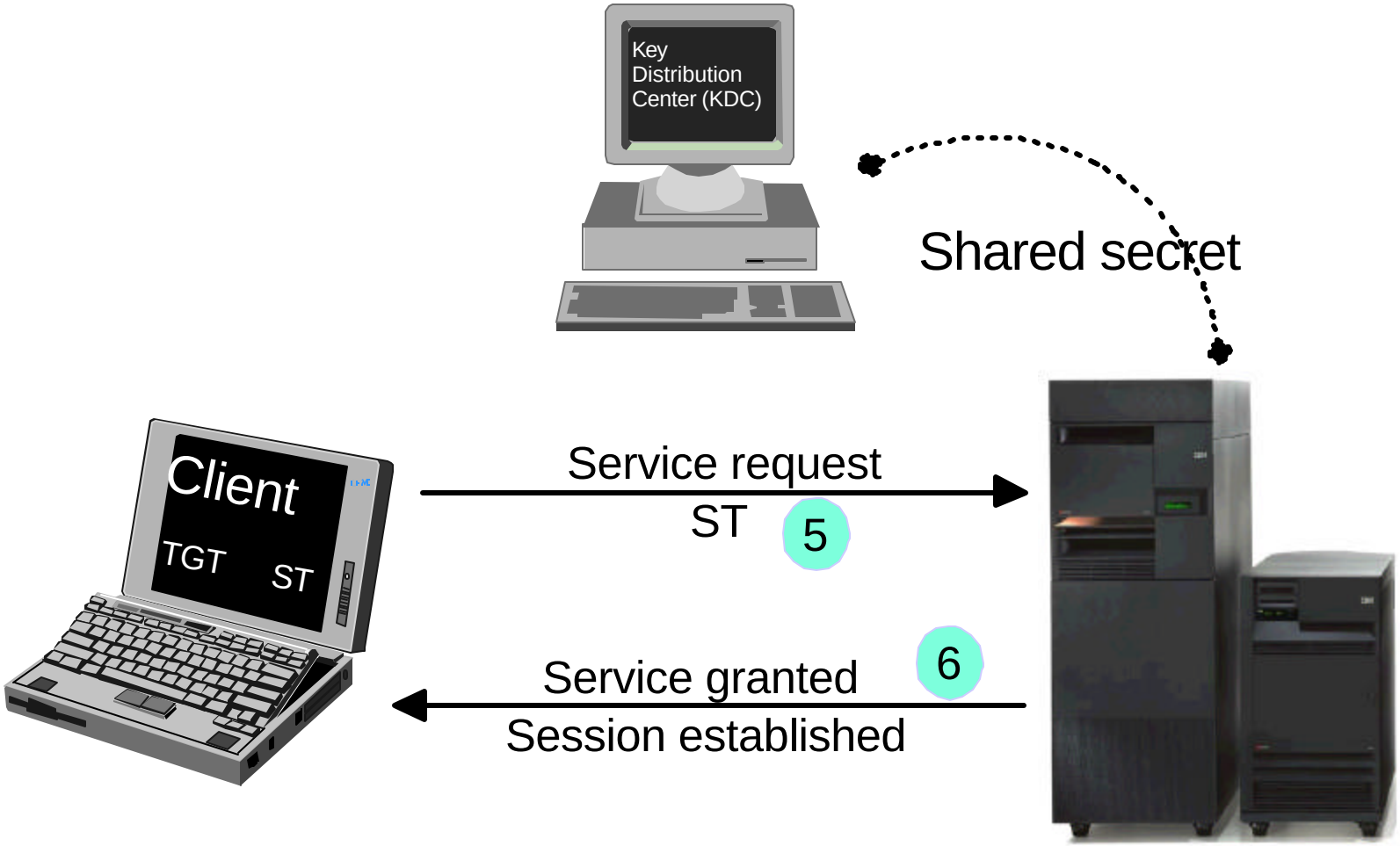
Kerberos Authentication Support

Kerberos Flows - Service Ticket Request



Kerberos Authentication Support

Kerberos Flows - Service Request



Kerberos Authentication Support

Configuration Steps:

- Configure kerberos realm - KDC
- Configure Network Authentication Support
- Configure Enterprise Identity Mapping
- NetServer Configuration

Kerberos Authentication Support - Realm

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 *

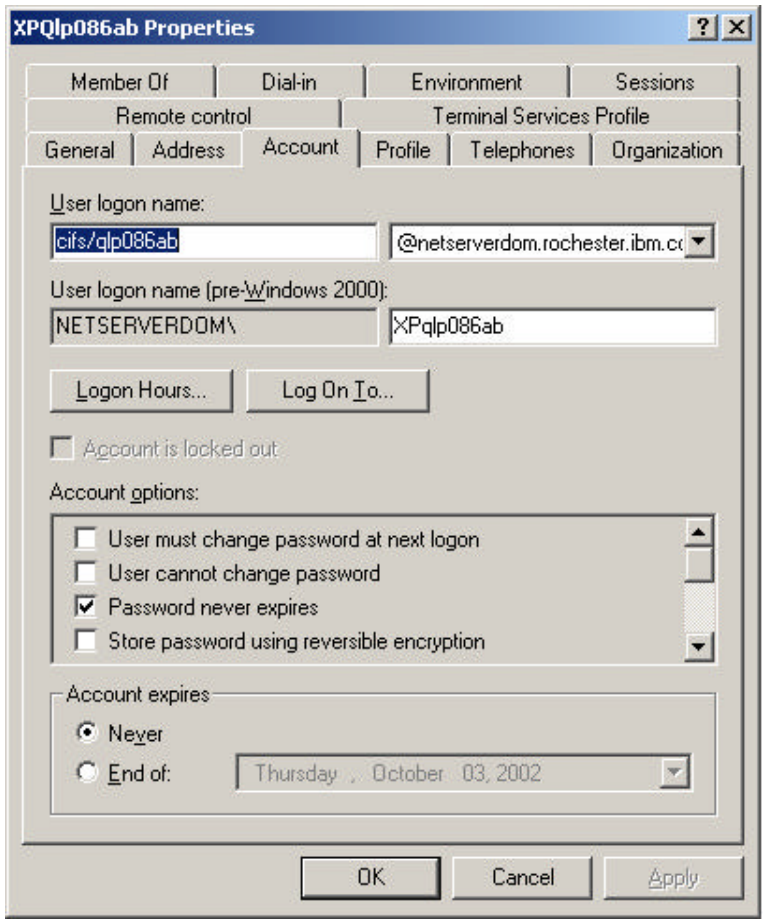
    ktpass -princ cifs/<name>@<REALM> -mapuser <user> -pass *

    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

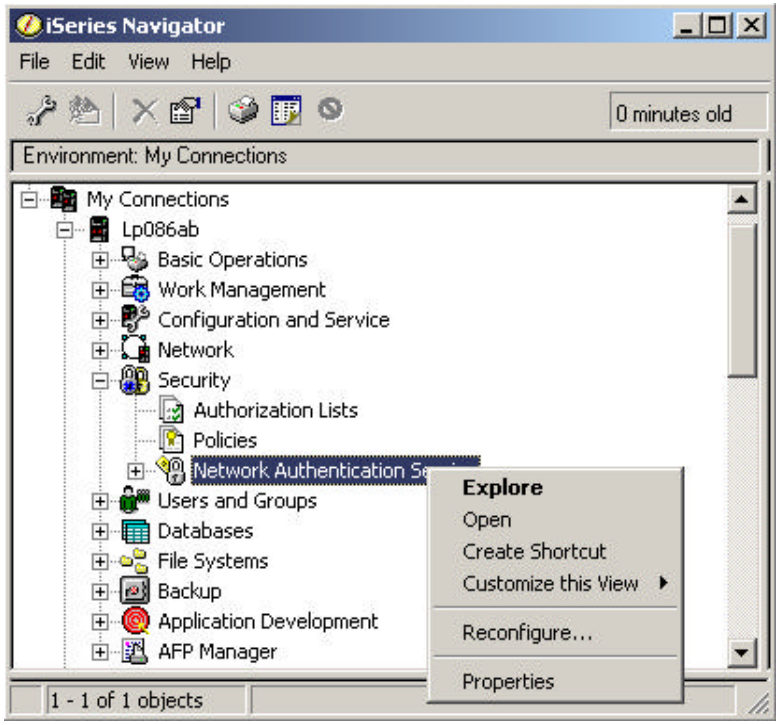
- View the Account tab in the user properties



