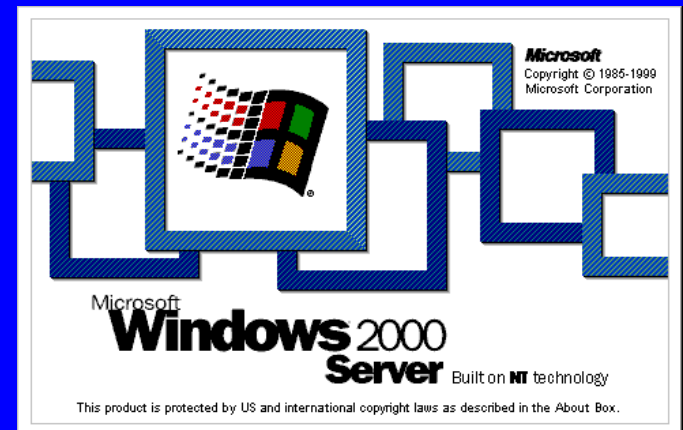


A large, vibrant firework explosion in shades of red, orange, and yellow dominates the upper center of the slide. To its left, several smaller firework trails in blue and white arc across the sky.

Windows 2000 Systems Administration

Bob Combs

bcombs@pcsiusa.com



What we'll discuss

- Windows 2000 Features
- Installation, DNS, Active Dir.
- Remote Access, DHCP, WINS
- File Quotas, DFS, EFS
- OUs, Groups, Policies
- COM+

Versions of Windows 2000

- Professional (workstation)
- Server (standard server)
- Advanced Server (clusters)
- Datacenter (hi-scale, future)

Windows 2000

Professional

- Desktop version
 - Single Processor
 - Plug & Play, Mobile User Support
 - NTFS, FAT32
 - Disk Defrag., Backup Utility
 - Kerberos 5
 - EFS, IPSec

Windows 2000 Server

- Practical baseline edition
 - Supports 2-way SMP
 - Active Directory Services
 - Group Policies
 - Admin via MMC & WMI
 - DFS, Disk Quotas

Windows 2000 Advanced Server

- High Availability Version
 - Supports 4-way SMP
 - Memory Support >4GB (64GB)
 - Clustering
 - Network Load Balancing
 - Component Load Balancing

Windows 2000 Datacenter Server

- High End Version
 - Support 16-way SMP (32 via OEM)
 - 64GB Memory Support

Installation

- H/W Requirements
 - Pentium 166 MHz or better
 - 64 MB (128 MB recommended)
 - 1 GB Disk minimum

Installation Preparation

- Check Hardware
Compatibility List (hcl.txt)
- NTFS vs. FAT32 vs. FAT

Installation Processes

- Load Setup into memory
- Start text-based setup
- Create/Format Win2k partition
- Copy files to disk
- Restart computer
- Start Setup Wizard

