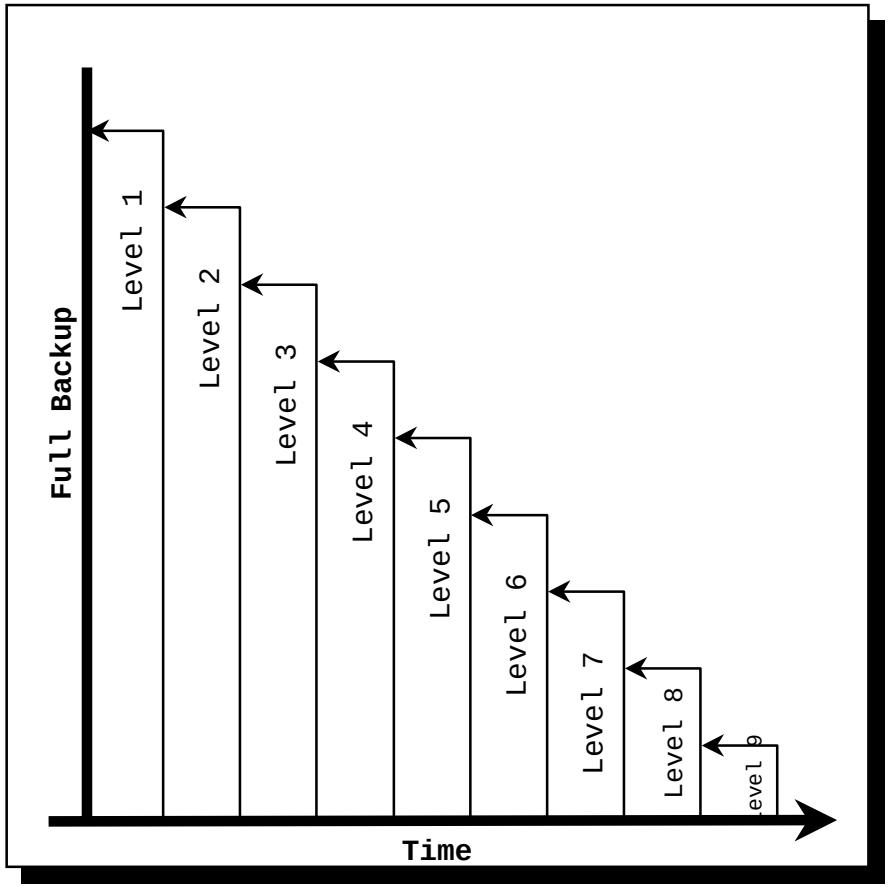
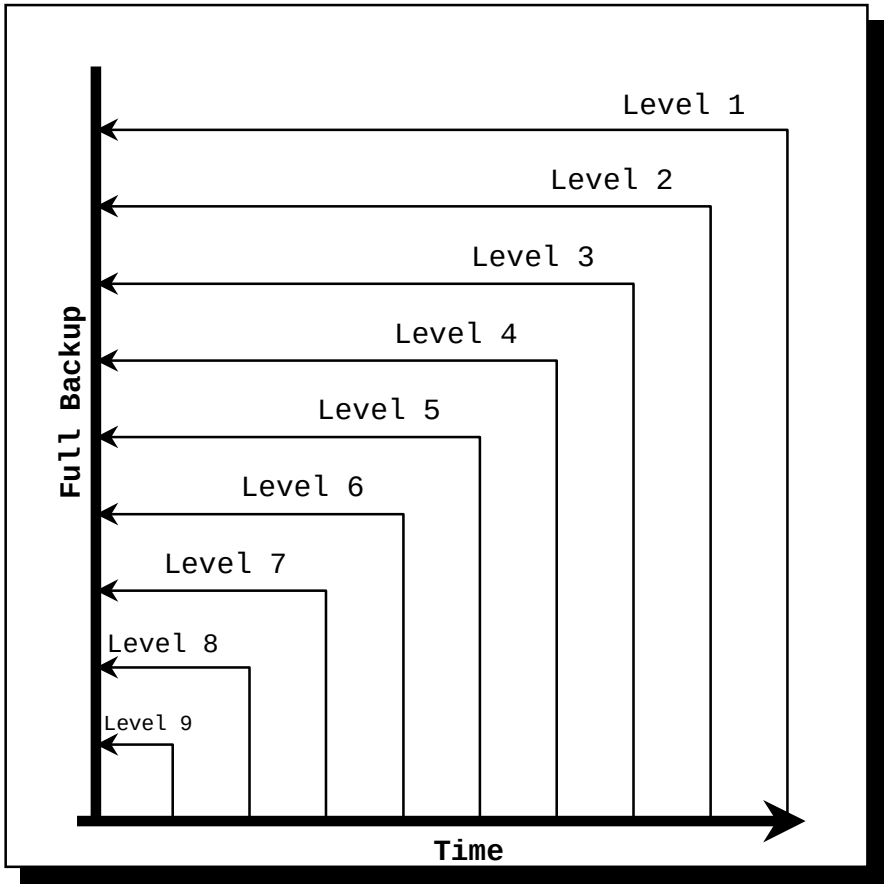
Backup Levels Overview