Kerberos Authentication Support

Configuring Network Authentication Service

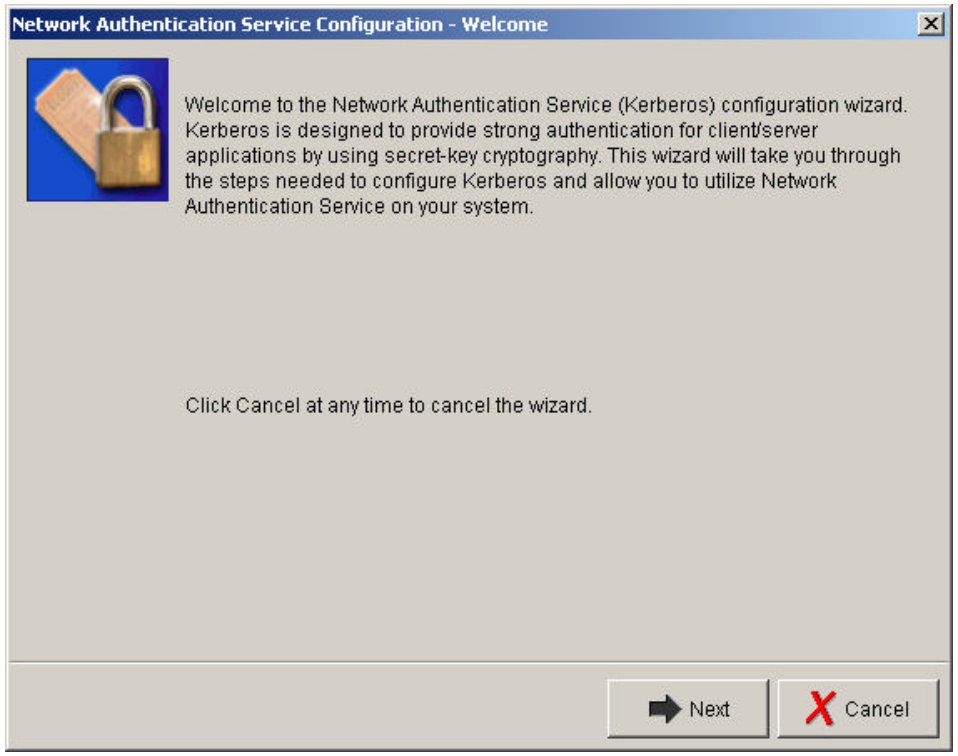
- Configuration iSeries Navigator
  - Security | Network Authentication Service
  - Right click and choose **Configure** or **Reconfigure...**



Kerberos Authentication Support

Configuring Network Authentication Service

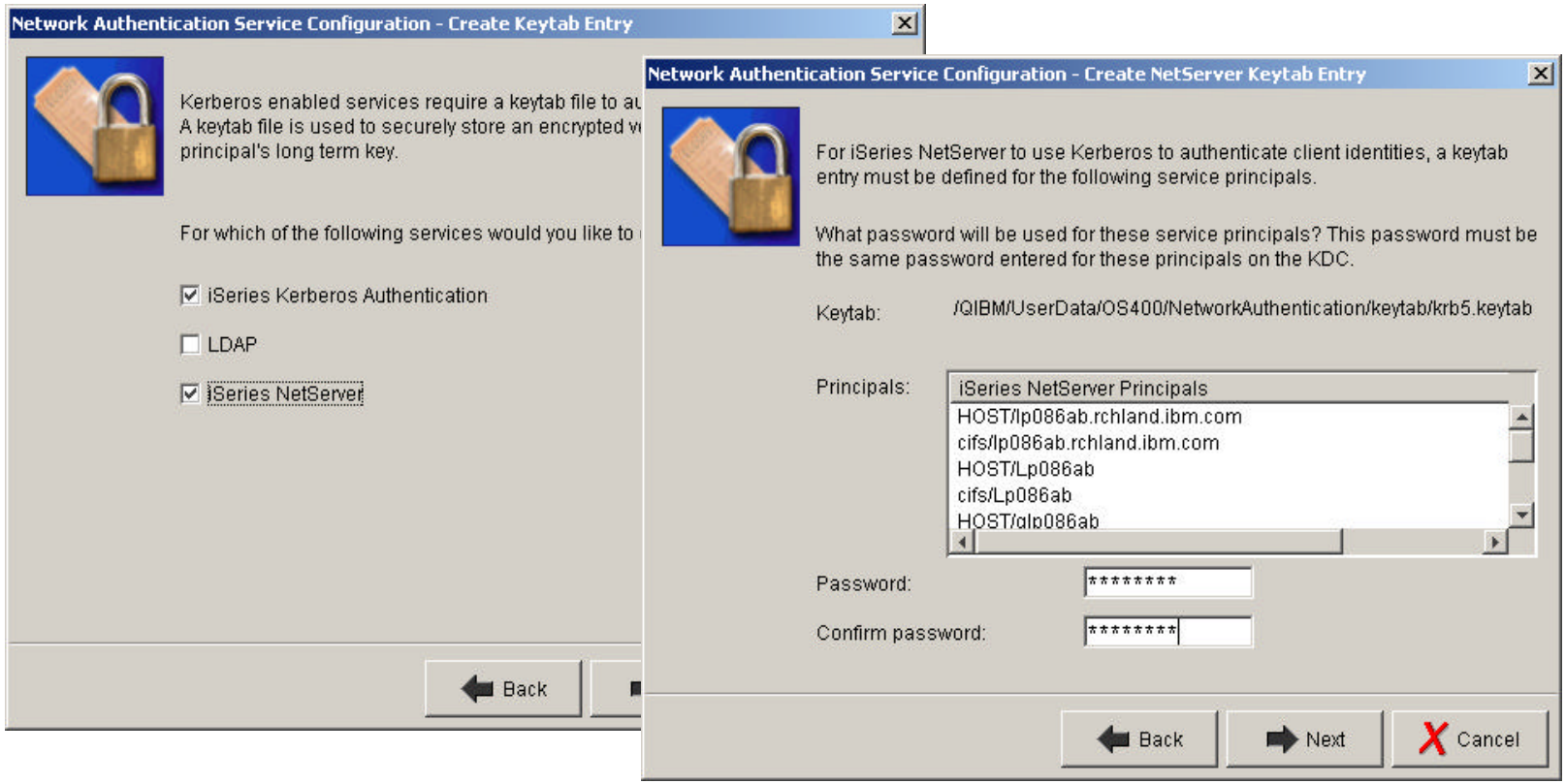
- Network Authentication configuration wizard through iSeries Navigator