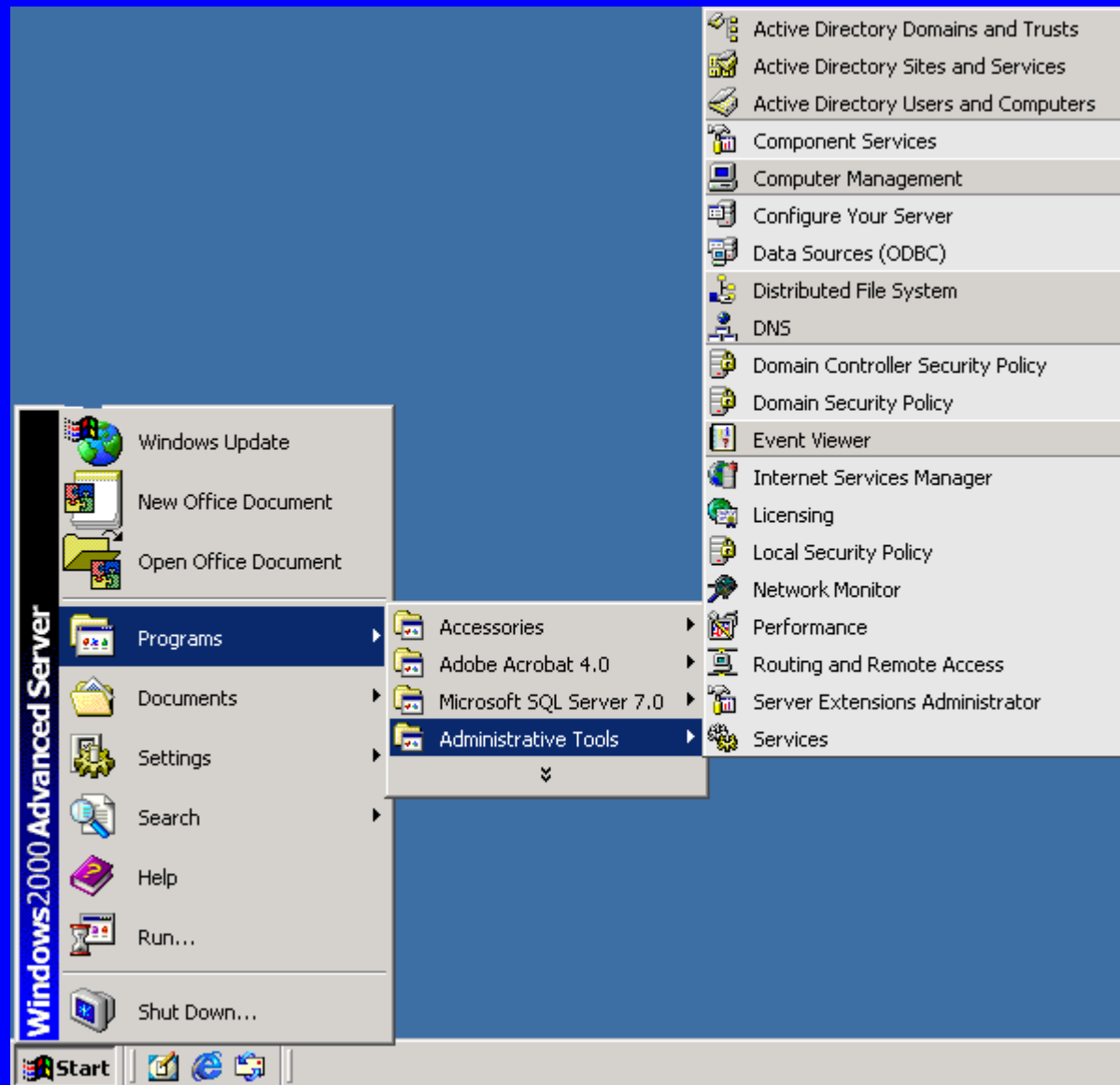
Installing Over Network

- Copy \i386 to a shared folder
- Client
 - Boot network client
 - Connect to shared folder
 - Run Winnt.exe
 - Boot from Setup boot diskettes
 - Install Windows 2000

Automating Installation

- Use Setup Manager to create Unattended.txt answer file
- Disk Image & Sysprep.exe

Administrative Tools



DNS

- Dynamic DNS (DDNS)
- Wizard aids creating zone
- Create in Active Directory or as Zone files (legacy)

DDNS

- Forward Lookups
- Reverse Lookups
- Caching, Iterative, Recursive
- Zone Transfers
 - Full
 - Incremental

DDNS Admin

The screenshot shows the Windows DNS console interface. The left pane displays a tree view with the following structure:

- DNS
 - GSISDC01
 - Forward Lookup Zones
 - gsistest.nfl.net**
 - Reverse Lookup Zones