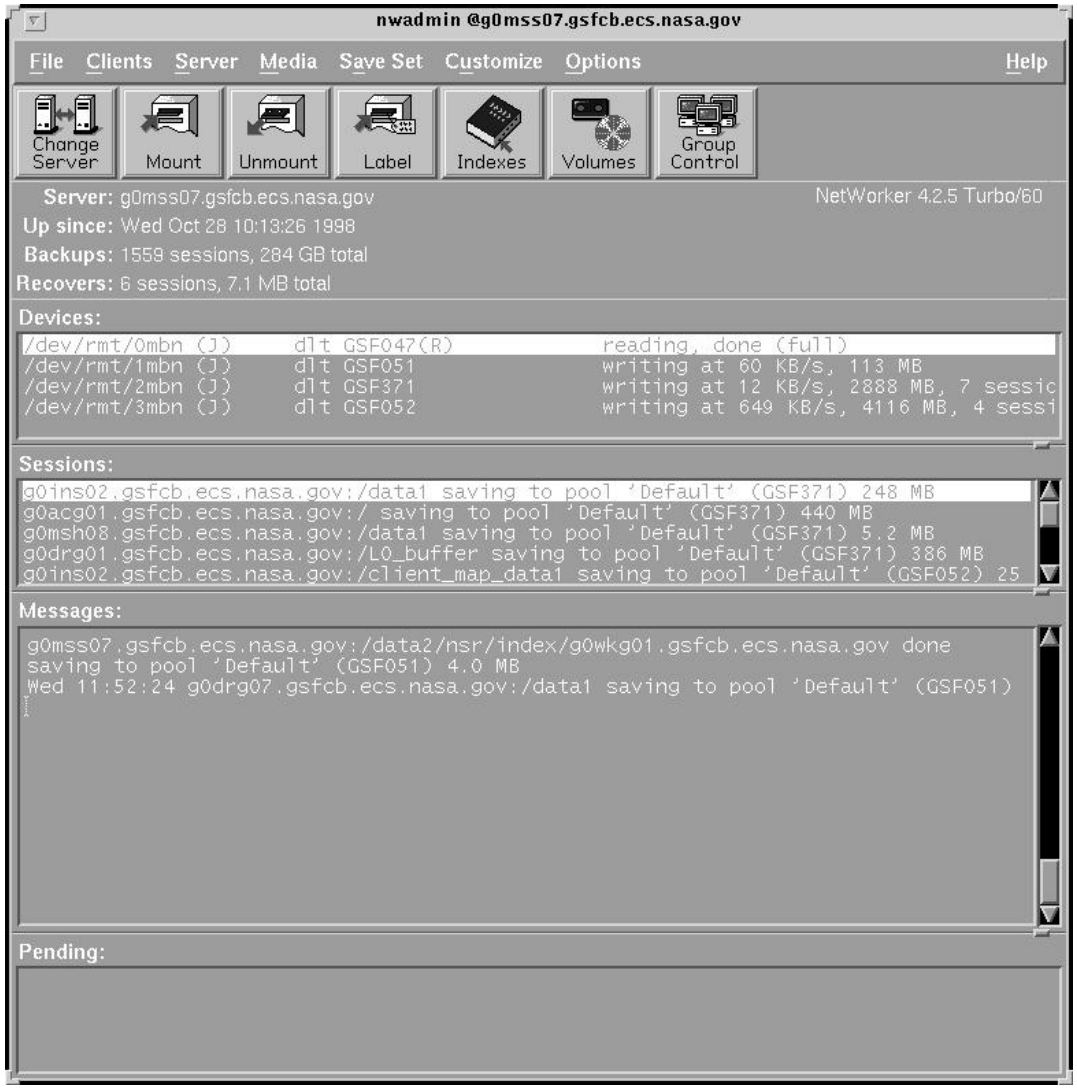
More incremental



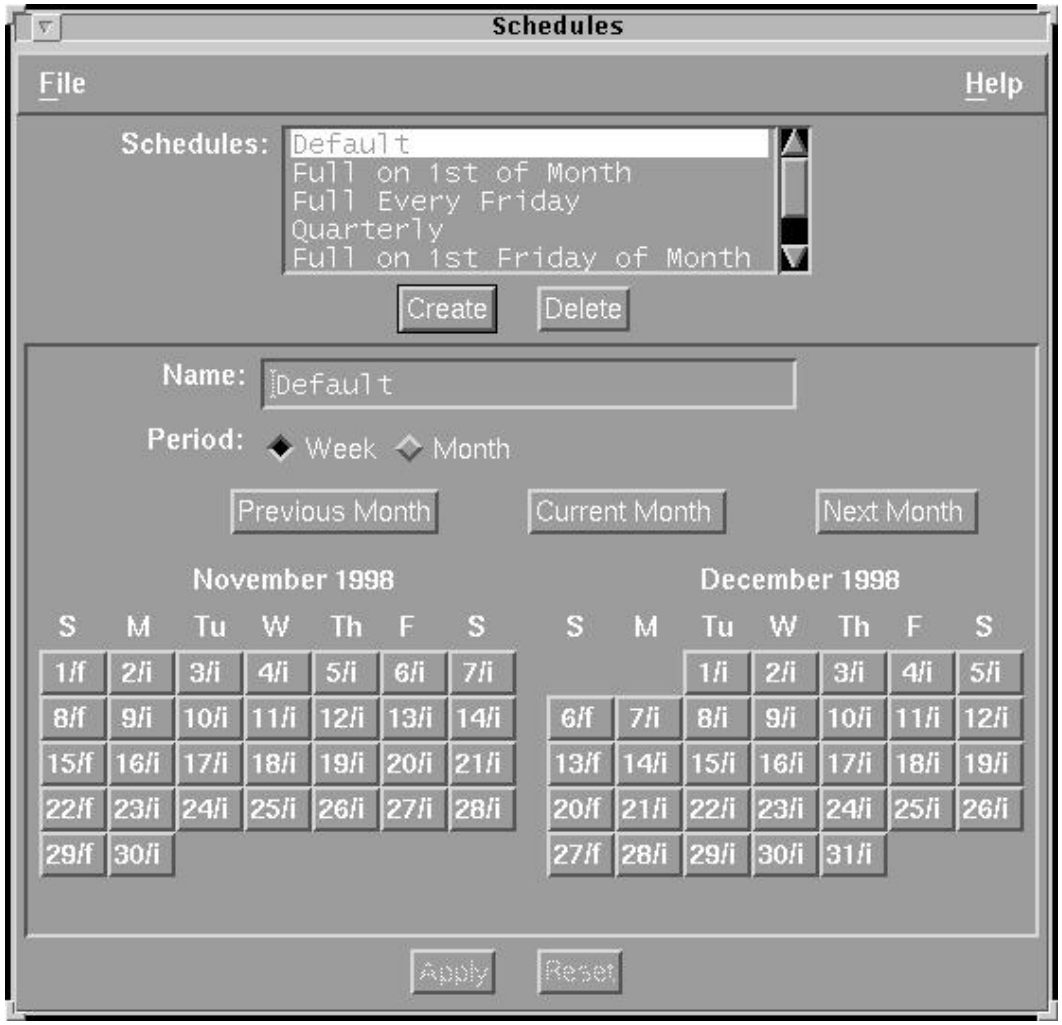
More cumulative



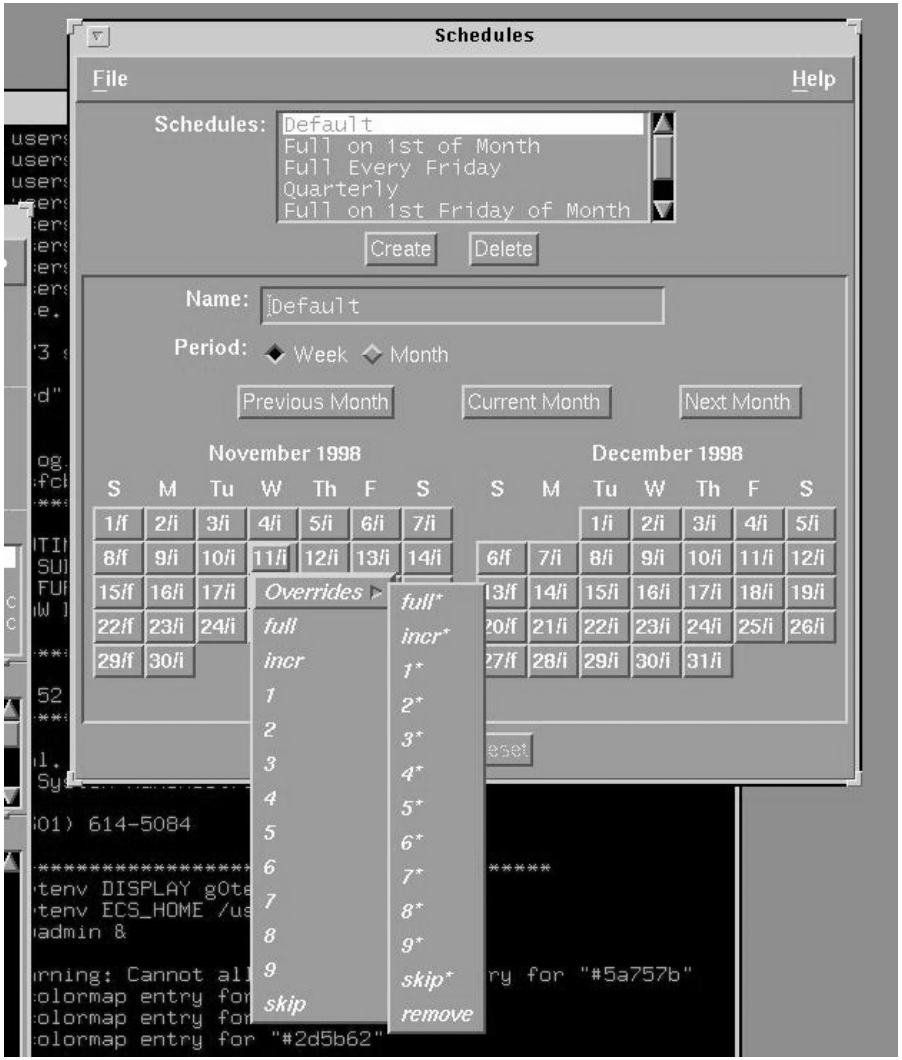
Networker Administrator's Window



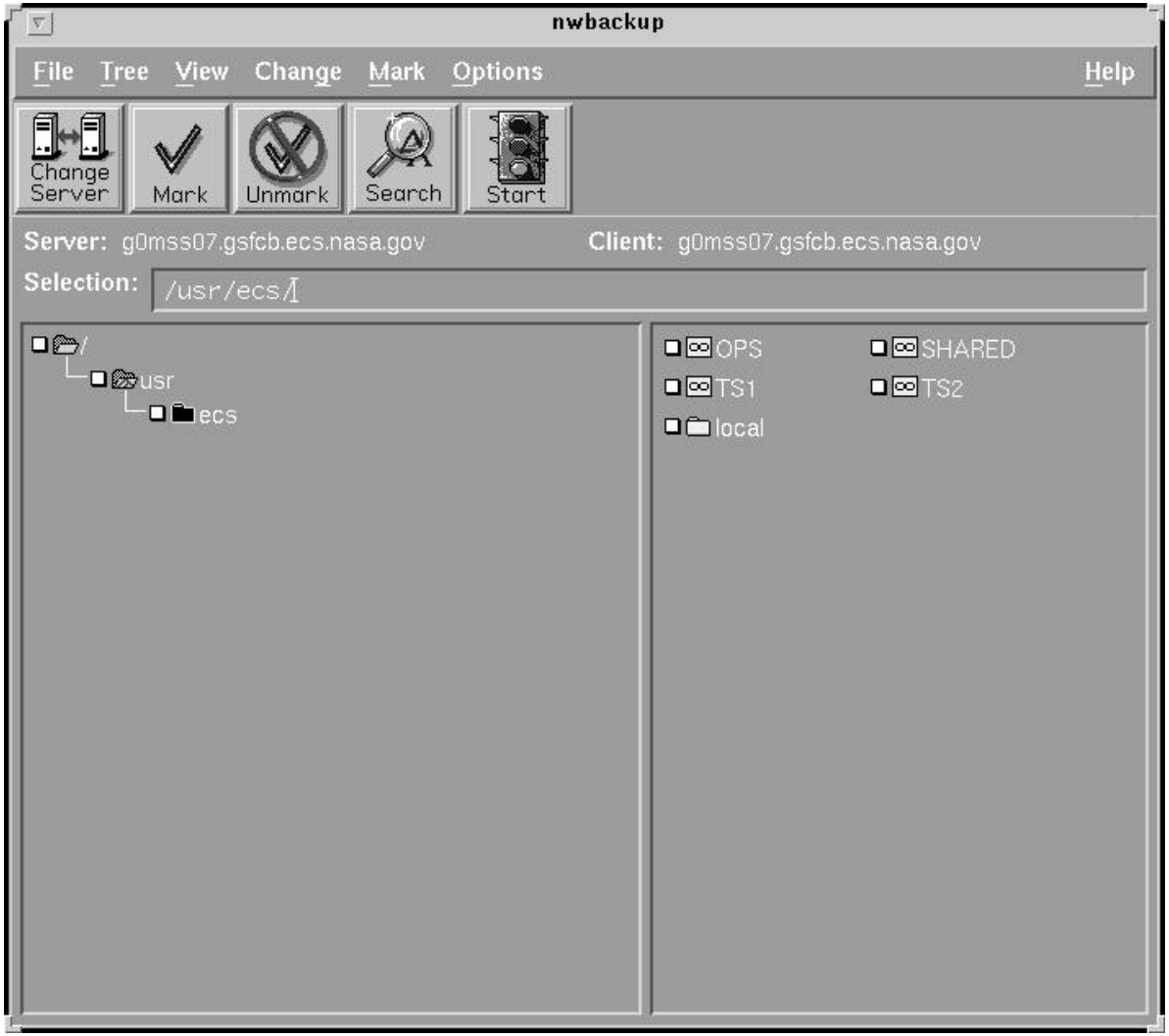
Networker Backup Scheduler



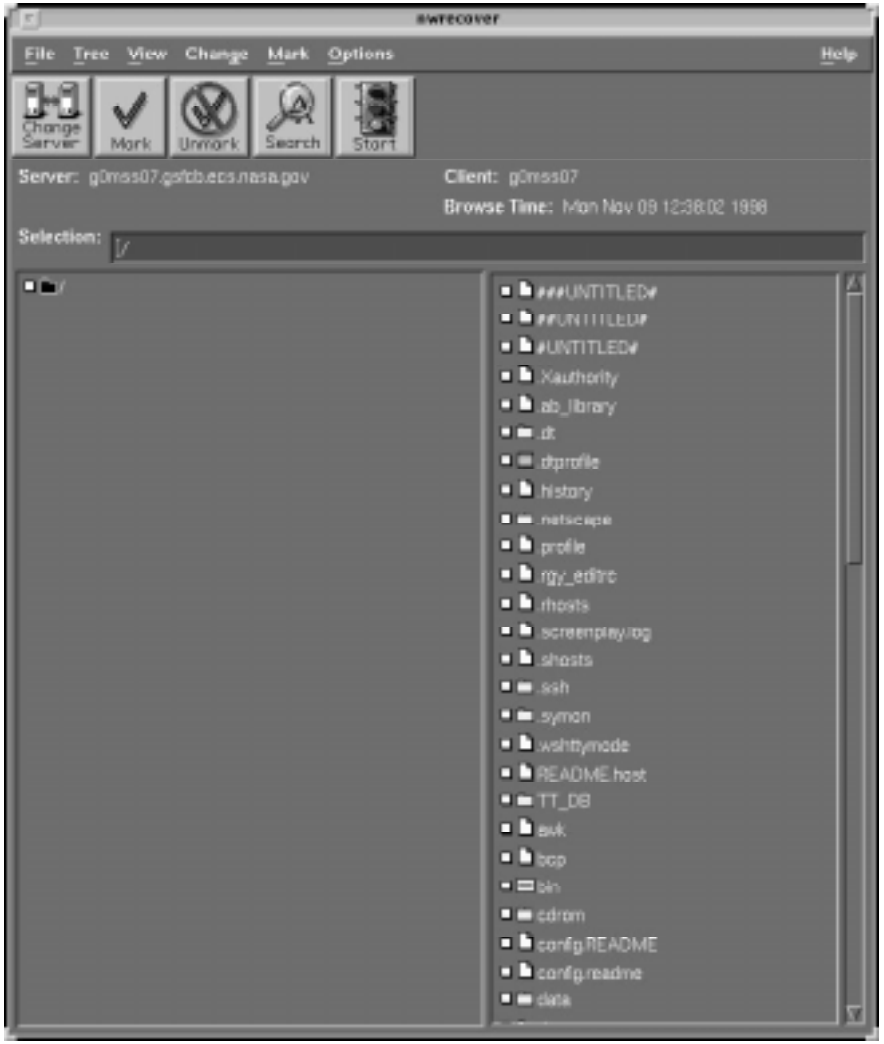
Networker Backup Scheduler Overrides Menus



