2142 What's New in Windows Server 2003 Active Directory

Gary Olsen, MCSE
Consultant
Americas Escalation Team
HP Services
gary.olsen@hp.com

HP WORLD 2003
Solutions and Technology Conference & Expo

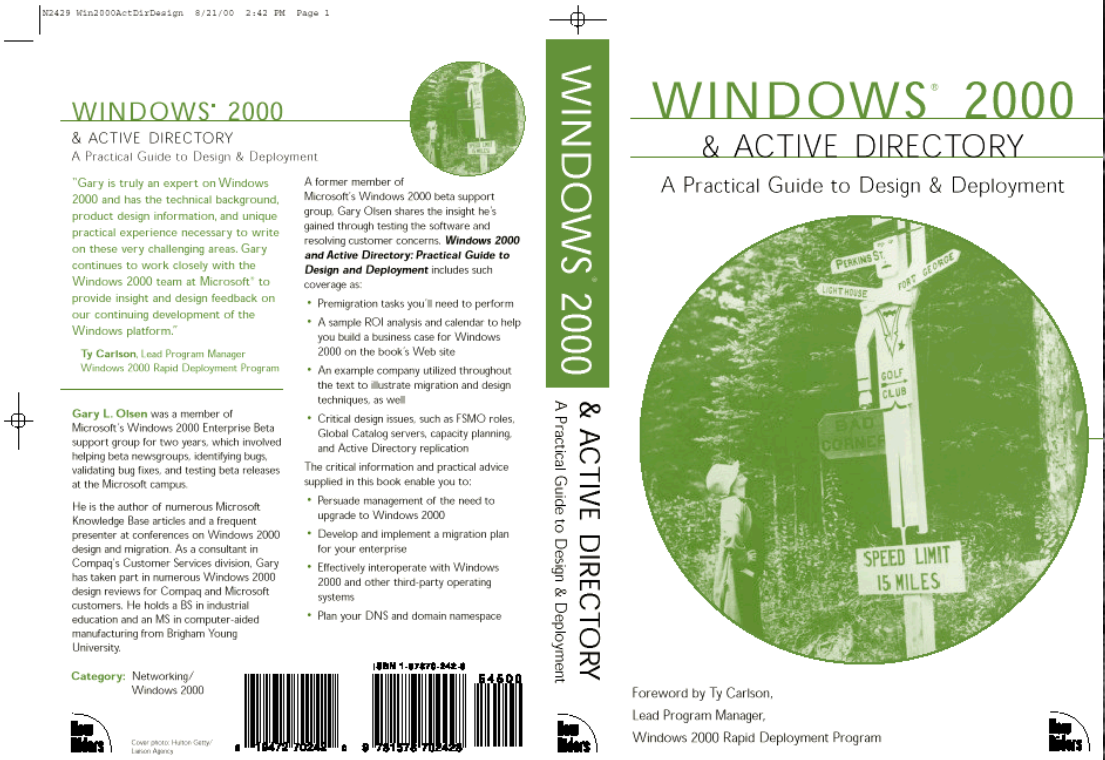
Other Sessions

- **2209 Kerberos Basics for Windows Administrators**
  - 12:10 – 1:20 Immediately following this session in this room
- **1183 Windows 2003 Migration Strategies**
  - 5:20-6:30 in this room (B308)

Windows 2000: Active Directory Design and Deployment

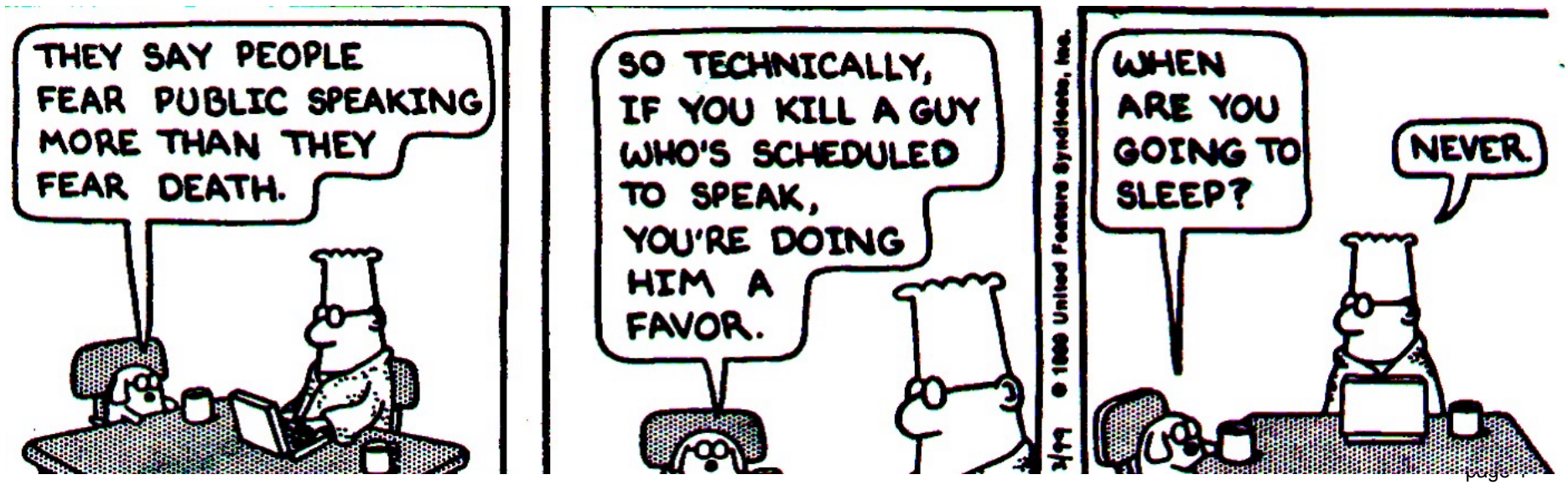
HP WORLD 2003
Solutions and Technology Conference & Expo