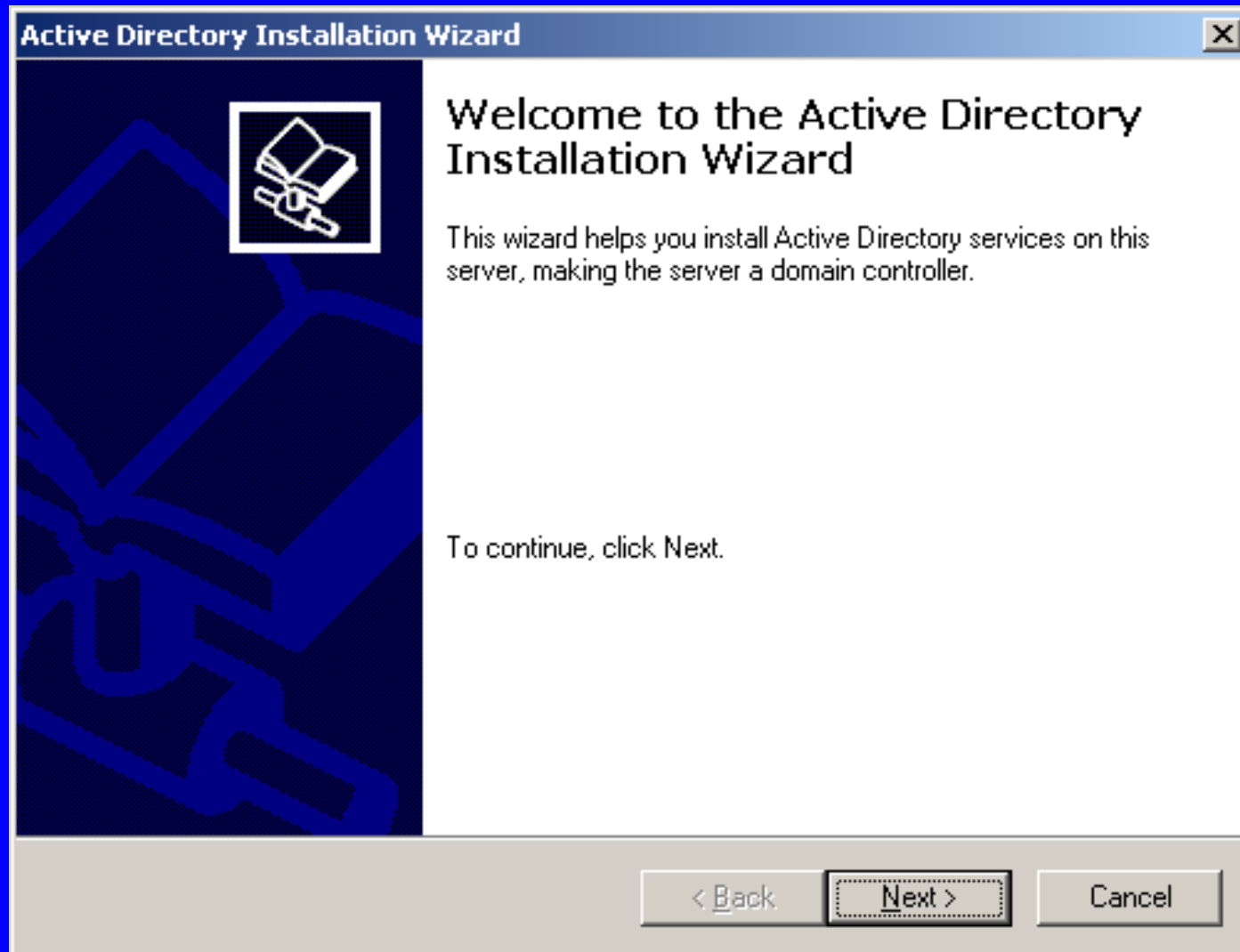
The right pane displays a table of DNS records for the selected zone:

Name	Type	Data
(same as parent folder)	Name Server	gsis00337b.gsis
(same as parent folder)	Name Server	gsis00314.gsis
(same as parent folder)	Name Server	gsis00329.gsis
(same as parent folder)	Name Server	gsis00342.gsis
(same as parent folder)	Host	209.201.63.133
(same as parent folder)	Host	172.16.2.10
(same as parent folder)	Host	209.201.63.144
(same as parent folder)	Host	209.201.63.242
(same as parent folder)	Host	172.16.2.13
(same as parent folder)	Host	172.16.2.12
(same as parent folder)	Host	209.201.63.230
(same as parent folder)	Host	209.201.63.227
(same as parent folder)	Host	209.201.63.229
(same as parent folder)	Host	172.16.2.11
GSIS00312	Host	209.201.63.227
GSIS00314	Host	172.16.2.13
GSIS00320	Host	172.16.2.10
GSIS00328	Host	209.201.63.144
GSIS00330	Host	209.201.63.227

Active Directory

- Replaces registry-based security account manager (SAM)
- 100% backwards-compatible
- Adds many new features
 - X.500 and DNS naming
 - Domain hierarchy
 - Extensible schema
 - LDAP access

Run “dcpromo” to create an Active Directory



AD Computers

The screenshot shows the Active Directory Users and Computers console window. The left pane displays a tree view of the directory structure for 'gsistest.nfl.net'. The 'Domain Controllers' folder is selected and expanded. The right pane shows a list of 12 computer objects under the 'Domain Controllers' folder.

Name	Type	Description
GSIS00312	Computer	
GSIS00316	Computer	
GSIS00328	Computer	
GSIS00329	Computer	
GSIS00331	Computer	
GSIS00333A	Computer	
GSIS00337B	Computer	
GSIS00340A	Computer	
GSIS00342	Computer	
GSISDC01	Computer	
NFL5W2K	Computer	
WALDO	Computer	

AD Users


The screenshot shows the Active Directory Users and Computers console. The left pane displays a tree view of the directory structure, with the 'Users' container selected. The right pane shows a list of 48 objects in the Users container, including the Administrator user and various security groups.