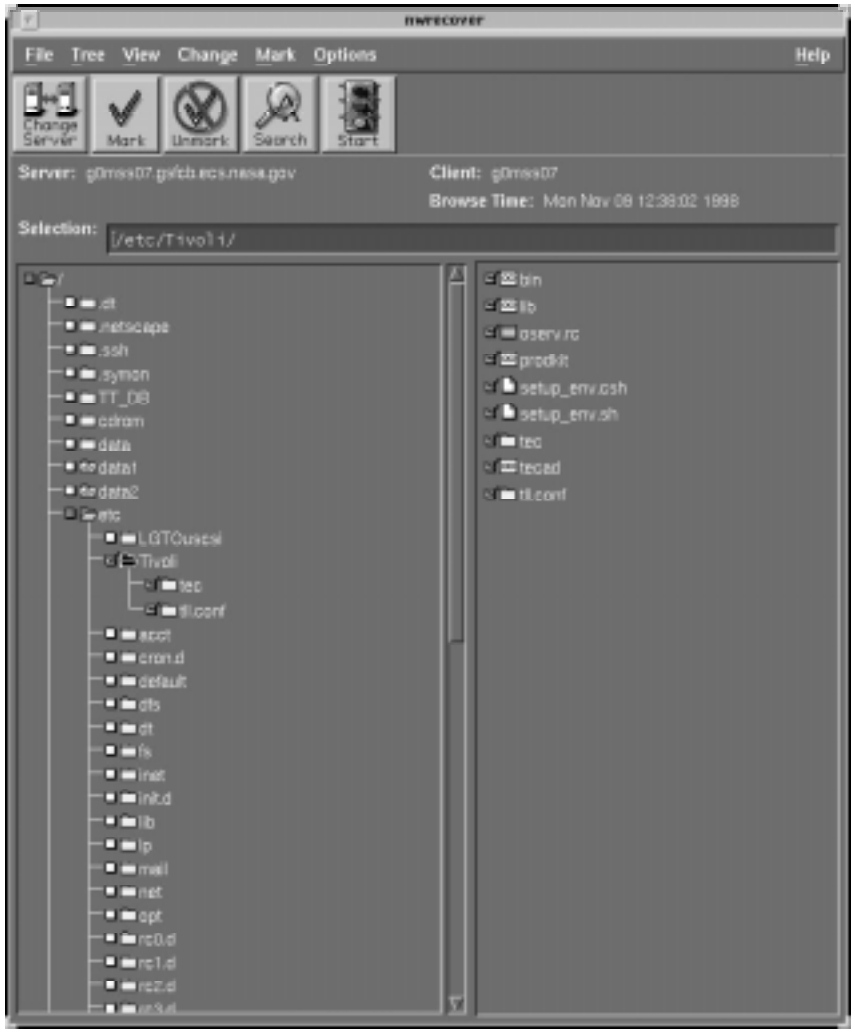
Networker Backup Window



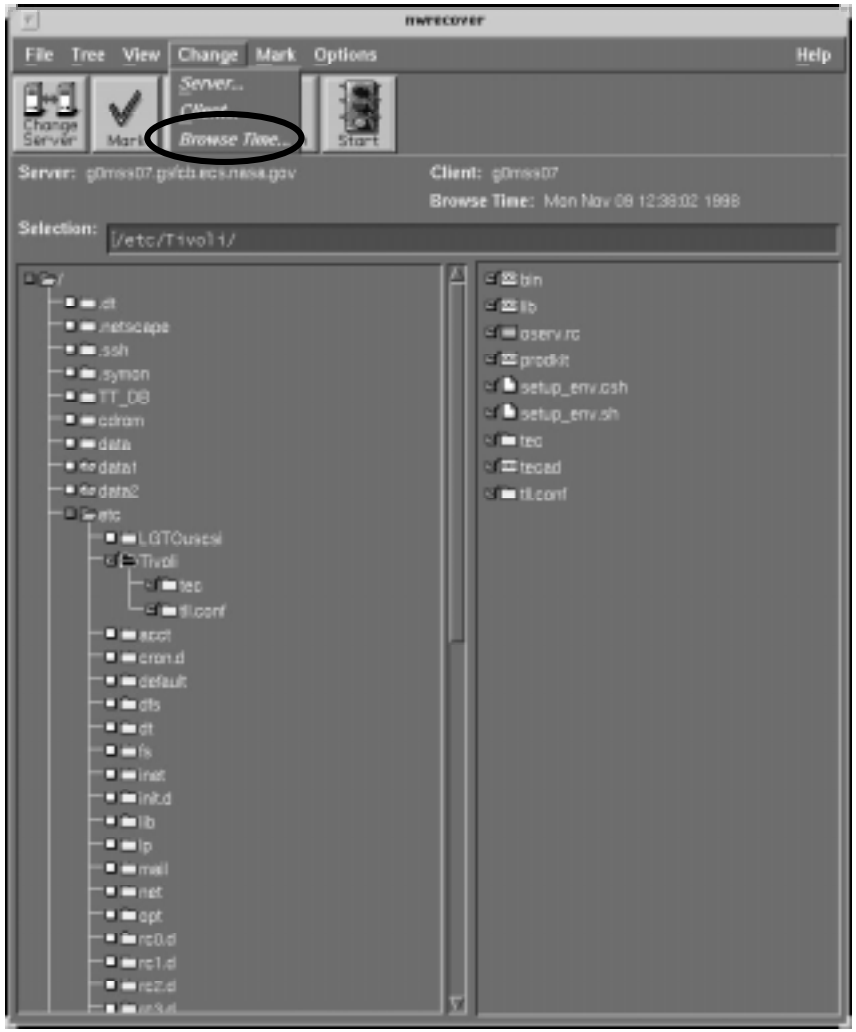
Networker Recover Window



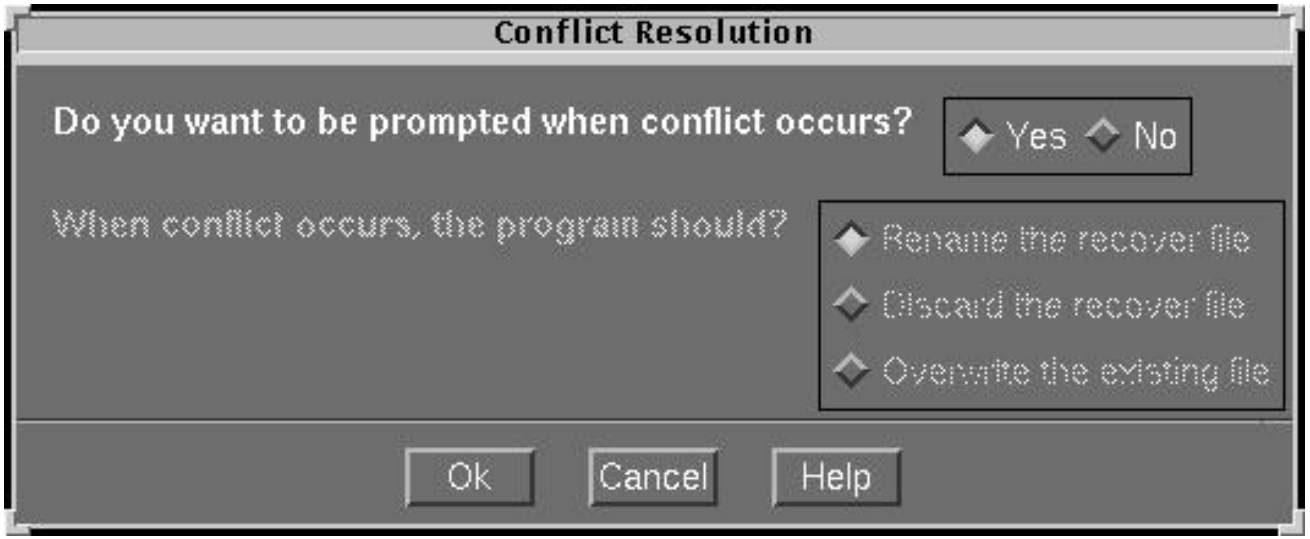
Networker Recover Window with Files Selected