Kerberos Authentication Support

Configuring Network Authentication Service

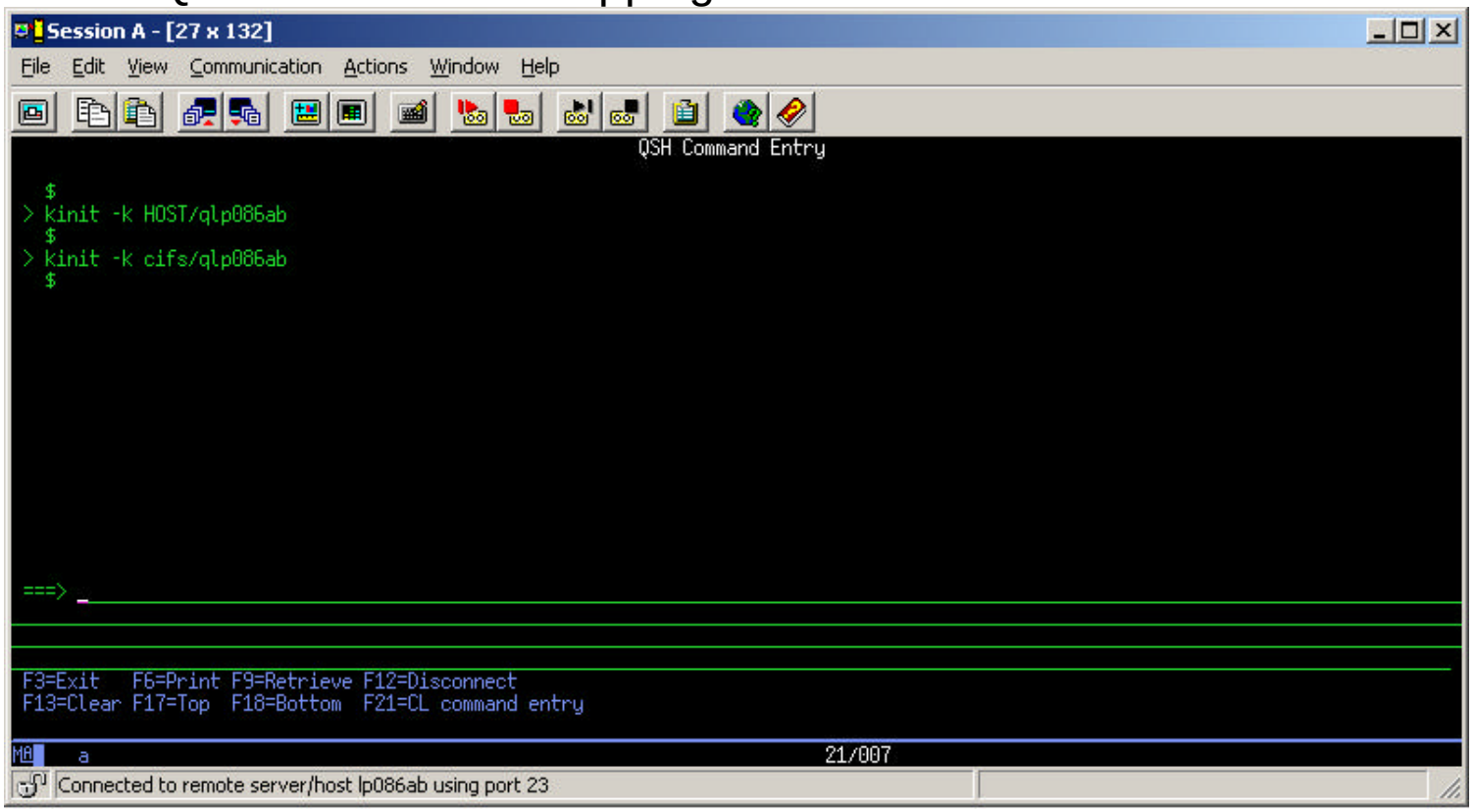
- During configuration be sure to choose to add the service principal names required by iSeries NetServer
- Remember the password used for the iSeries NetServer principals for later



Kerberos Authentication Support

Verifying that the Windows Principals are Correctly Configured

- Use Qshell to test the mappings



- If Qshell is not available, use the following command structure:

  CALL QKRBKINIT PARM('-k' 'HOST/<name>')

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

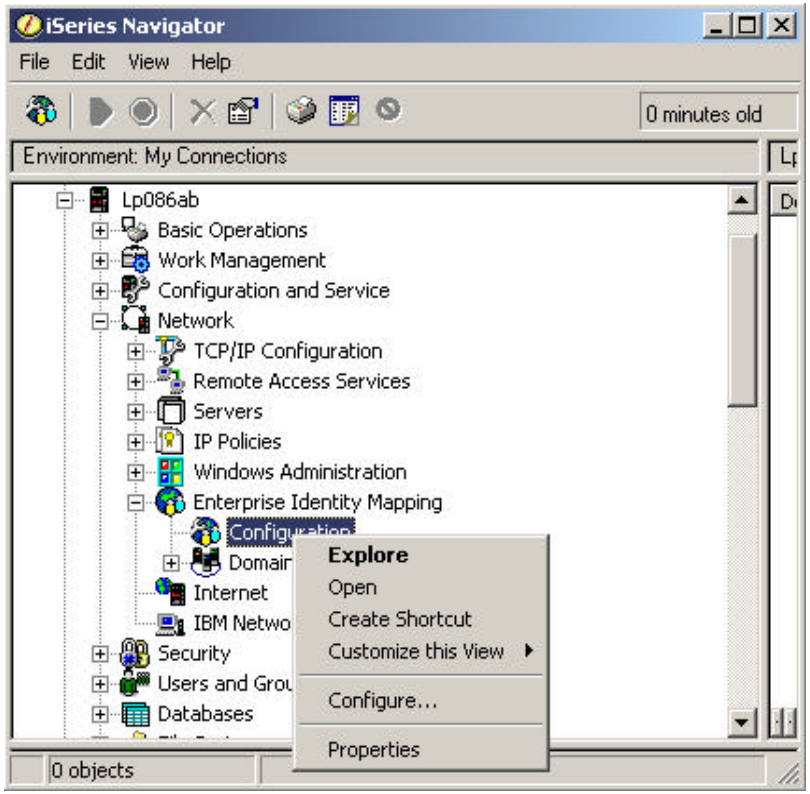
List Of EIM Associations For Jane Susan Doe			
EIM Identifier	**Registry Name**	**Registry User Name**	**Association Type**
Jane S. Doe	MYCOMPANY.COM	janedoe@mycompany.com	Source
Jane S. Doe	machine1	JANEDOE	Target
Jane S. Doe	machine2	JSDOE	Target
Jane S. Doe	mc3	JANED	Target

- **User authenticates on *source machine* with Keberos 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 EIM

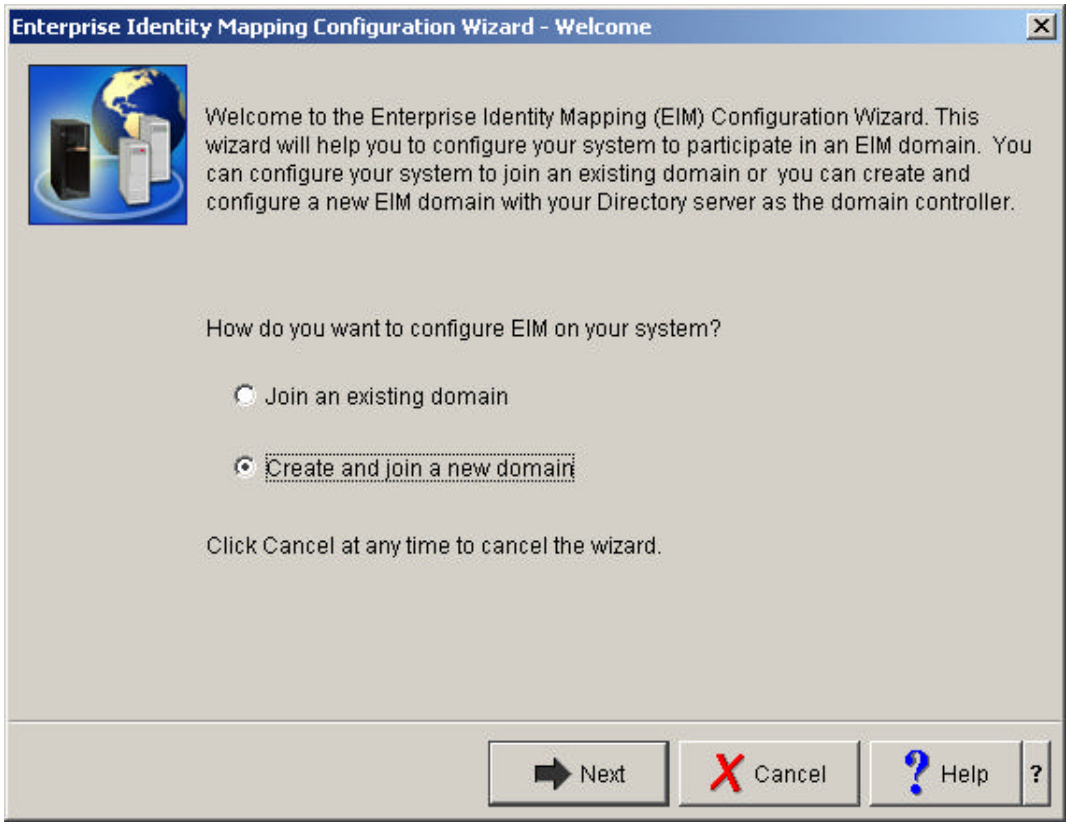
- Access EIM Configuration through iSeries Navigator
  - Network | Enterprise Identity Mapping | Configuration
  - Right click and choose **Configure...**