Name	Type	Description
Administrator	User	Built-in account for adm
Cert Publishers	Security Group ...	Enterprise certification
DnsAdmins	Security Group ...	DNS Administrators Gro
DnsUpdatePr...	Security Group ...	DNS clients who are pe
Domain Admins	Security Group ...	Designated administrat
Domain Comp...	Security Group ...	All workstations and se
Domain Contr...	Security Group ...	All domain controllers in
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Ad...	Security Group ...	Designated administrat
Group Policy ...	Security Group ...	Members in this group
GSIS00333A ...	Security Group ...	GSIS00333A Admins - f
GSIS00333A ...	Security Group ...	GSIS00333A Authors -
GSIS00333A ...	Security Group ...	GSIS00333A Browsers

User Properties

Administrator Properties [?] [X]

Member Of	Dial-in	MSMQ User Certificate	Environment
Sessions	Remote control	Terminal Services Profile	
General	Address	Account	Profile
Telephones	Organization		

 Administrator

First name: Initials:

Last name:

Display name:

Description:

Office:

Telephone number:

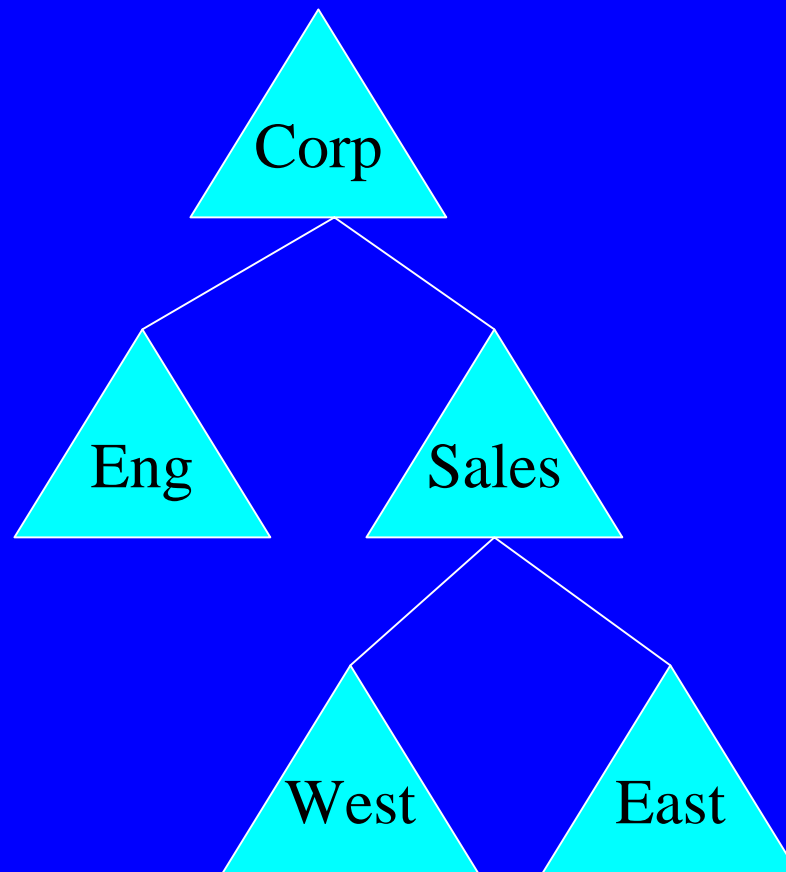
E-mail:

Web page:

AD Domains

- Tree hierarchy of domains
- Transitive trust among domains
- X.500 names are “attributed”
 - CN=Joe User, OU=Engineering, OU=NTDS, O=Microsoft, C=US
- Various DNS name formats
 - user@company.com
 - company.com/engineering/user