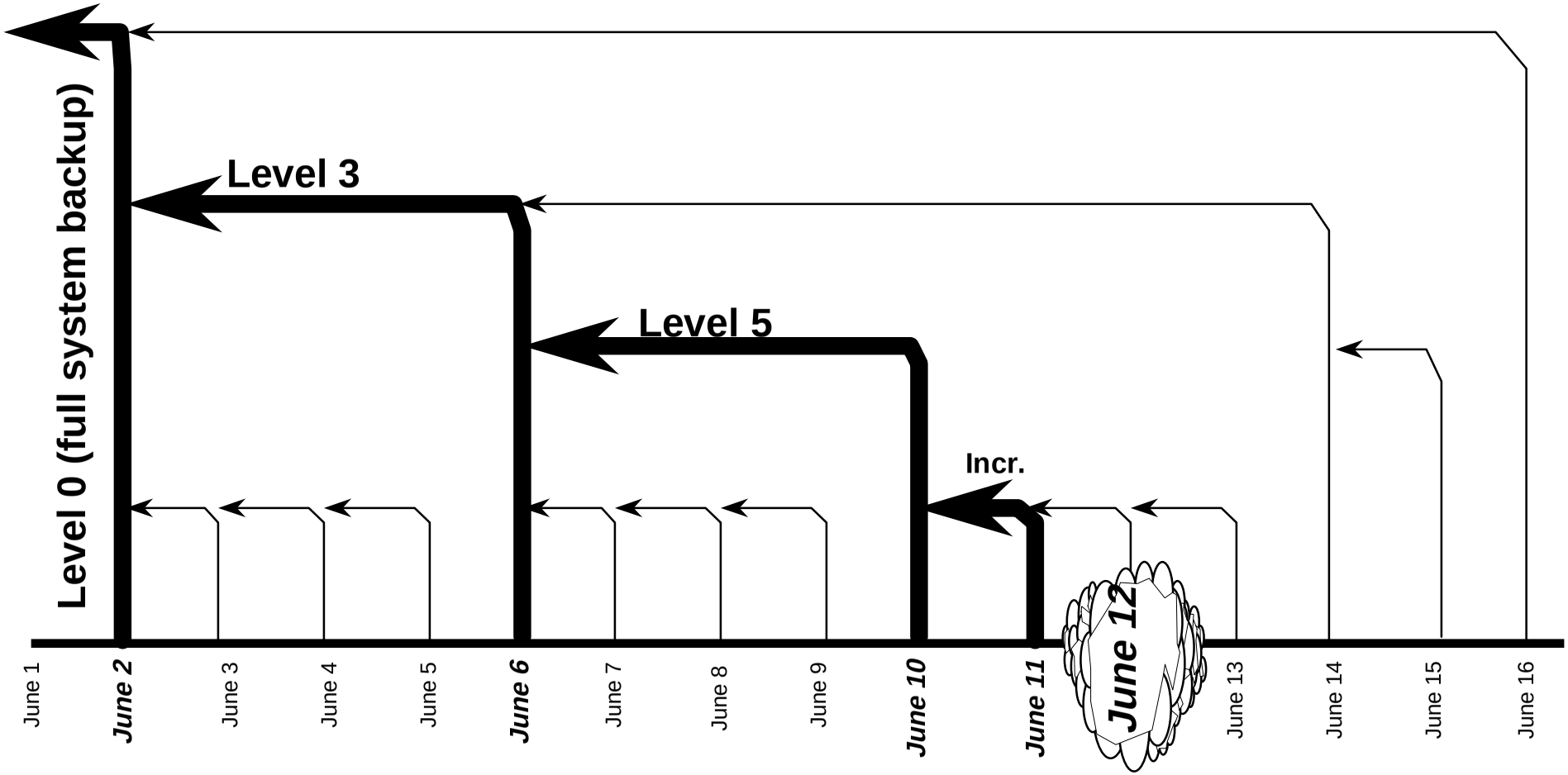
Networker Browse Time Window



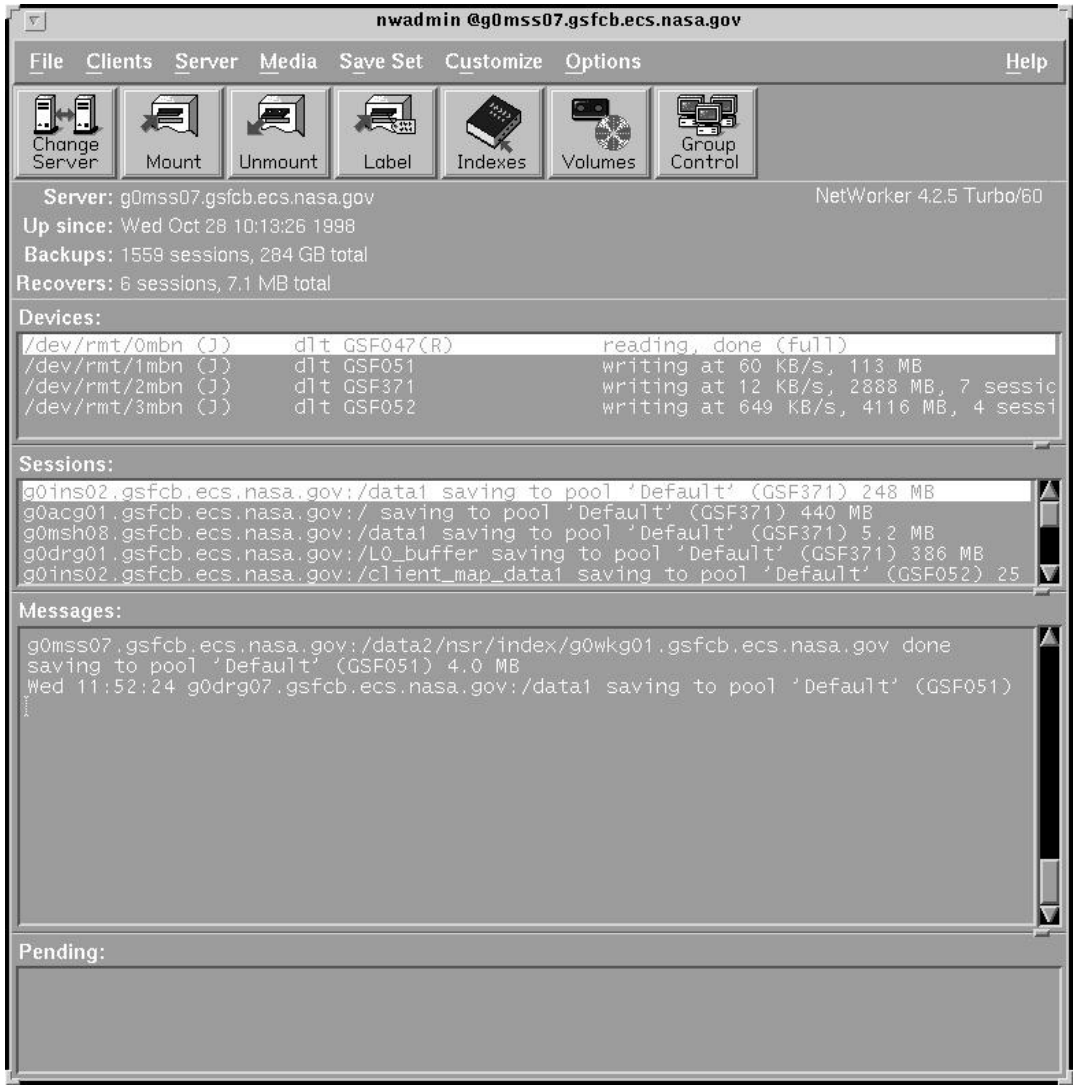
Networker Conflict Resolution Window



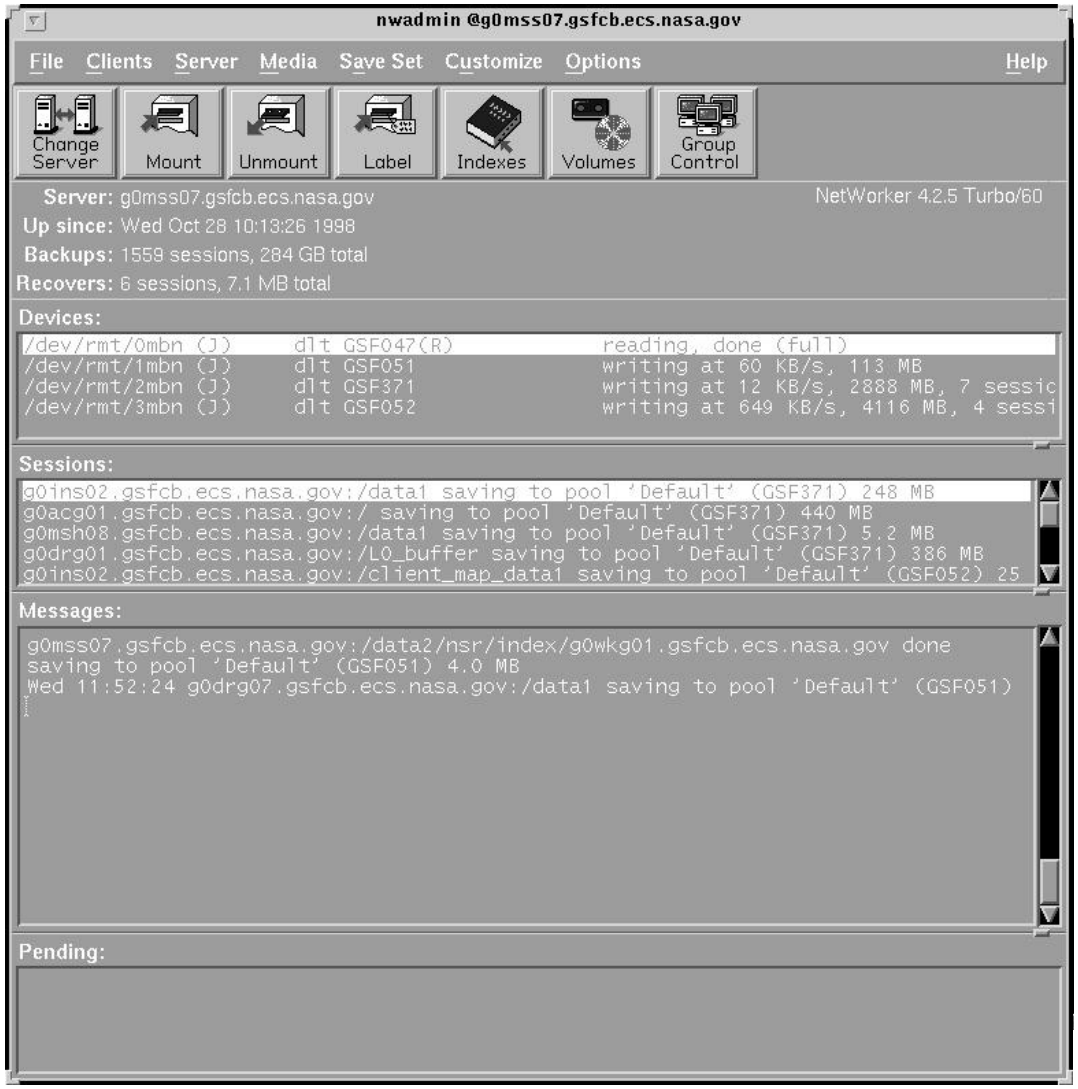
Tapes Required for Full System Restore



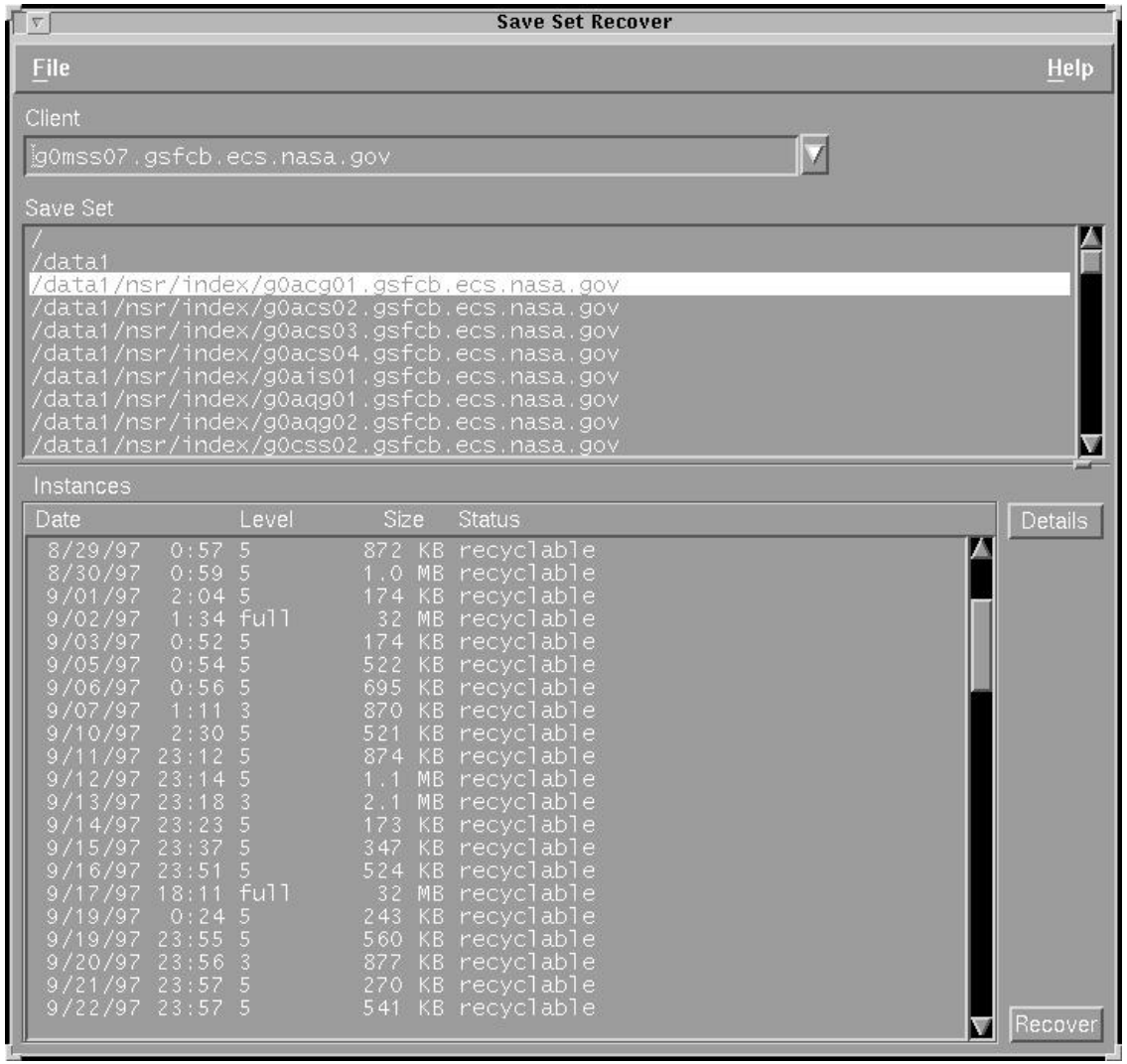
Networker Administrator Main Screen



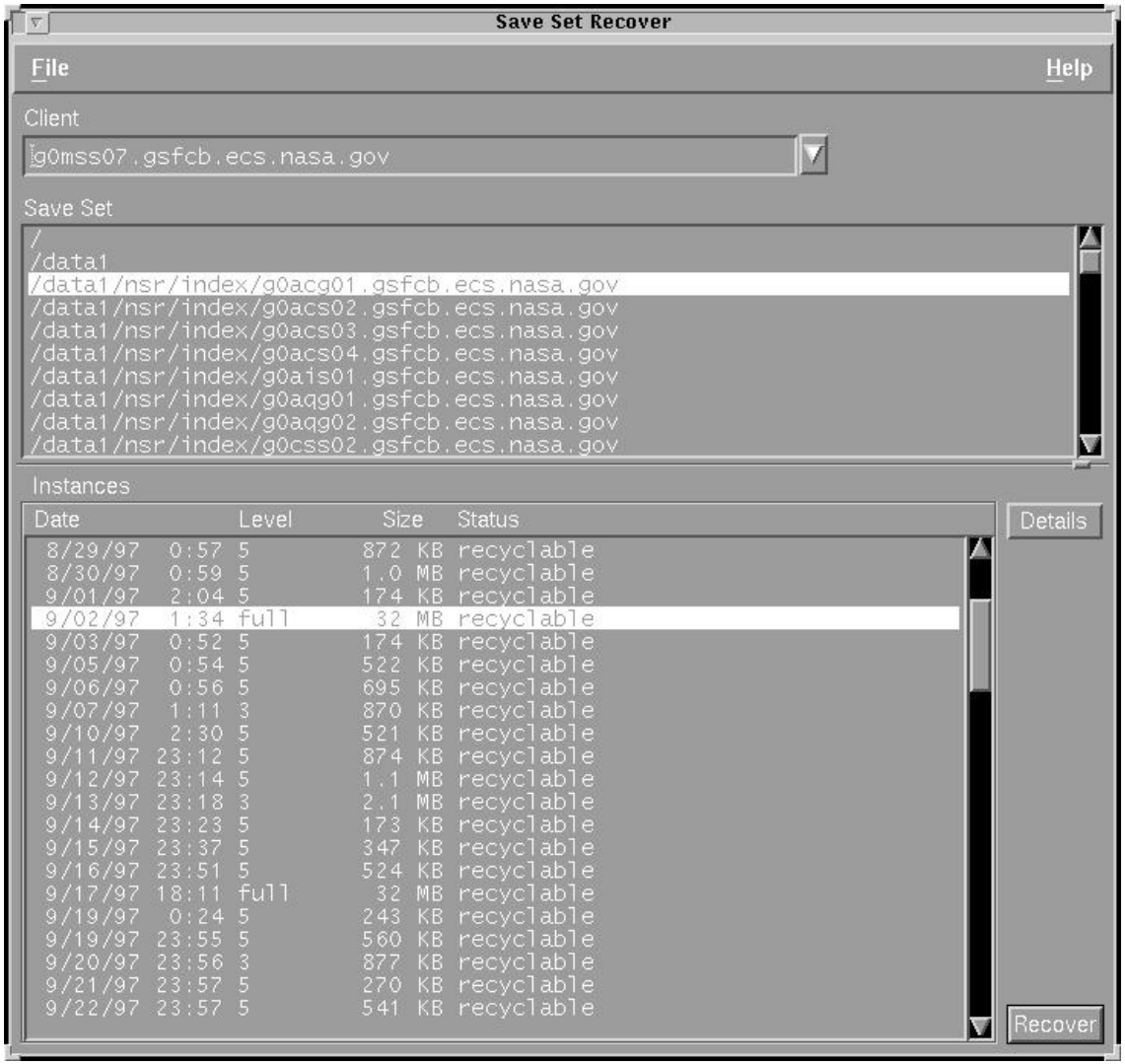
Networker Save Set Screen



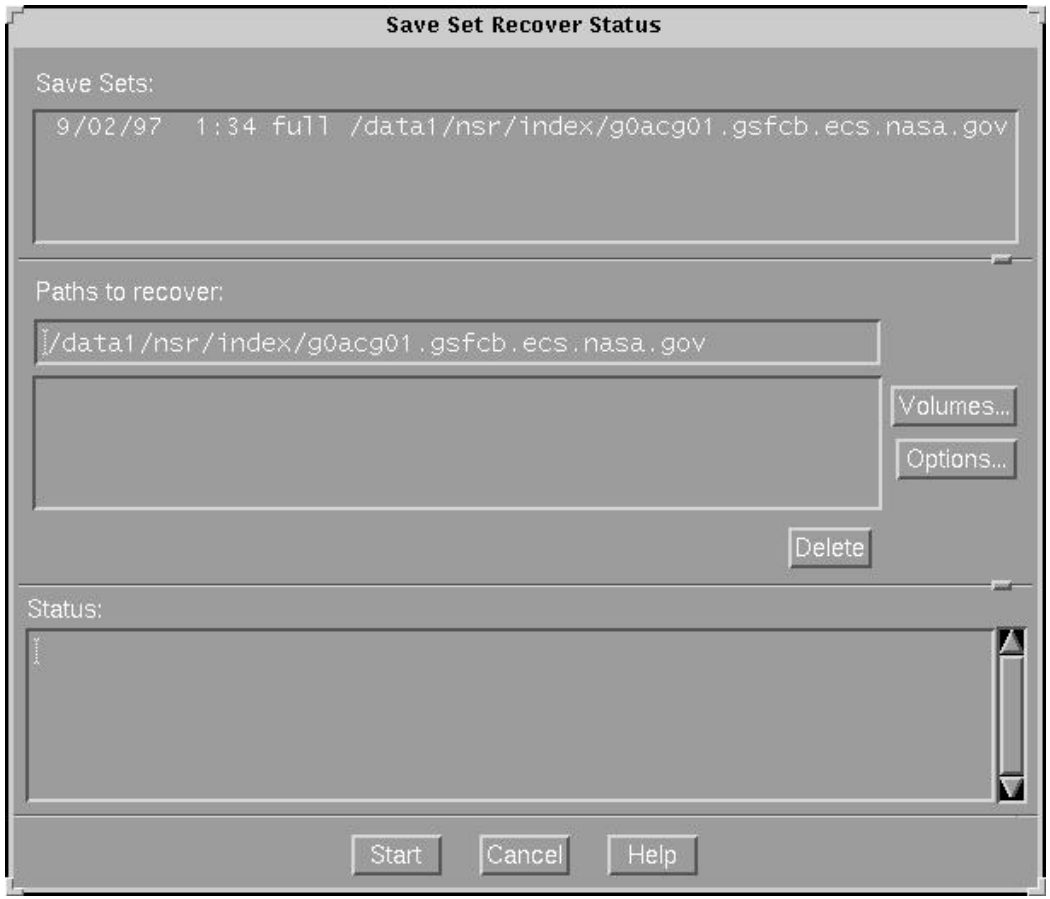
Networker Save Set Screen - cont'd



Networker Save Set Screen - cont'd



Networker Save Set Screen - cont'd

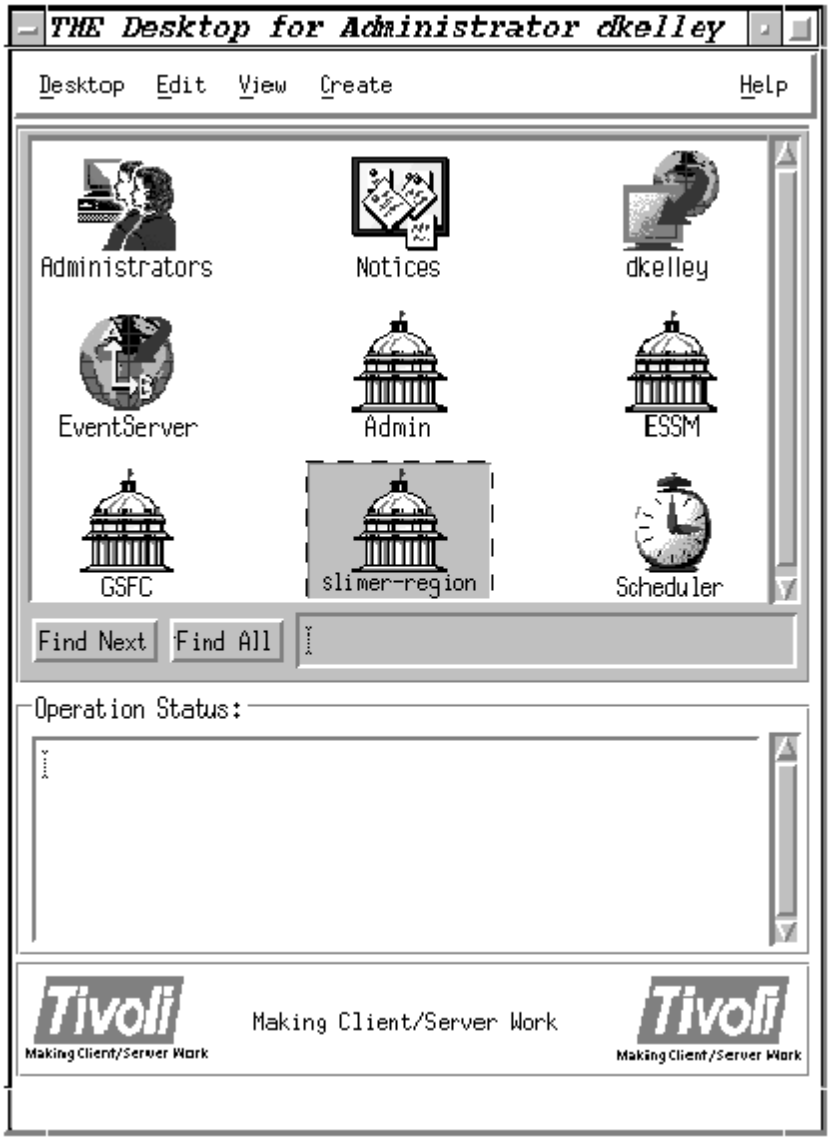


Networker Lab

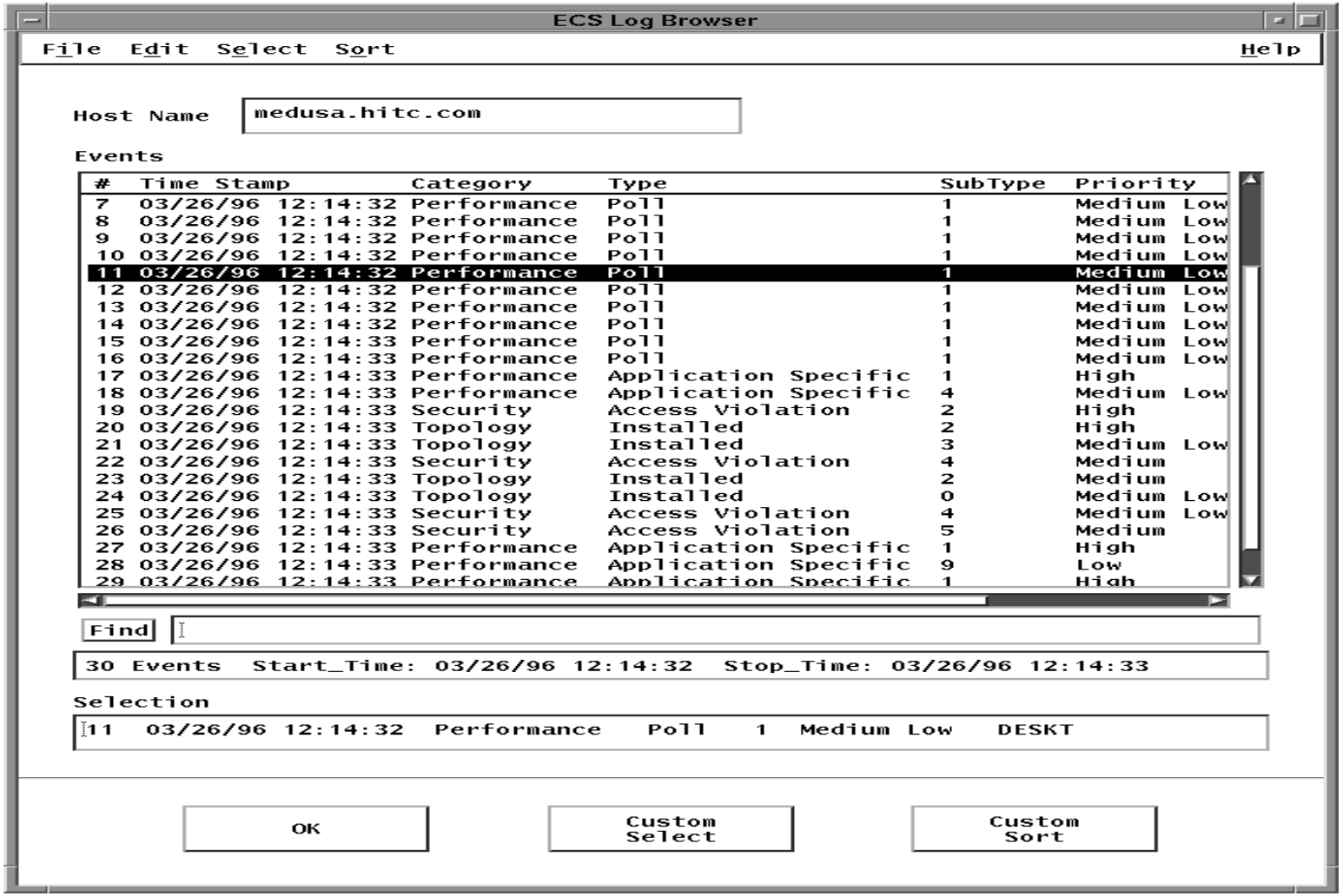
setenv DISPLAY (IP address)
setenv ECS_HOME /usr/ecs

nwadmin, nwbackup, nwrecover

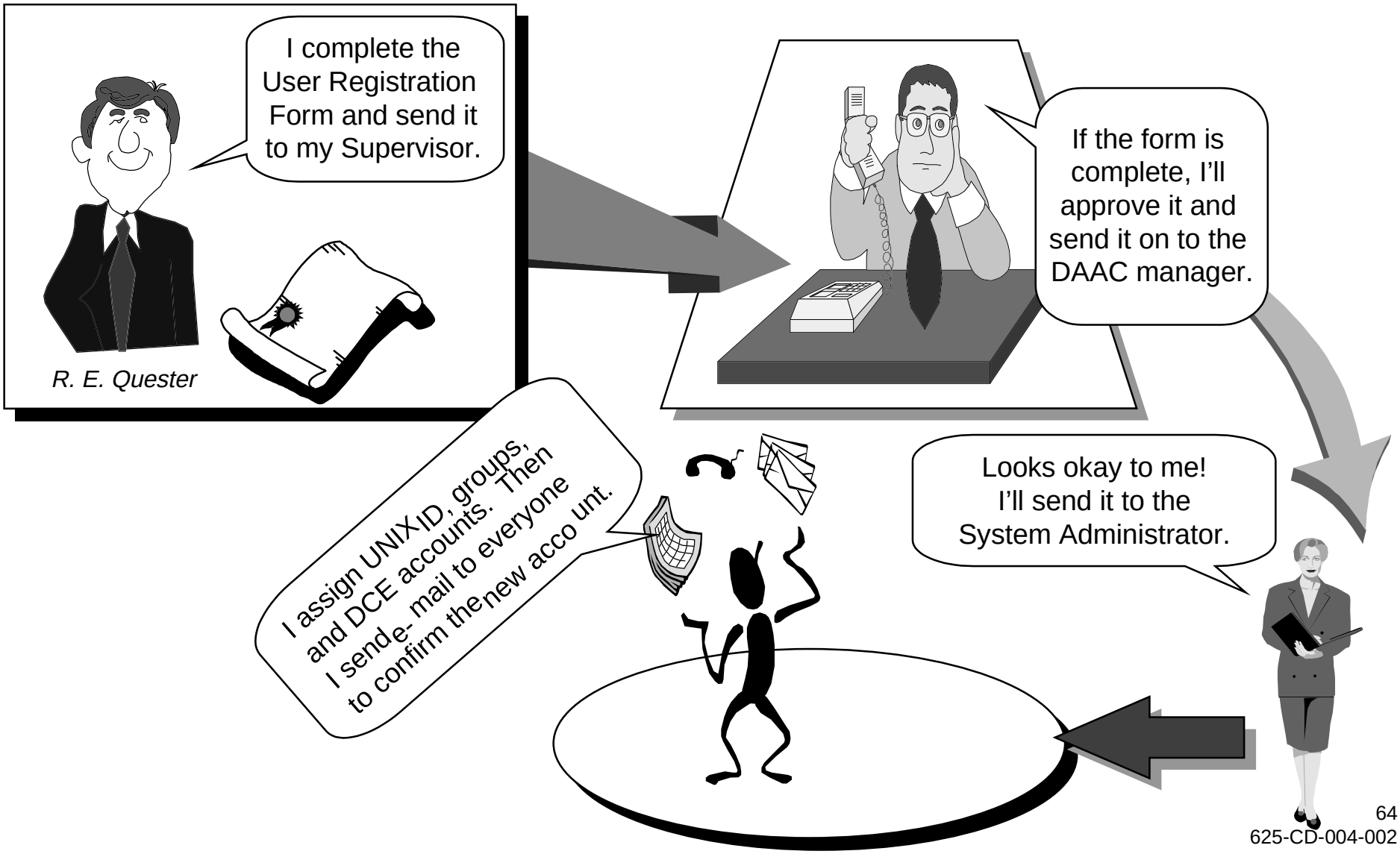
Tivoli Management Enterprise Desktop for Administrators



System Log Maintenance



New User Approval



/etc/passwd File

Logname

Encrypted Password

User ID Number

Group IDN umber

Personal Information

Home Directory

Login Shell

```
mresnick:$sy732az)[xyzz:510:1:Michael Resnick {x4076}:/home/mresnick:/bin/csh
jsmith:hY%dd98dwWrxPnm:511:1:Janet Smith {x0821}:/home/jsmith:/bin/csh
rknickerb::512:1:Robert Knickerbocker {x4111}:/home/rknickerb:/bin/csh
```

Empty field (no password)

/etc/group File

Group IDN umber

Logname

```
root::0:root
other::1:root,hpdb
bin::2:root,bin
sys::3:root,uucp
adm::4:root,adm
daemon::5:root,daemon
mail::6:root
lp::7:root,lp
users::20:root
nogroup:*:-2:
eb:*:10:
```

Group Member Lognames

Group Password Encrypted

/etc/auto.home File

Logname	Permissions	Location of Home Directory
dwashing	-rw,intr	acmn1sgi:/vol0/users/dwashing
jmangum	-rw,intr	acmn1sgi:/vol0/users/jmangum
mlynch	-rw,intr	acmn1sgi:/vol0/users/mlynch
ddavis	-rw,intr	acmn1sgi:/vol0/users/ddavis