Kerberos Authentication Support

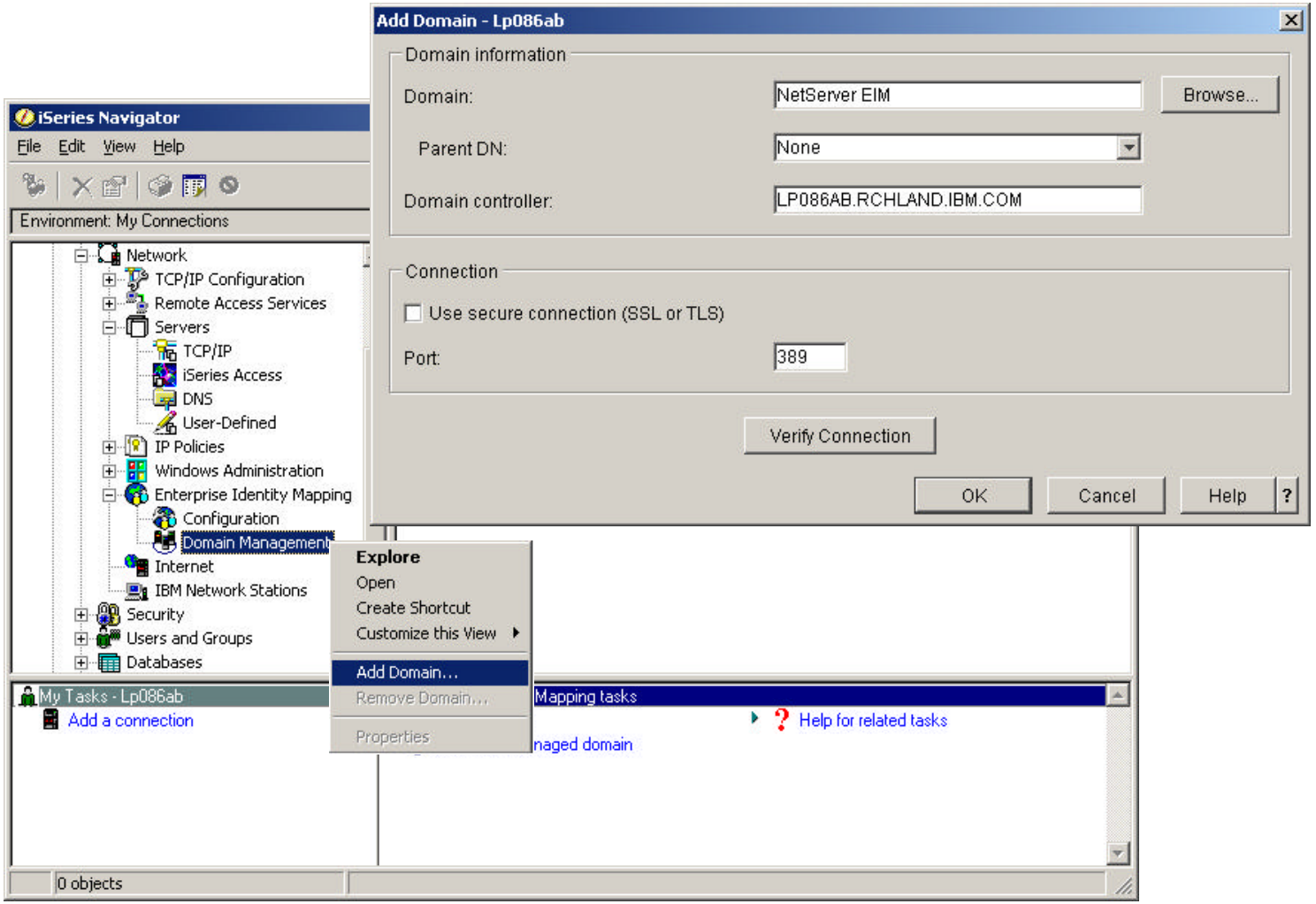
Configuring EIM

- Use the EIM configuration wizard



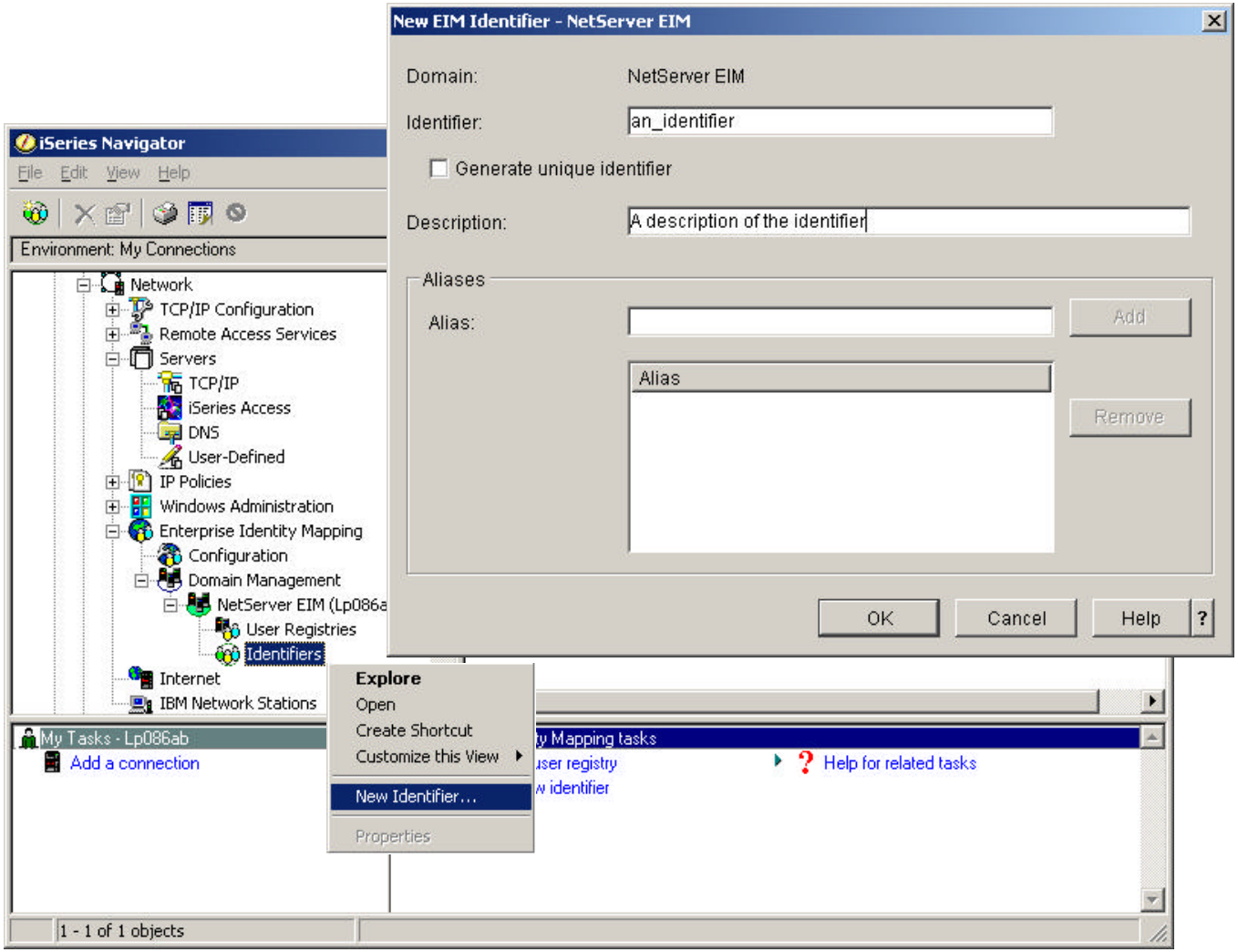
Kerberos Authentication Support

Configuring EIM - Adding the New Domain



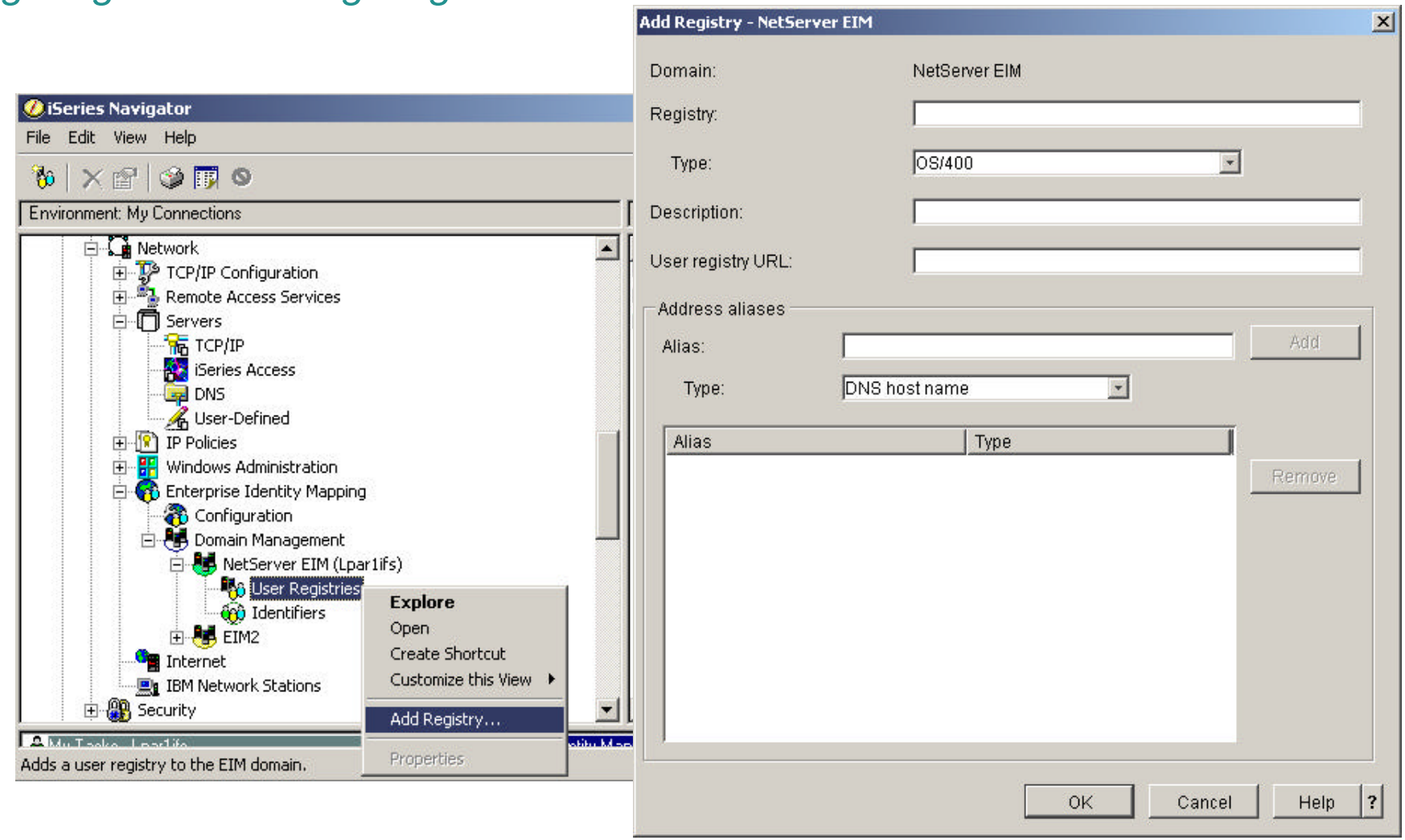
Kerberos Authentication Support

Configuring EIM - Adding Identifiers



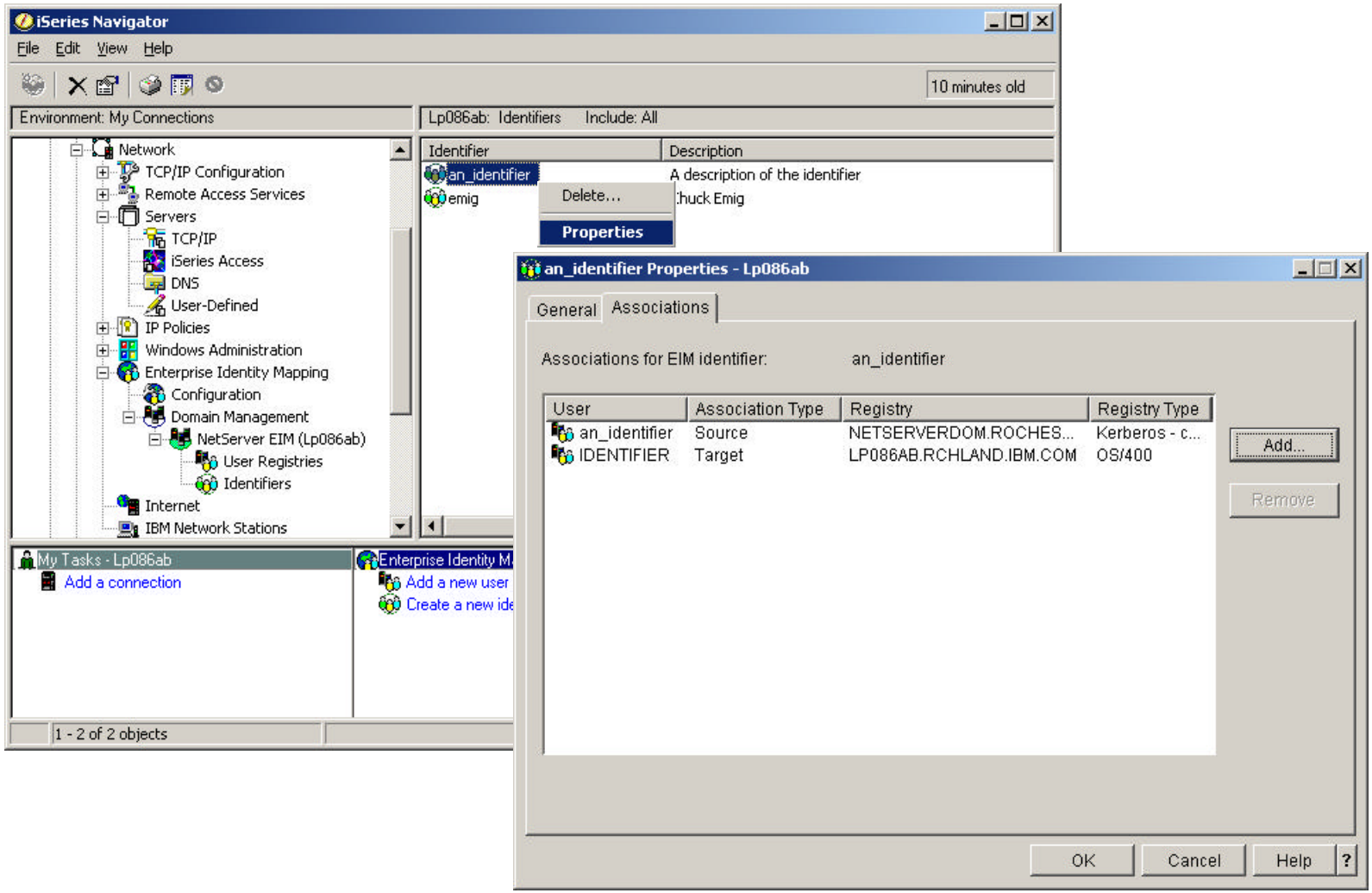
Kerberos Authentication Support

Configuring EIM - Adding Registries