Hierarchy Example



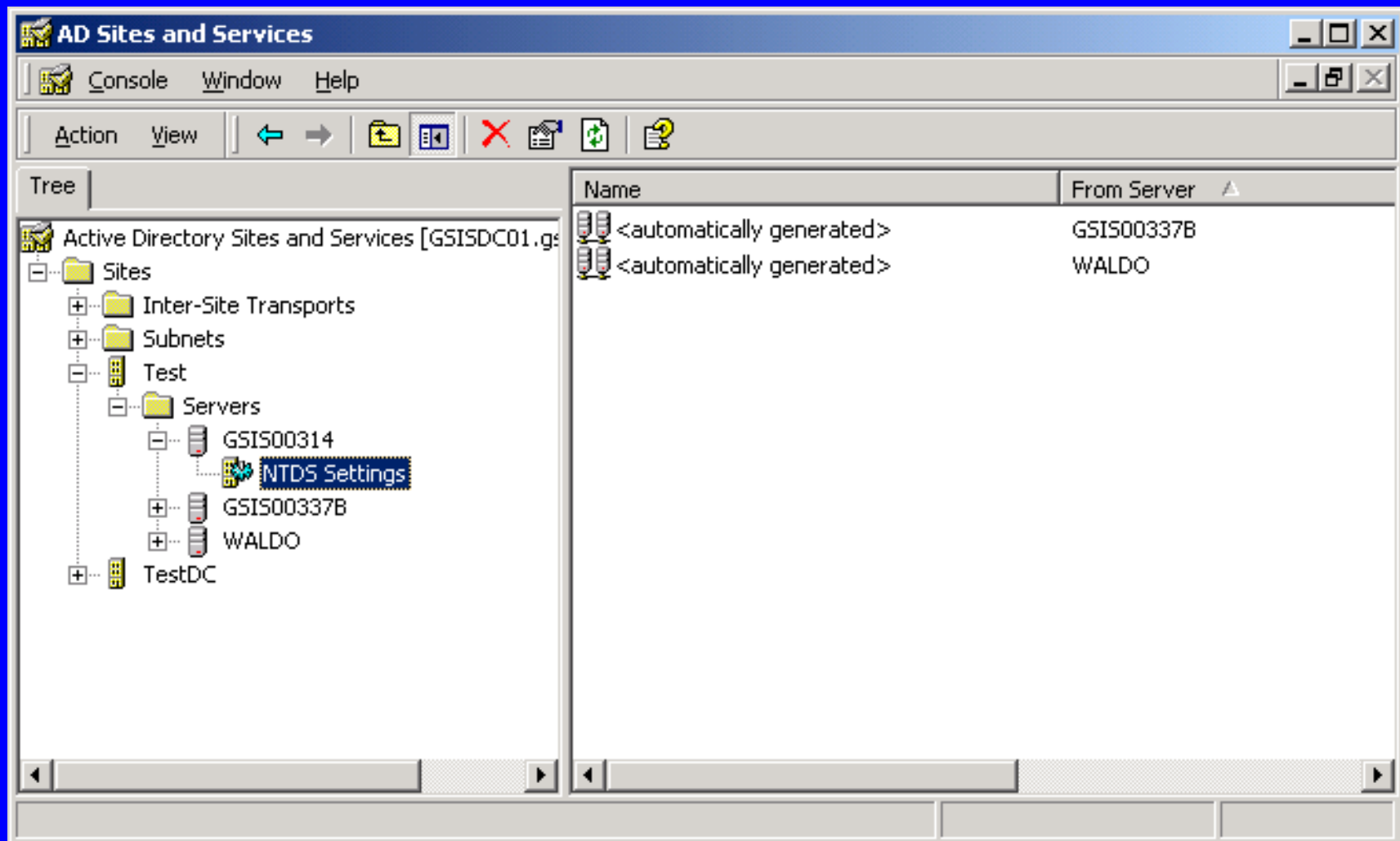
AD Site Links

- Site is one or more subnets
- Subnet can belong to only one site
- Site Link is a connection between two or more sites