rcampbel	-rw,intr	acmn1sgi:/vol0/users/rcampbel
spete	-rw,intr	acmn1sgi:/vol0/users/spete
kkleis	-rw,intr	acmn1sgi:/vol0/users/kkleis
echeung	-rw,intr	acmn1sgi:/vol0/users/echeung

ls -l Output Explanation

File permissions | Links | File Owner | Group | File size in bytes | Modification date/time | File name

```
drwxrwxrwx    3    mresnick    training    8192    Jun 14 08:34    archive
drwxr-xr-x   11    mresnick    training    4096    Jul 03 12:42    daacdata
-rw-rw-rw-    1    mresnick    training     251    Jan 02 1996     garbage
lrw-r--r--    2    jjones      admin      15237    Apr 30 20:07    junk
-rwxr--rw-    1    mresnick    training    5103    Oct 22 1994     trash
```

Access Permissions

d=directory l = symbolic link - = regular file	OWNER permissions	GROUP permissions	OTHER permissions
d	r w x	r w x	r w x
l	r w -	r w -	r w -
-	r w x	r - x	r w x
-	r w -	r - -	r - -

4 r=read *Look/copy/print*

2 w=write *Change/save/delete*

1 x=execute *Run commands/ use directory*

User Account Configuration Change Request Form

USER ACCOUNT CONFIGURATION CHANGE REQUEST FORM

Name of Requester:_____

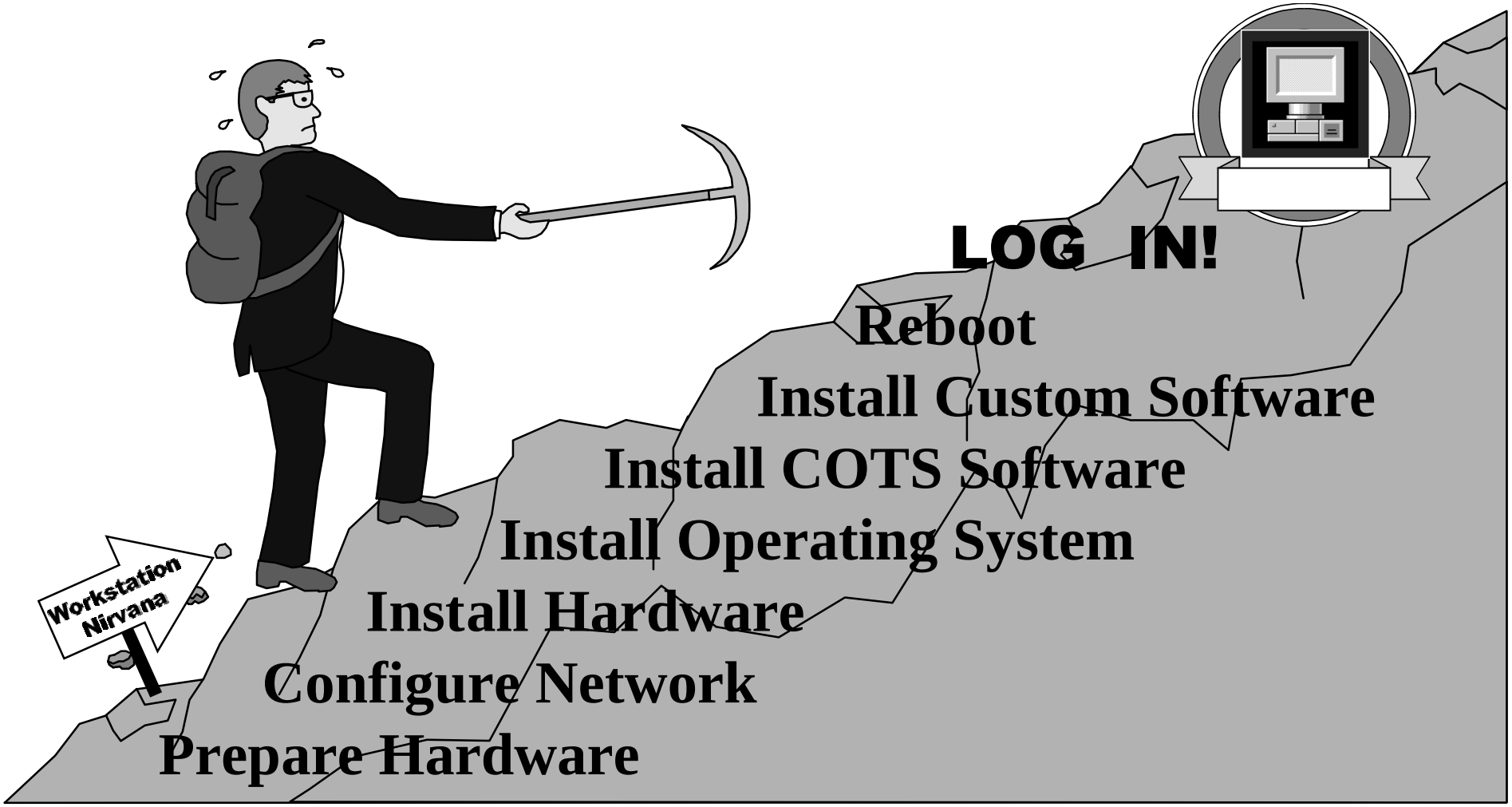
Reason for request: _____

CURRENT INFORMATION		CHANGE TO:
User ID:		
Office Address:		
Office Phone:		
Home Phone:		
E-Mail Address:		
UNIX Group ID:		
DCE Group ID:		
Login Shell:		

Date of Request: / / **Required by:** / /

Approval: _____ **Date:** _____

Workstation Installation Steps



Commercial Off The Shelf - COTS Products

The ECS Project software consists of various architectures in addition to - customized code, science software and COTS products

The project maintenance philosophy for software is to provide ECS centralized support for developed items and vendor-directed support for COTS software.