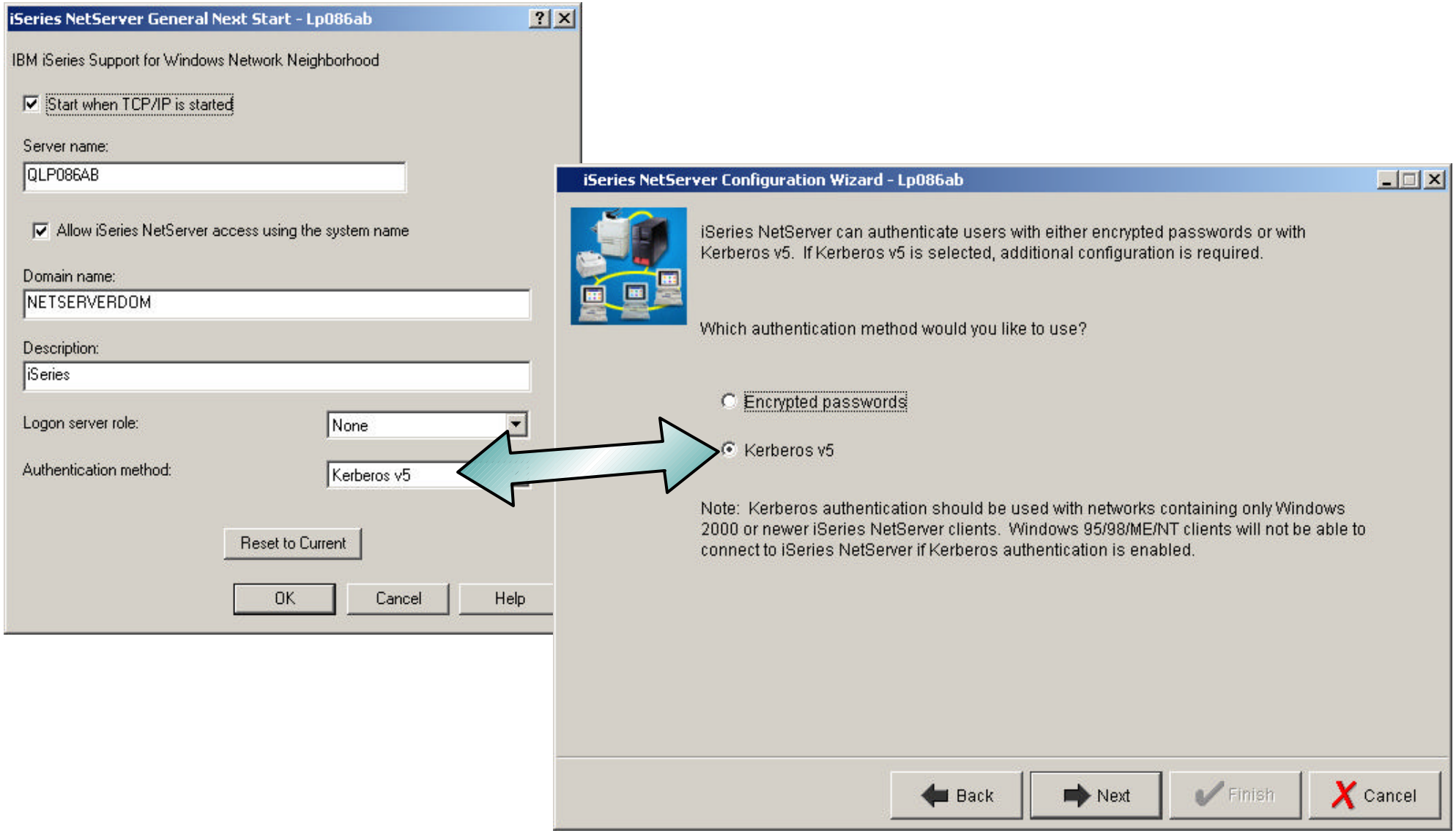
Kerberos Authentication Support

Configuring EIM - Adding Associations



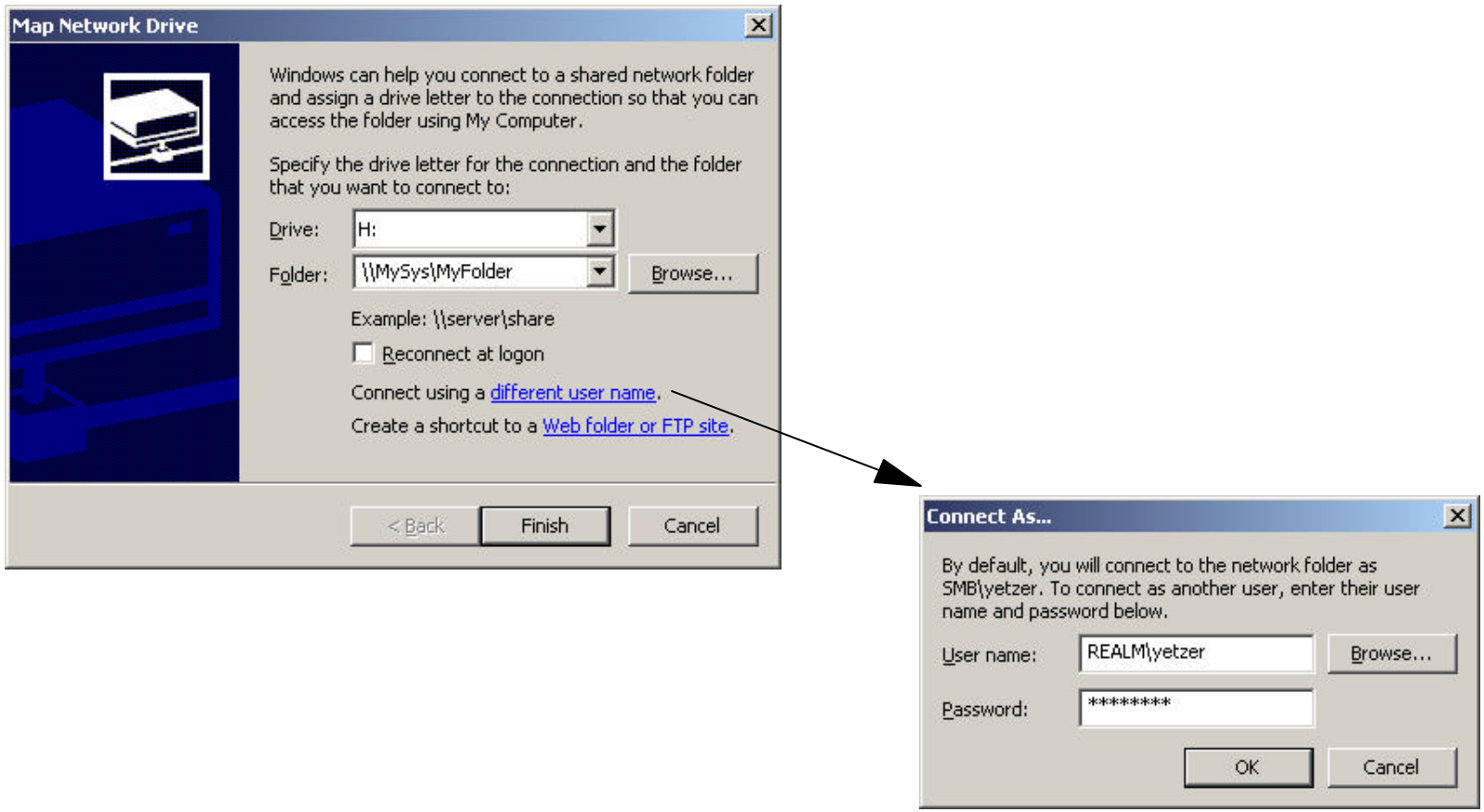
Kerberos Authentication Support

Configuring iSeries NetServer



Kerberos Authentication Support

Accessing NetServer



User Defined Subsystem Support

User Defined Subsystem Support

What does this mean?

Pre V5R2

Opt	Subsystem/Job	User	Type
	QSERVER	QSYS	SBS
	QPWFSERVSD	QUSER	BCH
	QSERVER	QPGMR	ASJ
	QZDASRVSD	QUSER	BCH