Site Link Config

- Site Links are configured
 - Cost
 - Replication interval
 - Schedule

AD Sites and Services



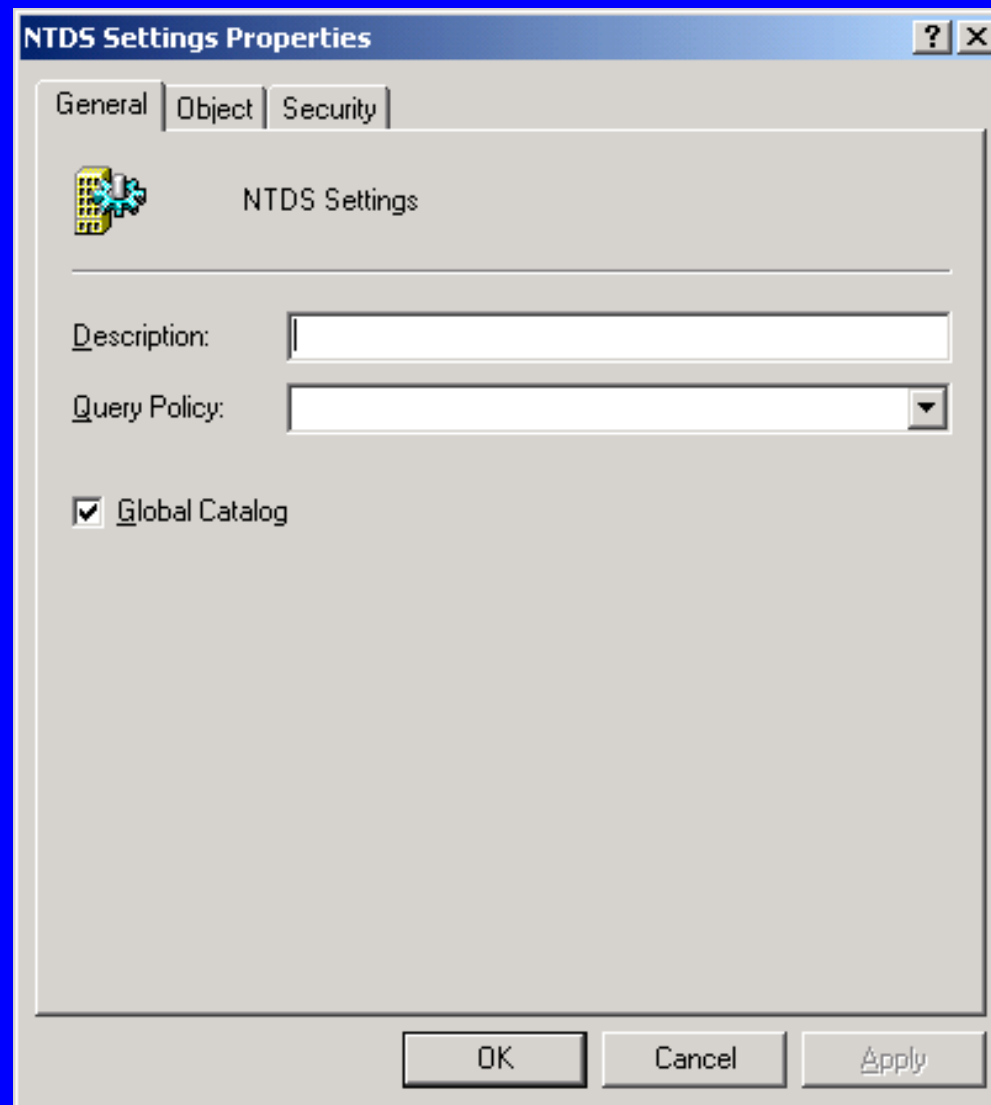
Active Directories

- 1st DC is default primary (FSMO)
- Other DCs do not contain Global Catalog
- Logon must access a GC
 - Administrator logon is exception

Global Catalog

- GC Servers improve network performance
 - Contain partial list of all AD objects
 - Allow logon to stay within site
 - Provide redundant logon servers
 - Contain Universal Groups

Global Catalog



User Groups

- Types of Groups
 - Local Group
 - Global Group
 - Universal Group
- Native mode vs. Mixed mode

Local groups can contain -

- User accounts (any domain)
- Other local groups
- Global groups (any domain)
- Universal groups
- Resources (from local domain)

Global groups can contain -

- User accounts (local domain)
- Other Global groups (local domain)
- Resources (from any domain)

Universal groups can contain -

- User accounts (any domain)
- Global groups (any domain)
- Other Universal groups (any domain)
- Resources (from any)

Group Tips

- Use Local groups to manage resources
- Use Global groups to manage user access
- Use Universal group to manage enterprise-wide policies

Network/Dial-up

- Create Dial-up Connections using Settings -> Network and Dial-up Connections -> Make New Connection

Remote Access Administration

- Extensible Authentication Protocol
 - Token Cards
 - CHAP (MD5-CHAP)
 - Transport Level Security (TLS)
- RADIUS
- IPSec
- L2TP (Layer 2 Tunneling Protocol)
- BAP (Bandwidth Allocation Protocol)

DHCP

- Loaded as additional service
- DHCP integrated with DNS
- GUI interface

WINS

- NetBIOS name server
 - No longer needed in Windows 2000
 - Support legacy Windows NT and 9x
 - Resolves NetBIOS names to IP
- Increased Fault Tolerance
 - Up to 12 WINS servers