Log files are to be maintained for documenting all COTS installations and modifications.

Because each DAAC site is unique, COTS patches may be provided by the vendor to resovle a DAAC specific problem

CCB approval is required before COTS software upgrades can be loaded on any platform. DAAC CCB must be informed via CCR

What is DCE?

- **Distributed Computing Environment**
- **Provides a basis for building applications that are**
  - **Scalable**
  - **Secure**
  - **Distributed**
  - **Interoperable with other resources**
  - **Portable across heterogeneous platforms**
- **Offers tools for**
  - **Application developers (APIs)**
  - **Administrators (administrative commands)**
  - **Users (user commands)**

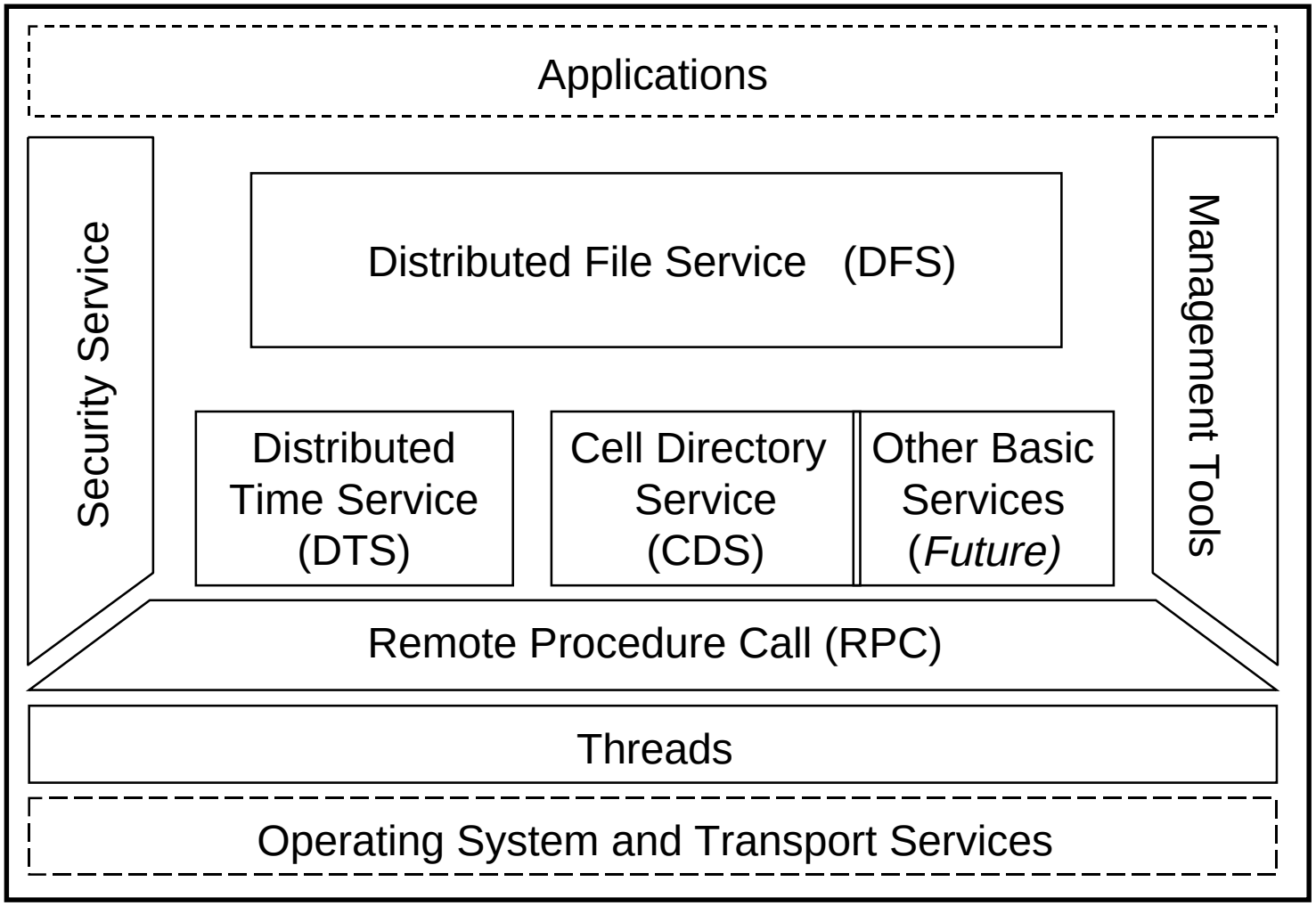
DCE Components

- DCE comprises these components
- Secure Core
  - Threads
  - Remote Procedure Call (RPC)
  - Naming
    - Cell Directory Service (CDS)
    - Global Directory Services (GDS)
    - Global Directory Agent (GDA)
  - Security Service
  - Distributed Time Service (DTS)

Additonal DCE Components

- **Extended Services**
  - **Global Directory Services (GDS)**
  - **Distributed File Service (DFS)**