	QZLSFILE	QUSER	PJ
	QZLSSERVER	QPGMR	BCH

iSeries NetServer jobs in QSERVER

V5R2

Opt	Subsystem/Job	User	Type
	QSERVER	QSYS	SBS
	QPWFSERVSD	QUSER	BCH
	QSERVER	QPGMR	ASJ
	QZDASRVSD	QUSER	BCH
	QZLSSERVER	QPGMR	BCH
	ACCOUNTING	QSYS	SBS
	QZLSFILE	QUSER	PJ
	QZLSFILE	QUSER	PJ
	MARKETING	QSYS	SBS
	QZLSFILE	QUSER	PJ
	QZLSFILE	QUSER	PJ

Customer decides where iSeries NetServer jobs will run.

User Defined Subsystem Support

Why?

- Client Manageability
  - Control access
  - Manage connections
    - Example:

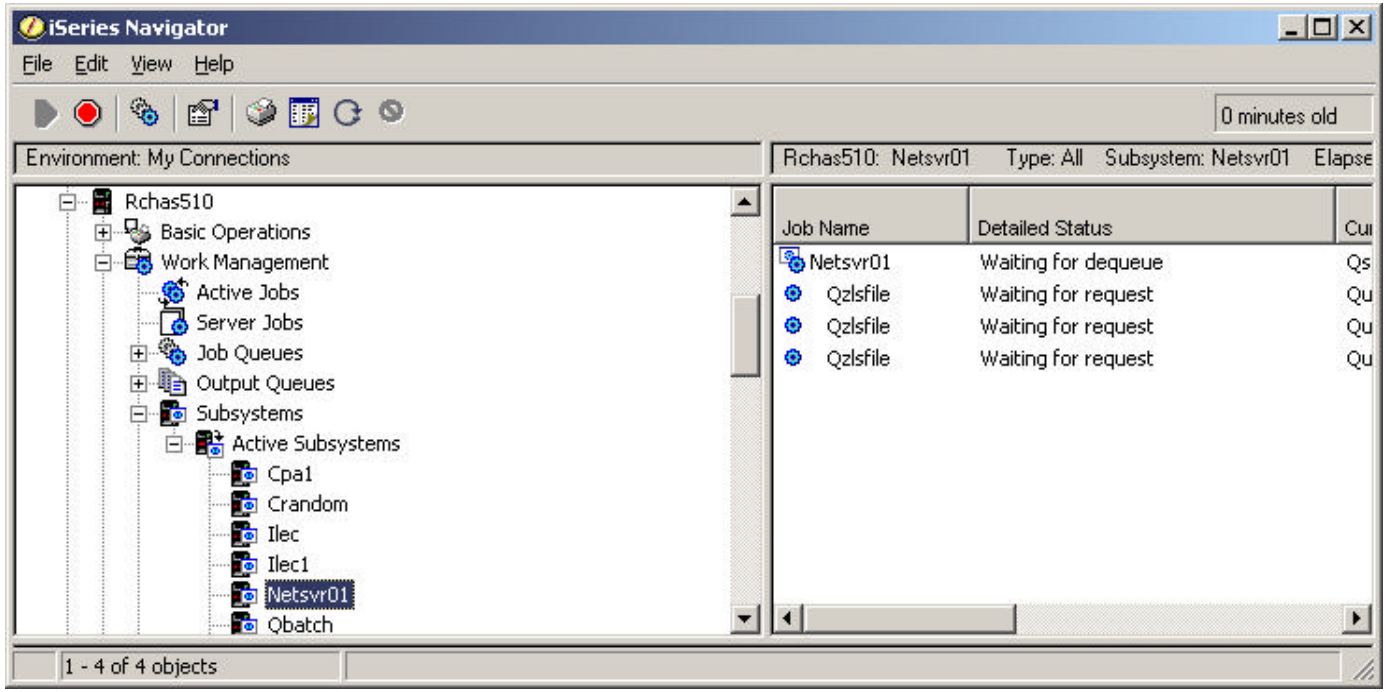
      An IT Manager can control which subsystem each group of users will run in. A separate subsystem is created for each division.
      When the manager needs to restrict access to the system, a subsystem can be ended without impacting other operations.
      When the manager needs to find a particular user's file server job,
      he will only have to look in the subsystem for that division.