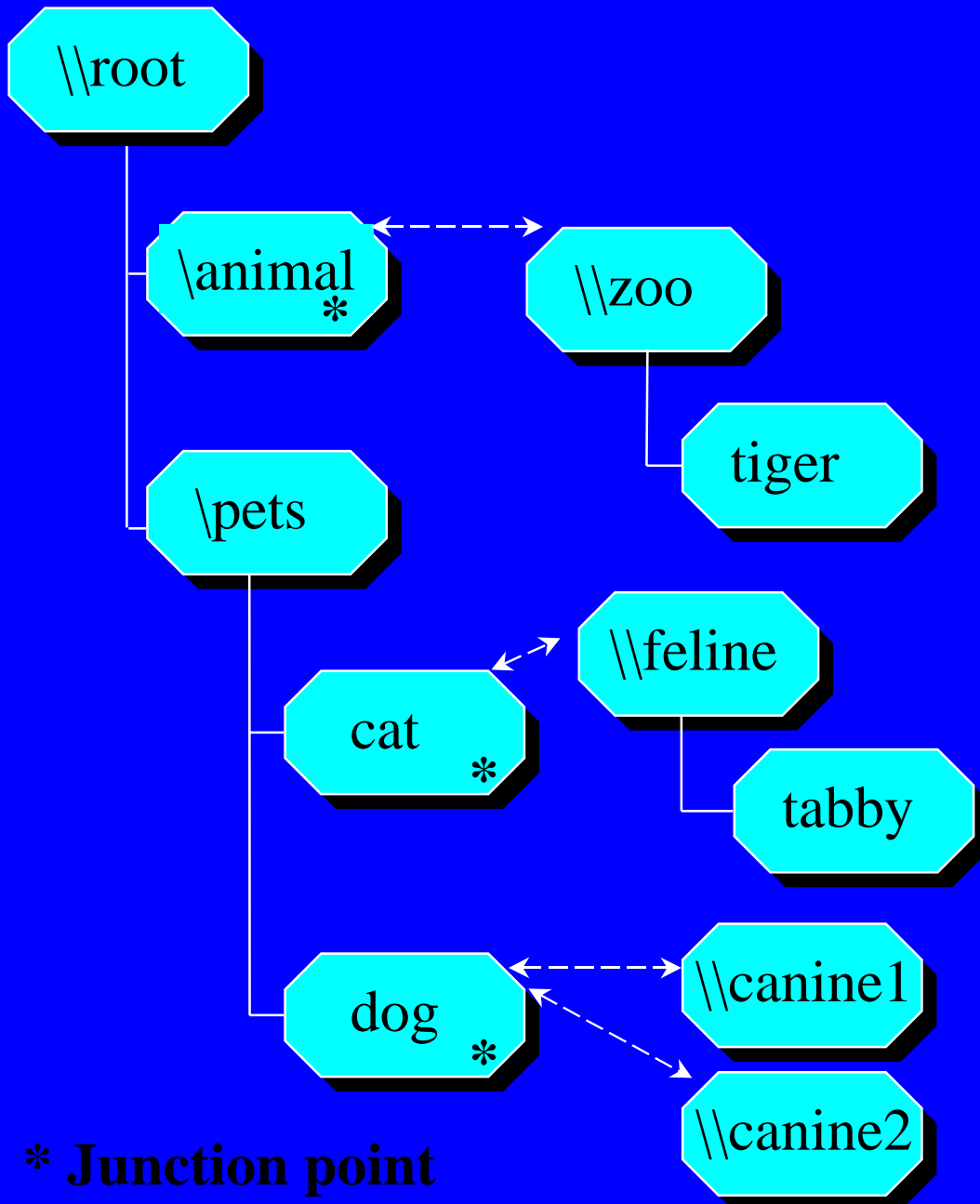
Distributed File System

- DFS
 - Stand-alone DFS stored on single machine
 - Fault-tolerant DFS stored in AD for multiple machines

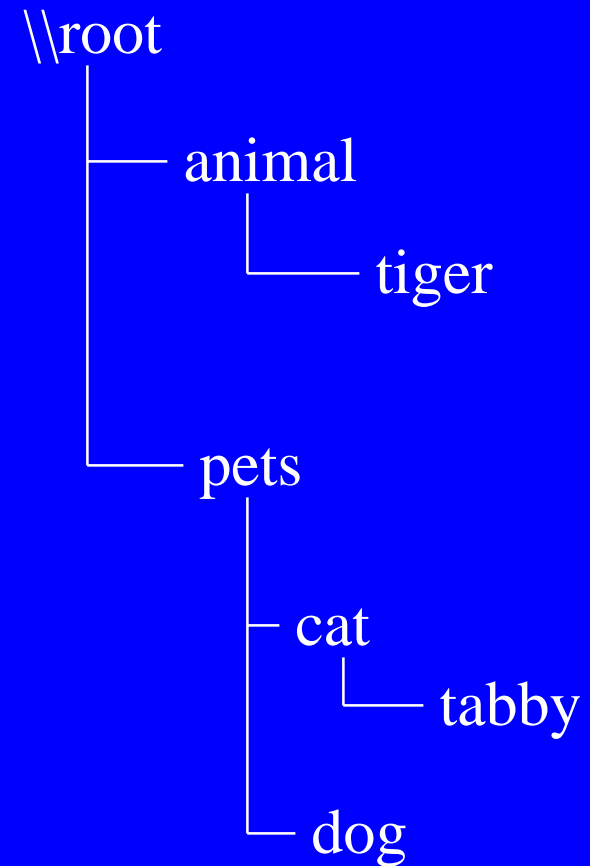
DFS

- Dfs root is a starting point of logical namespace
- Dfs root share is a junction point which maps to two or more alternate physical destinations