Overview of DCE Technology Components



DCE Terminology

Cell = Collection of users computers, and other resources managed as a group

Distributed Computing Environment

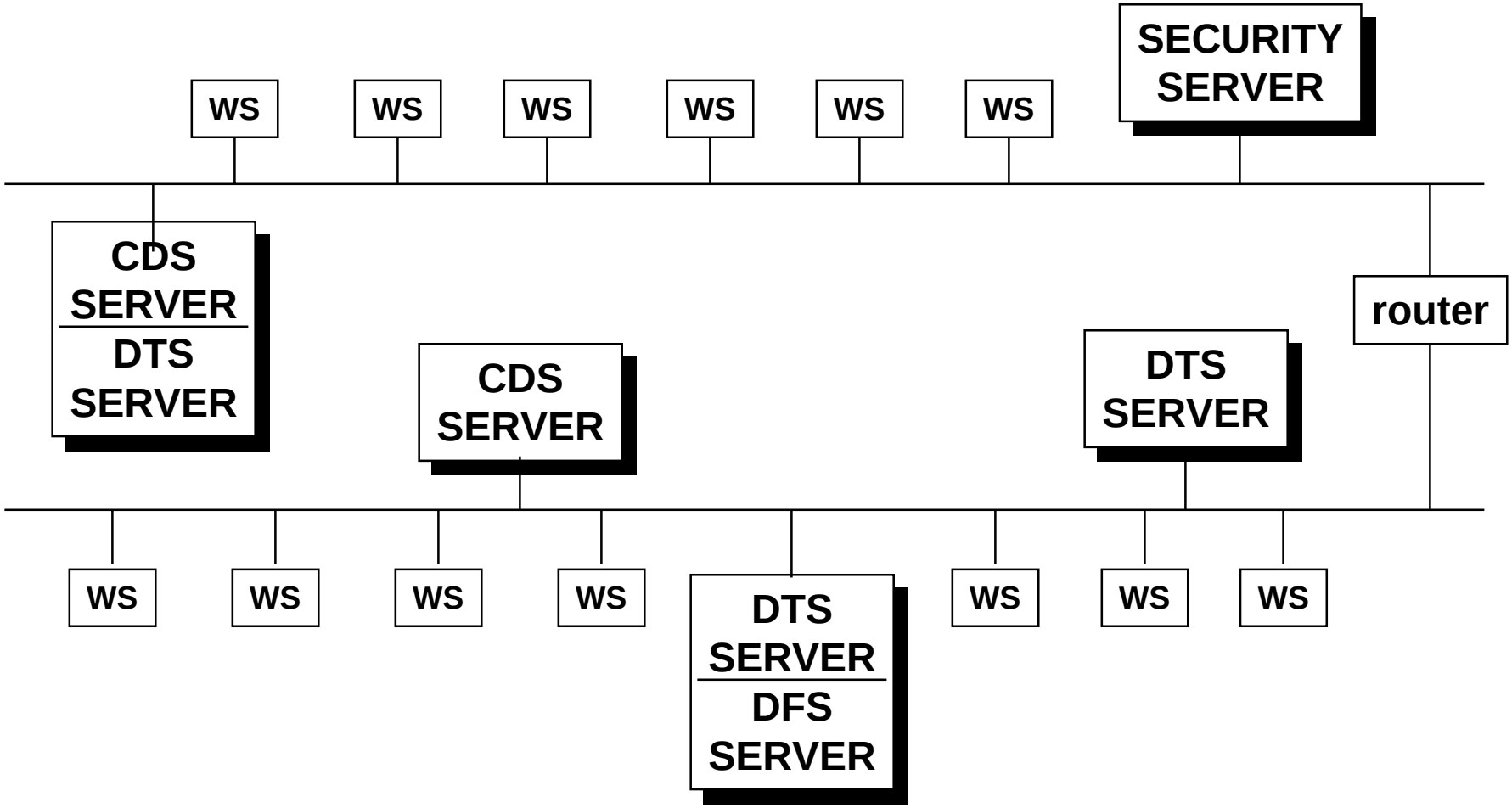
RPC = Remote Procedure Call

CDS = Cell Directory Service

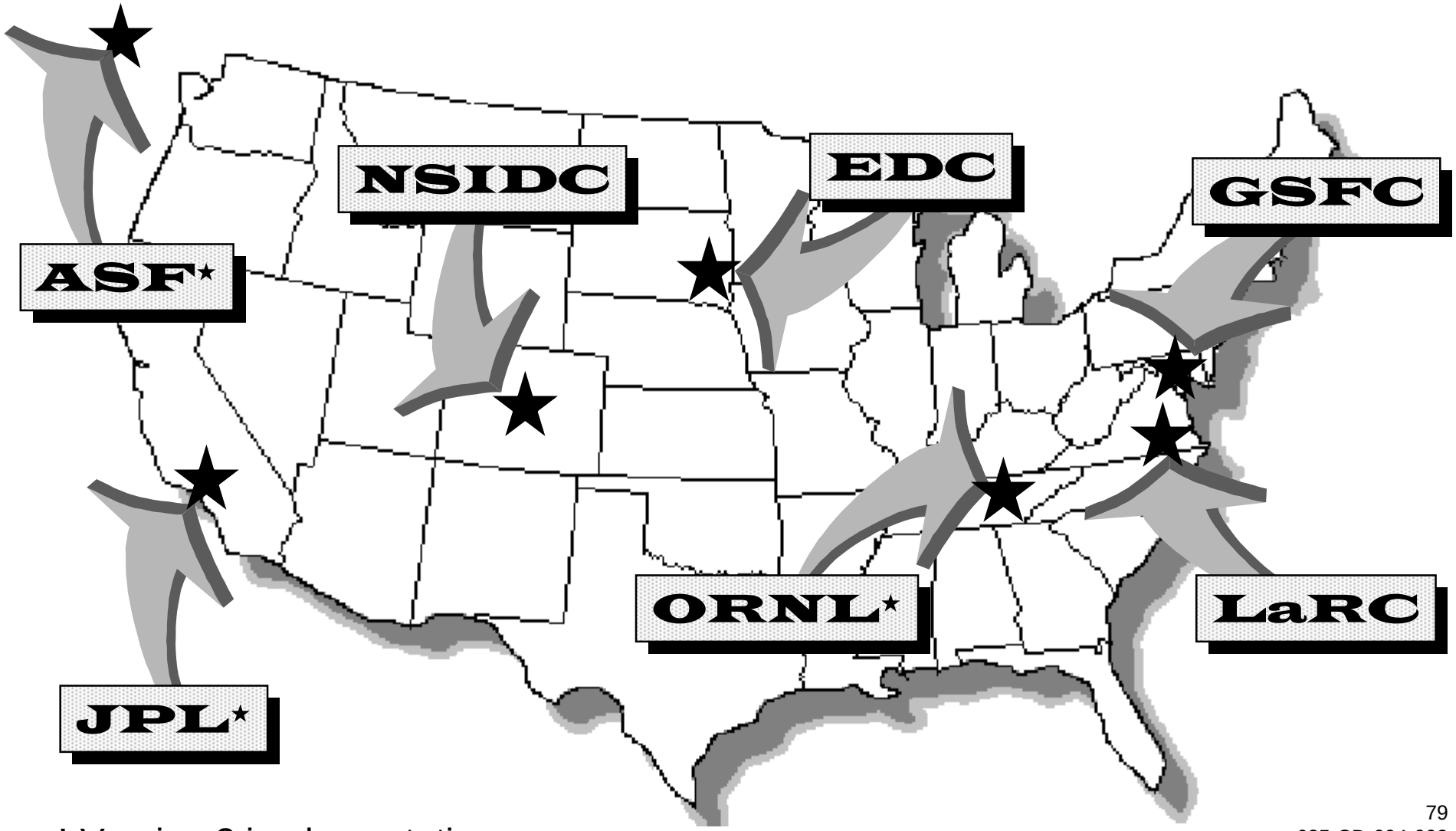
DTS = Distributed Time Service

DFS = Distributed File Service

Example of a DCE Cell

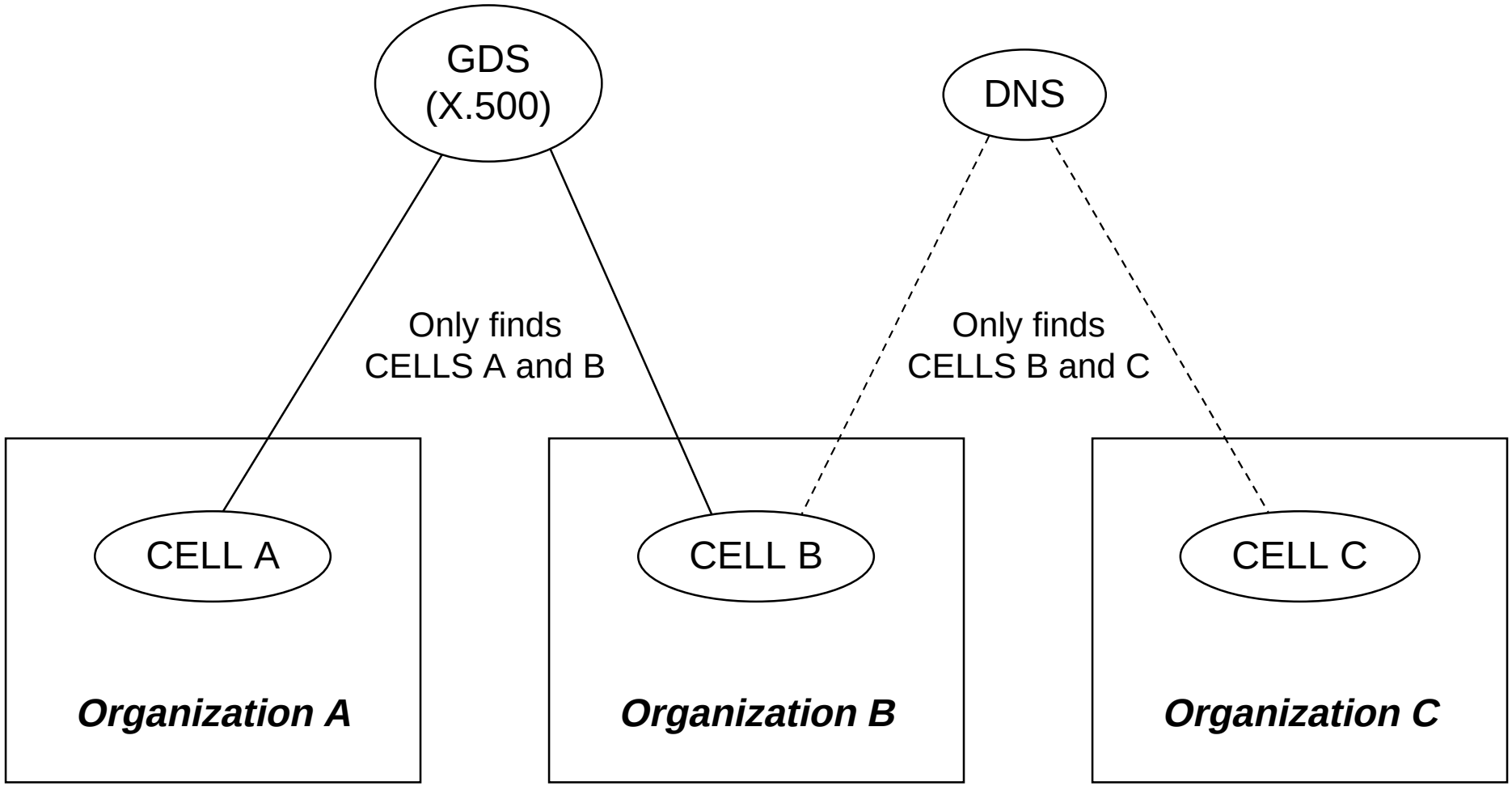


DCE Cells for Version 2

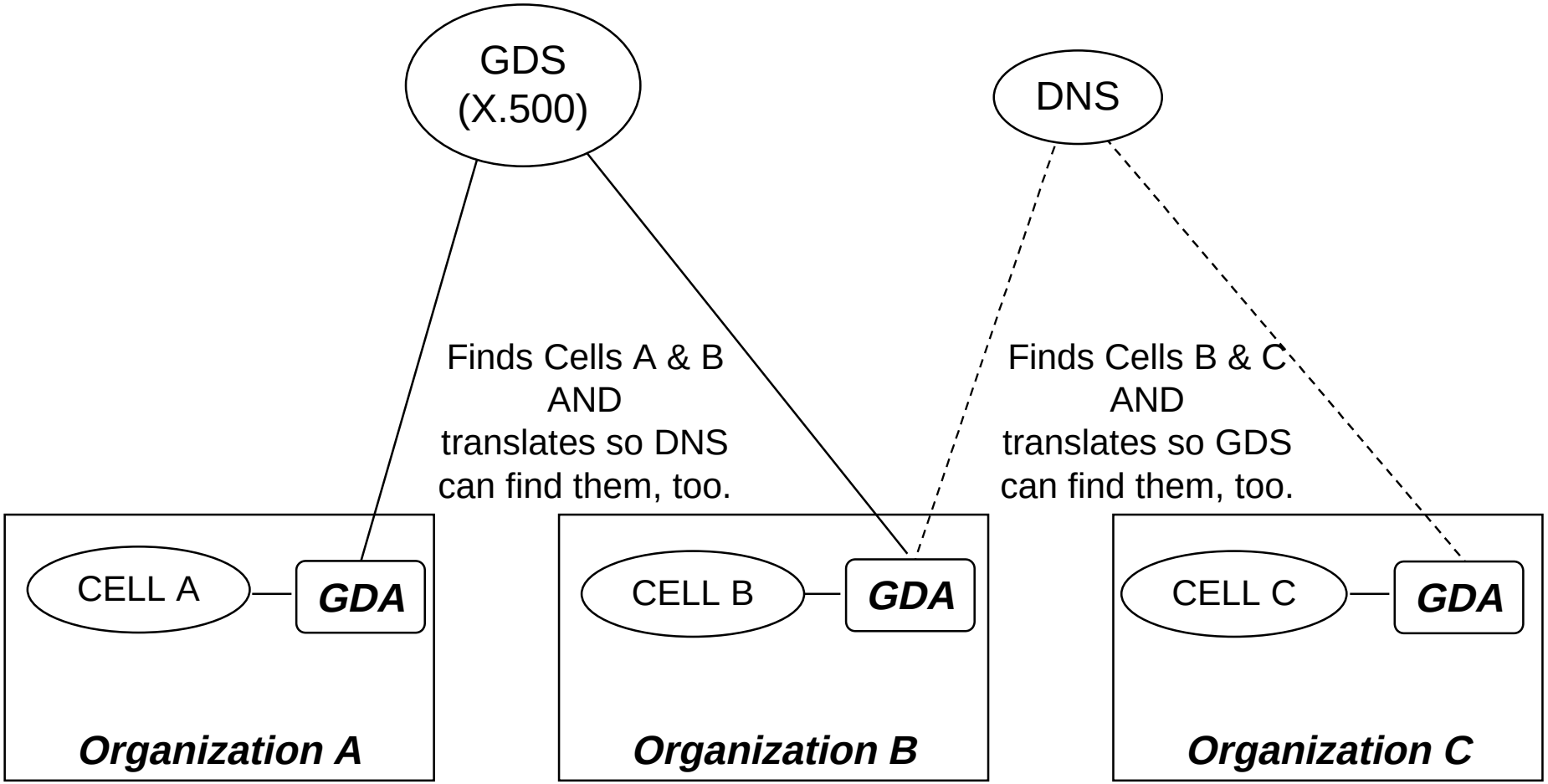


* Version 2 implementation

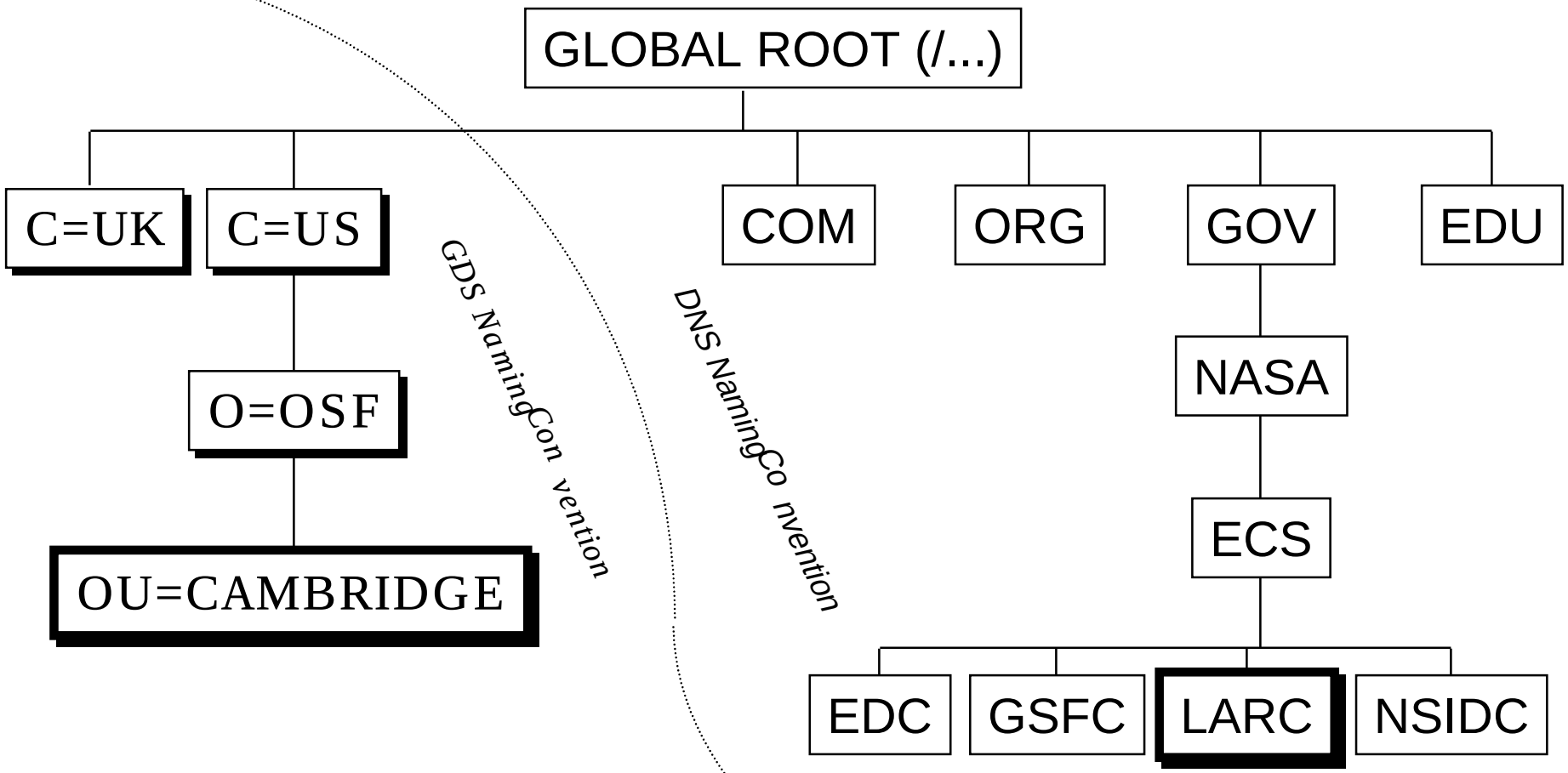
GDS and DNS Connect DCE Cell Namespaces



Global Directory Agents



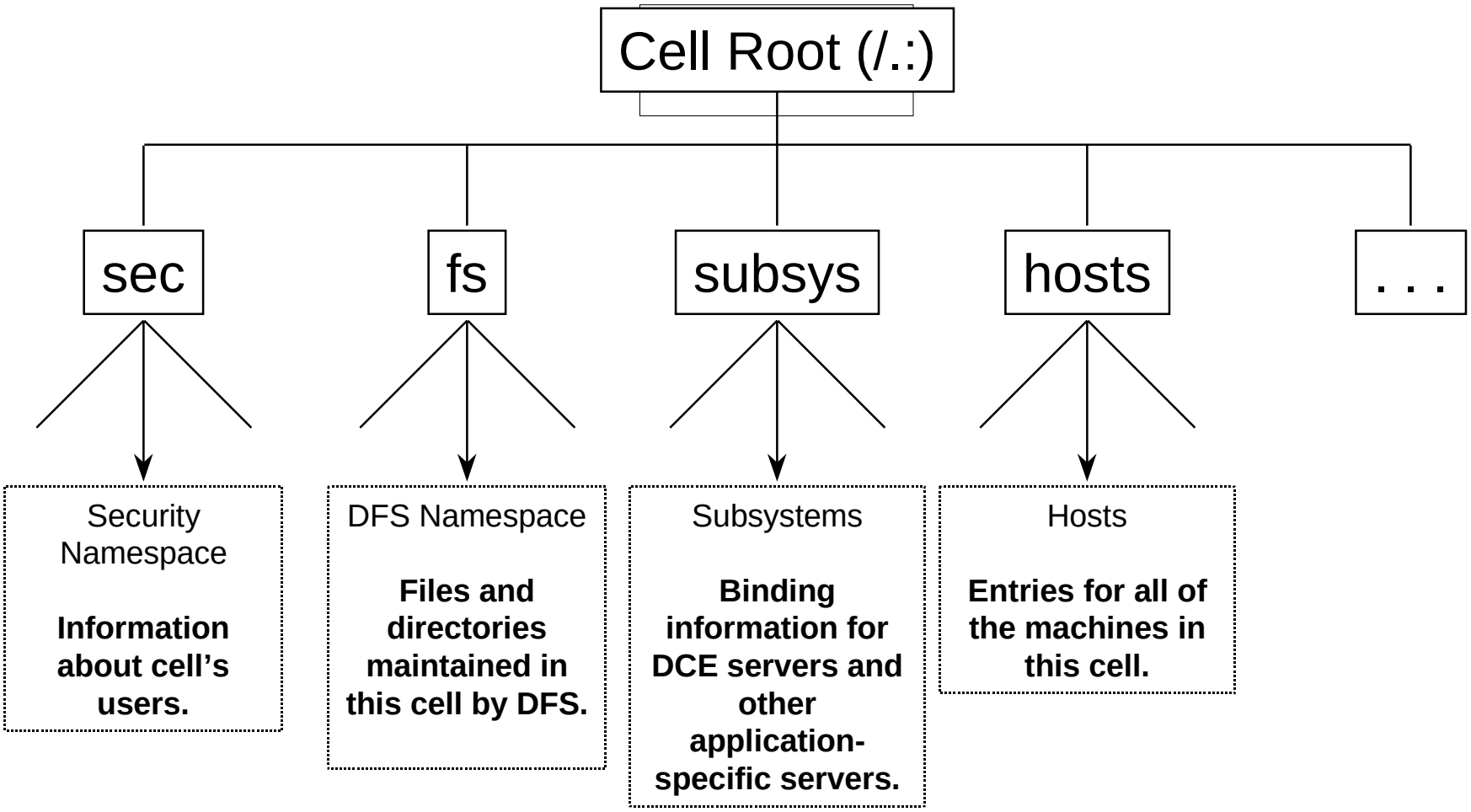
Global Namespace



/.../C=US/O=OSF/OU=CAMBRIDGE

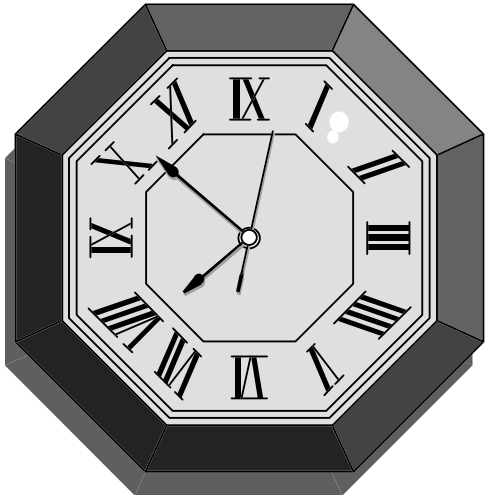
/.../LARC.ECS.NASA.GOV

Cell Namespace

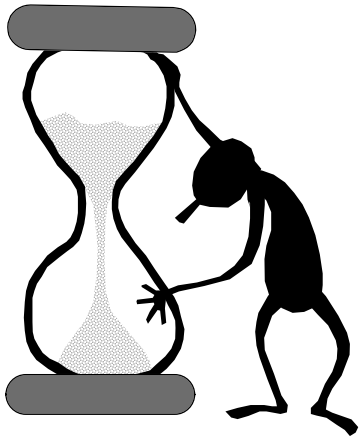


Distributed Time Service

- Provides precise, fault-tolerant synchronization of system clocks.
- Closely matches synchronized time to Coordinated Universal Time (UTC).
- Well integrated with the rest of DCE
- DTS can acquire high-quality time from the Internet Network Time Protocol



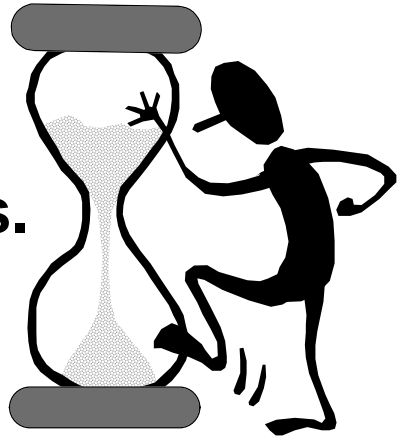
Distributed Time Service (cont.)



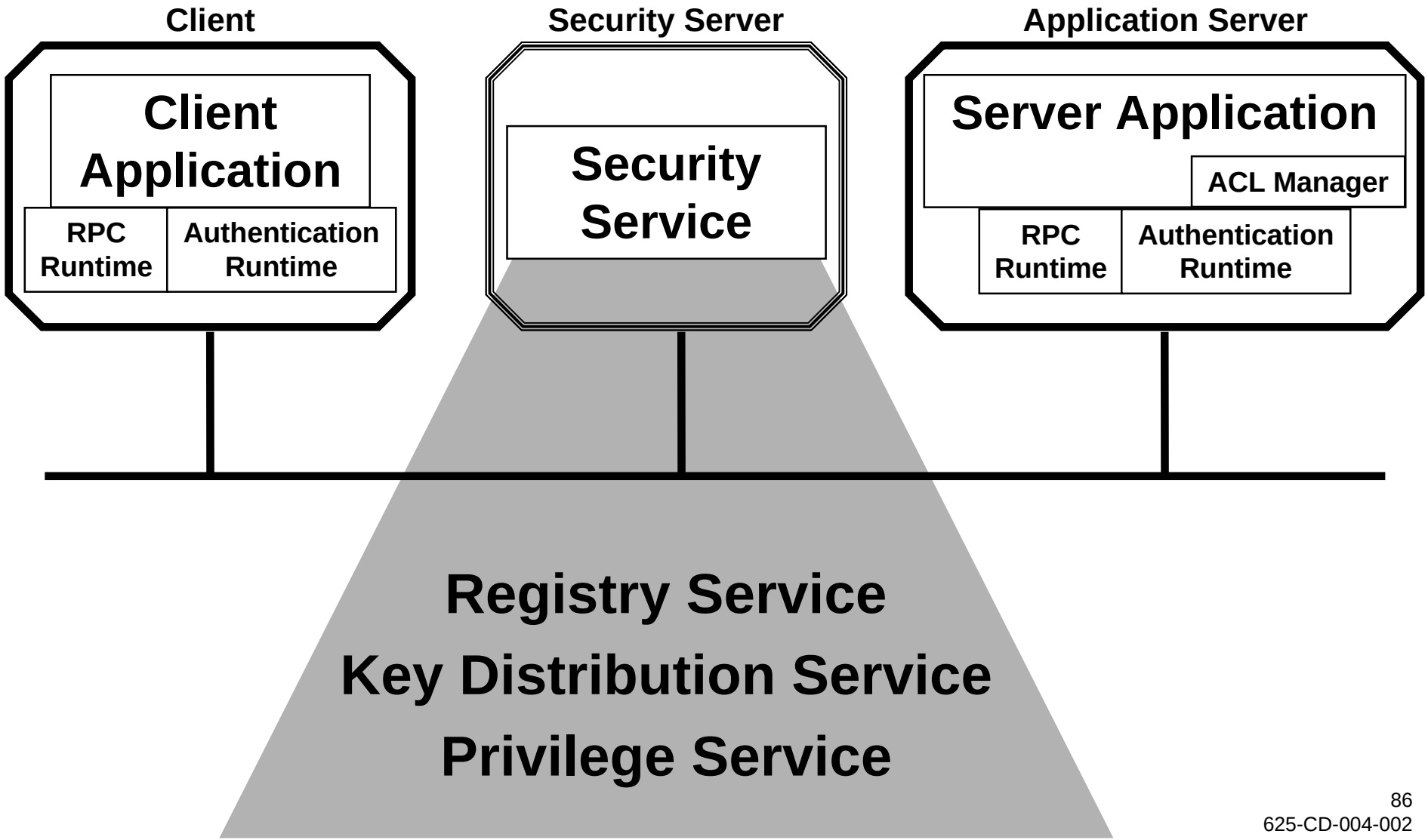