User Defined Subsystem Support

Setup

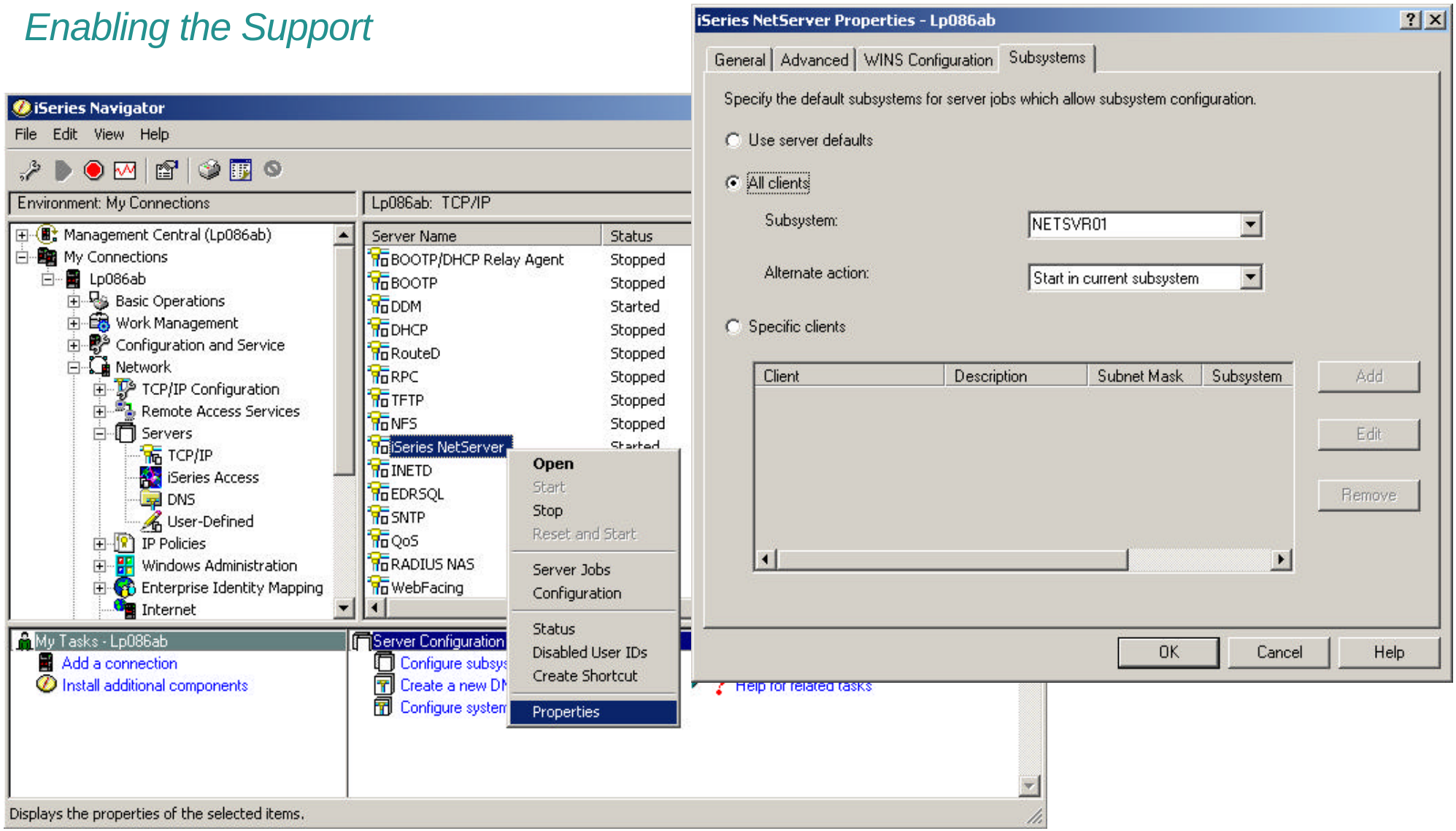
- **Create the subsystem description to be used by the iSeries NetServer QZLSFILE jobs**
  - CRTSBSD SBSD(QSYS/NETSVR01) POOLS((1 *BASE)) TEXT('NetServer Subsystem')
- **Add the required prestart jobs to the subsystem description**
  - ADDPJE SBSD(QSYS/NETSVR01) PGM(QSYS/QZLSFILE) CLS(QSYS/QPWFSERVER)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

User Defined NetServer Subsystem



User Defined Subsystem Support

Enabling the Support

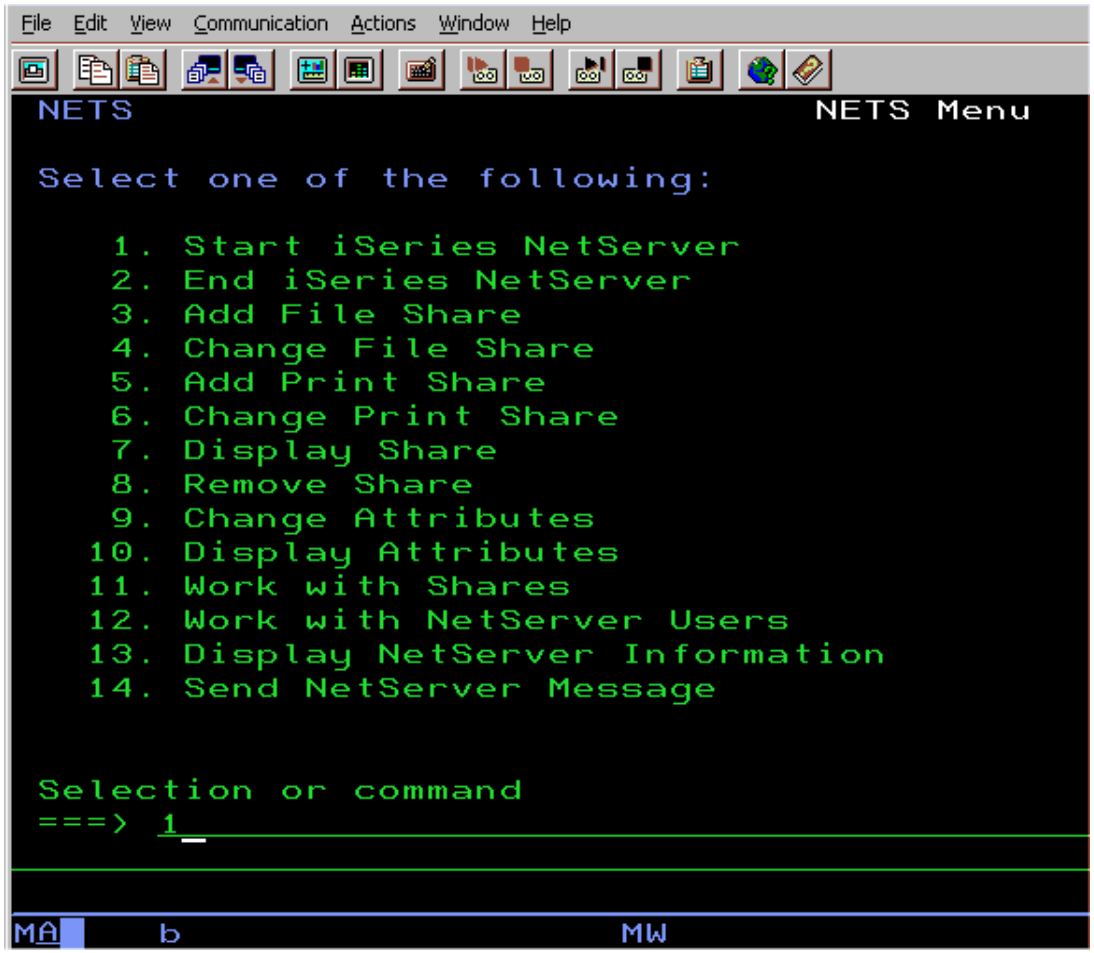


V5R2 GO NETS

GO NETS

Administration Power on a Green Screen

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



GO NETS

Setting up GO NETS

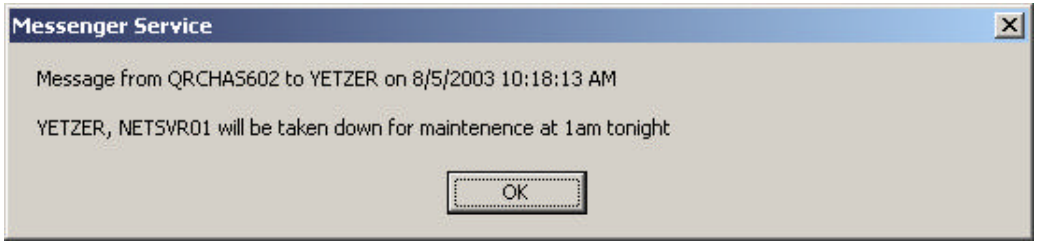
- Follow these example steps to build the GO NETS command tool into library NETSRVCMD.
  1. Create the target library. NETSRVCMD may be replaced with the library name of your choice.
     - CRTLIB LIB(NETSRVCMD) TEXT('iSeries NetServer menu and commands')
  2. Expand the necessary files:
     - CALL 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, NETSVR01 will be taken down for maintenance at 1am tonight') 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 &

Popup Messaging - Setup

iSeries Setup and Use

- Change the message logging severity of the QZLSSERVER job
  - CHGJOBD JOBD(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 QPCSMPRT 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/iseries/netserver/

Documentation including iSeries NetServer can be found on InfoCenter

- http://www.ibm.com/eserver/iseries/infocenter

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

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.