DFS junction links:



User sees:



Disk Quotas

- Set from Disk Management
- Usage based on ownership
- Quotas do not use compression in calculation
- Free space for applications base upon quota limit

Encrypting File System

- EFS
 - Public key encryption based
- Cipher command line utility
 - `cipher [/e] [/s:folder] [filename] ...`
- Recovery Agent
 - Third party person who can open file

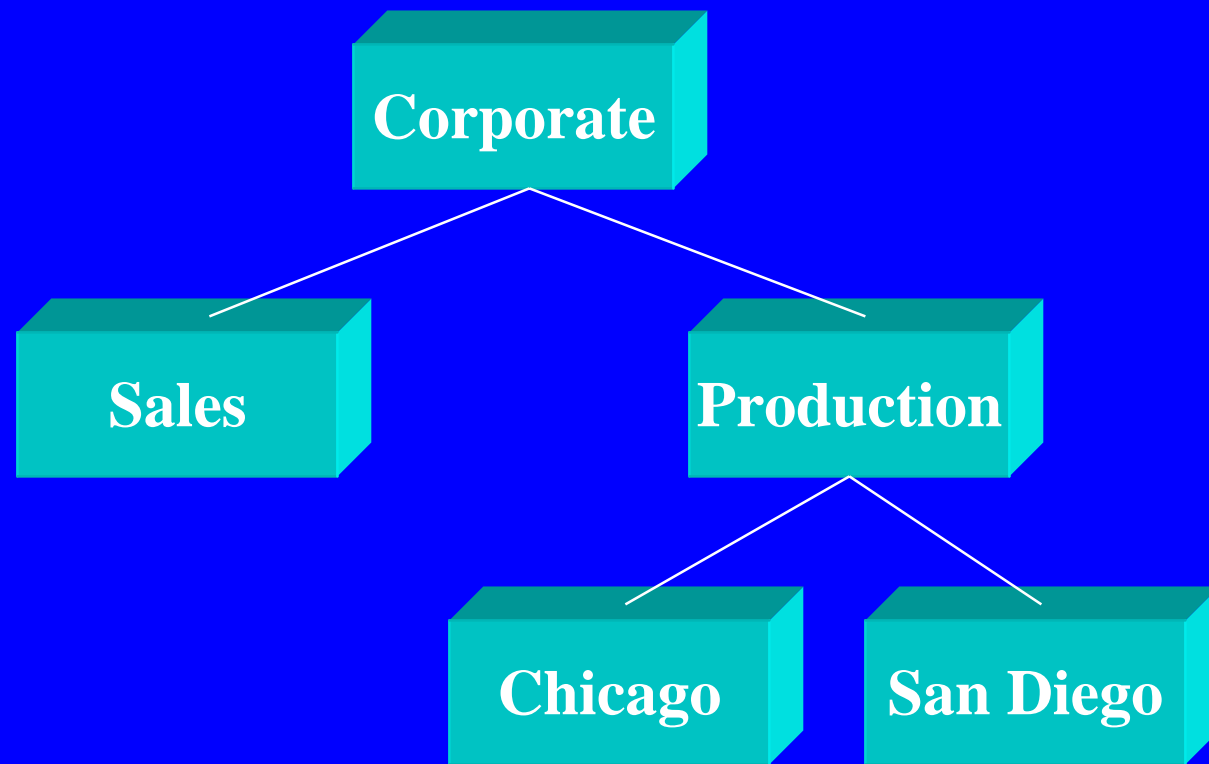
Group Policies

- Windows 2000 encompasses both Users and Computers
- Can still differentiate either
- Use Organizational Units in hierarchical fashion w/policies

Organizational Units

- OUs
 - created from AD Users and Computers
 - Select tree node and right-click for New -
> Organizational Unit
- Can apply Group Policies to OUs for finer control of users

Organizational Units



OU=Corporate, OU=Production, OU=San Diego

COM+ Services

- Role-based security
- Threading models
- Transaction Service (replaces MTS)
- Component Load Balancing (CLB)
- Object Pooling
- Queued components (uses MSMQ)
- Just-In Time (JIT) activation
- Programmatic component administration

Windows 2000