- A system is either a DTS SERVER or a DTS CLERK (client), but not both.
- When clock inaccuracy on each system exceeds a configured amount, resynchronization occurs.

– DTS clerks resync with DTS servers.

– DTS servers resync with other DTS servers.



DCE Cell Security Components



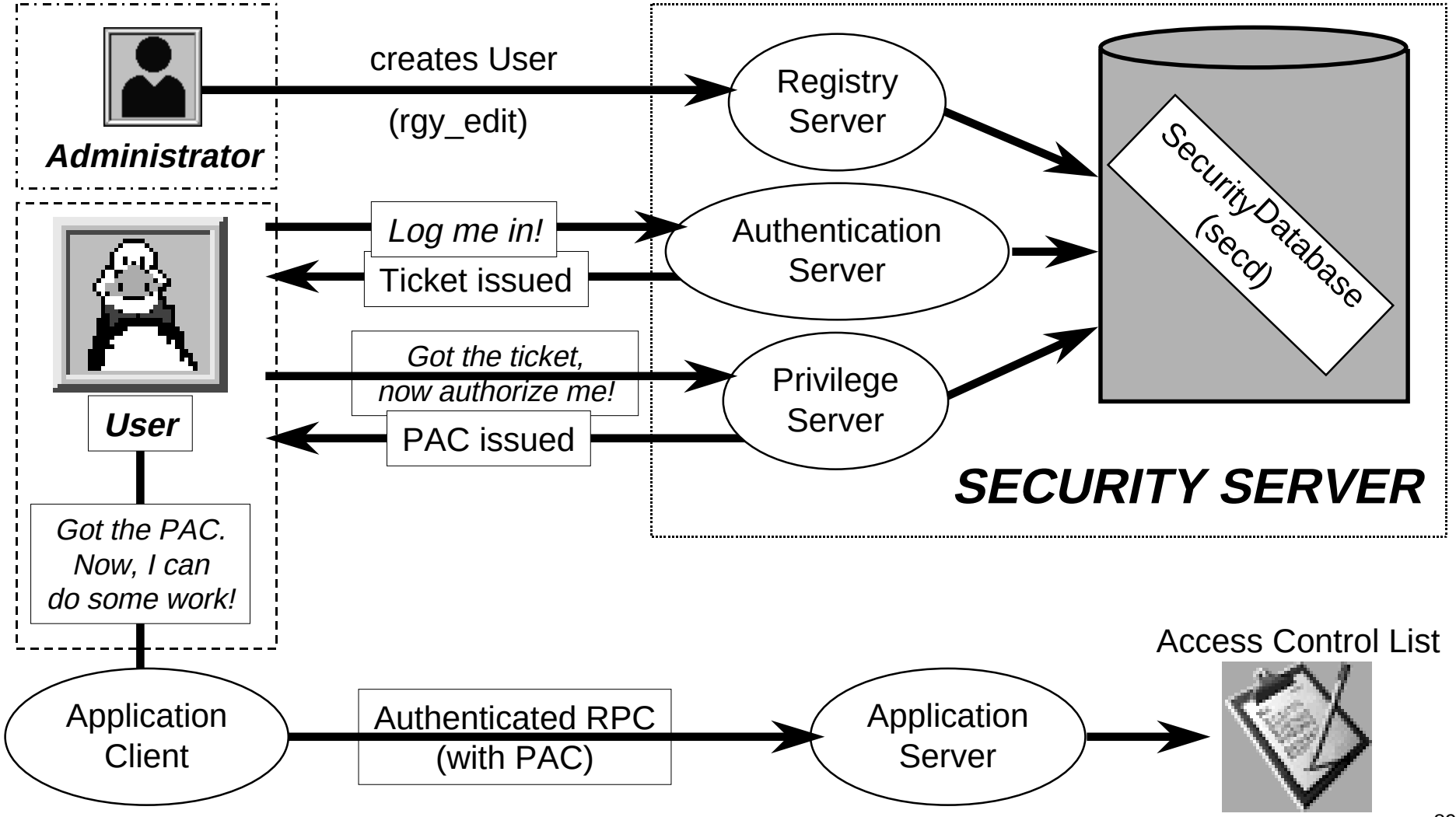
DCE Security Principles

- Every user and server is a PRINCIPAL.
- Every principal has a PRIVATE KEY.
  - Users = password provided at login.
  - Servers = password contained in a file.
- Every prinicpal has a UNIVERSAL UNIQUE IDENTIFIER (UUID).
- Each principal can belong to one or more groups.
- Each group is assigned a UUID.

Privilege Attribute Certificates (PACs)

- Every client principal has a PAC.
- Each PAC contains the PRINCIPAL's UUID.
- Each PAC contains the UUIDs of all the groups the principal belongs to.
- PACs cannot be forged.

How DCE Security Works

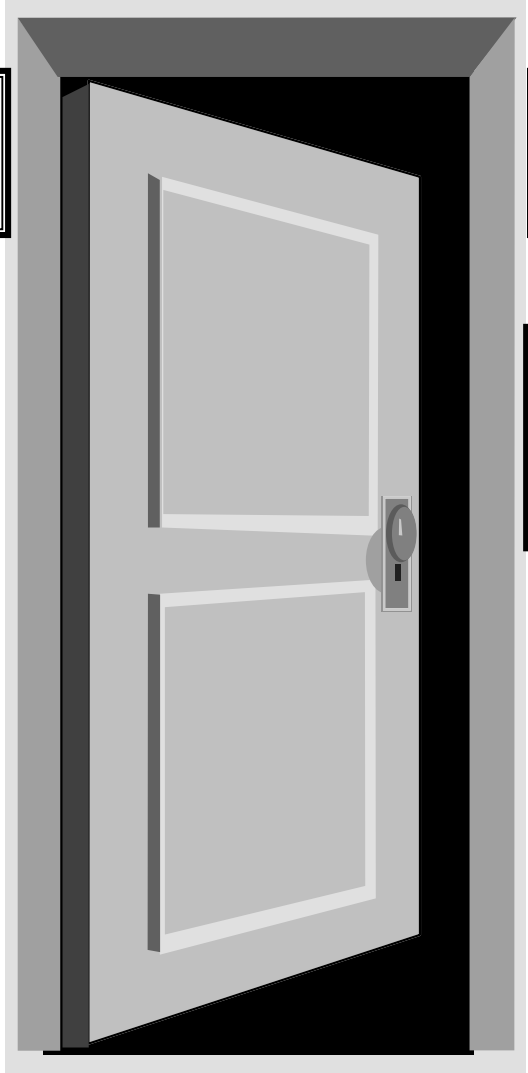


Security

OSF/DCE
for primary authentication

DCE Cell Manager
for groups and
system architecture

Kerberos & ACL
for authenticating users



TCP Wrappers
for network access control

npassword, Crack, SATAN
for password protection,
local and network access

Tripwire
for flagging unauthorized
file changes