Author: Gary Olsen
Publisher: New Riders
ISBN: 1578702429



Windows 2003 Server

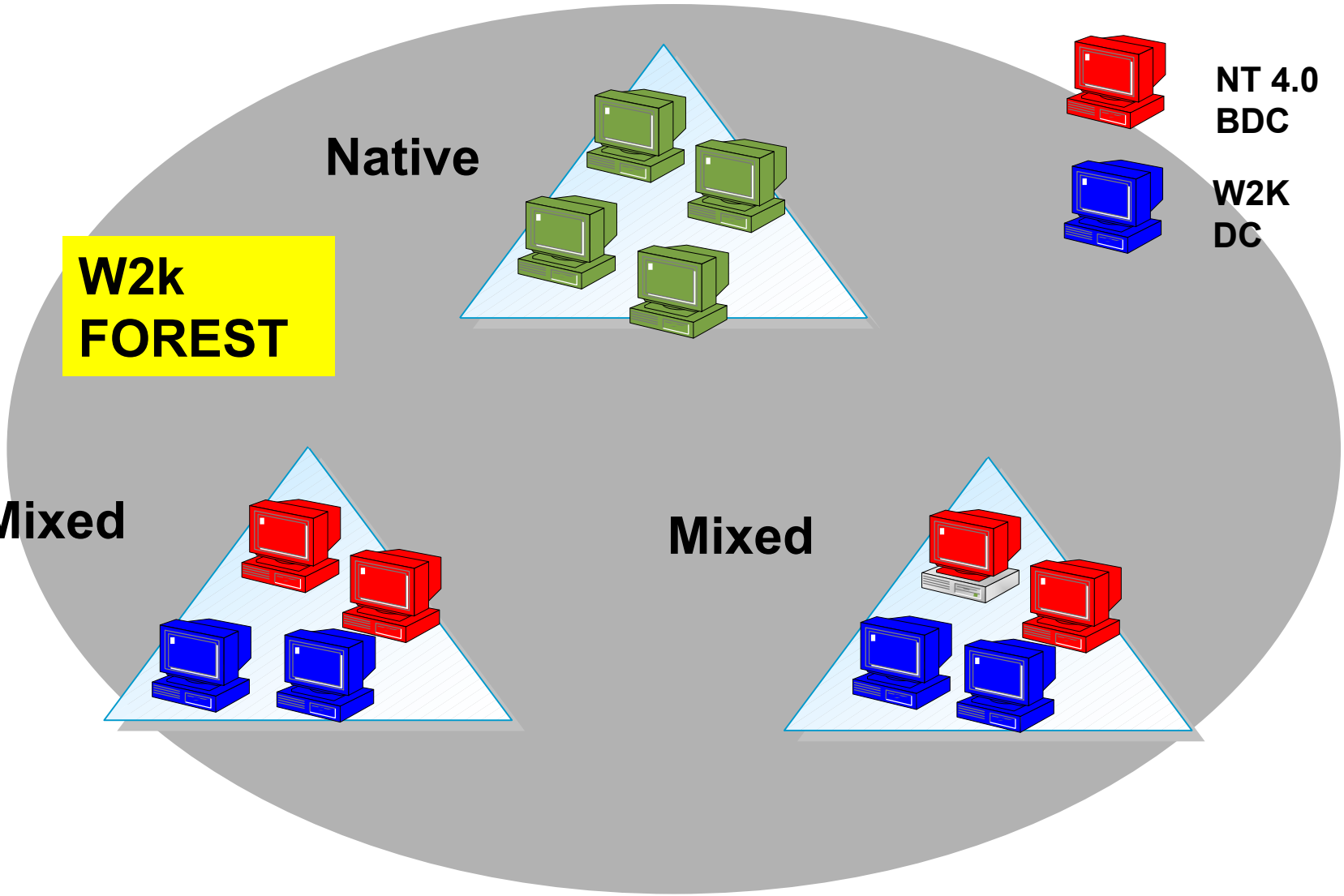
- Isn't it just a bunch of bug fixes?
- What exactly are the "enhancements" and how will they help me?
- Is it worth my while to examine it?
- What are the migration paths?



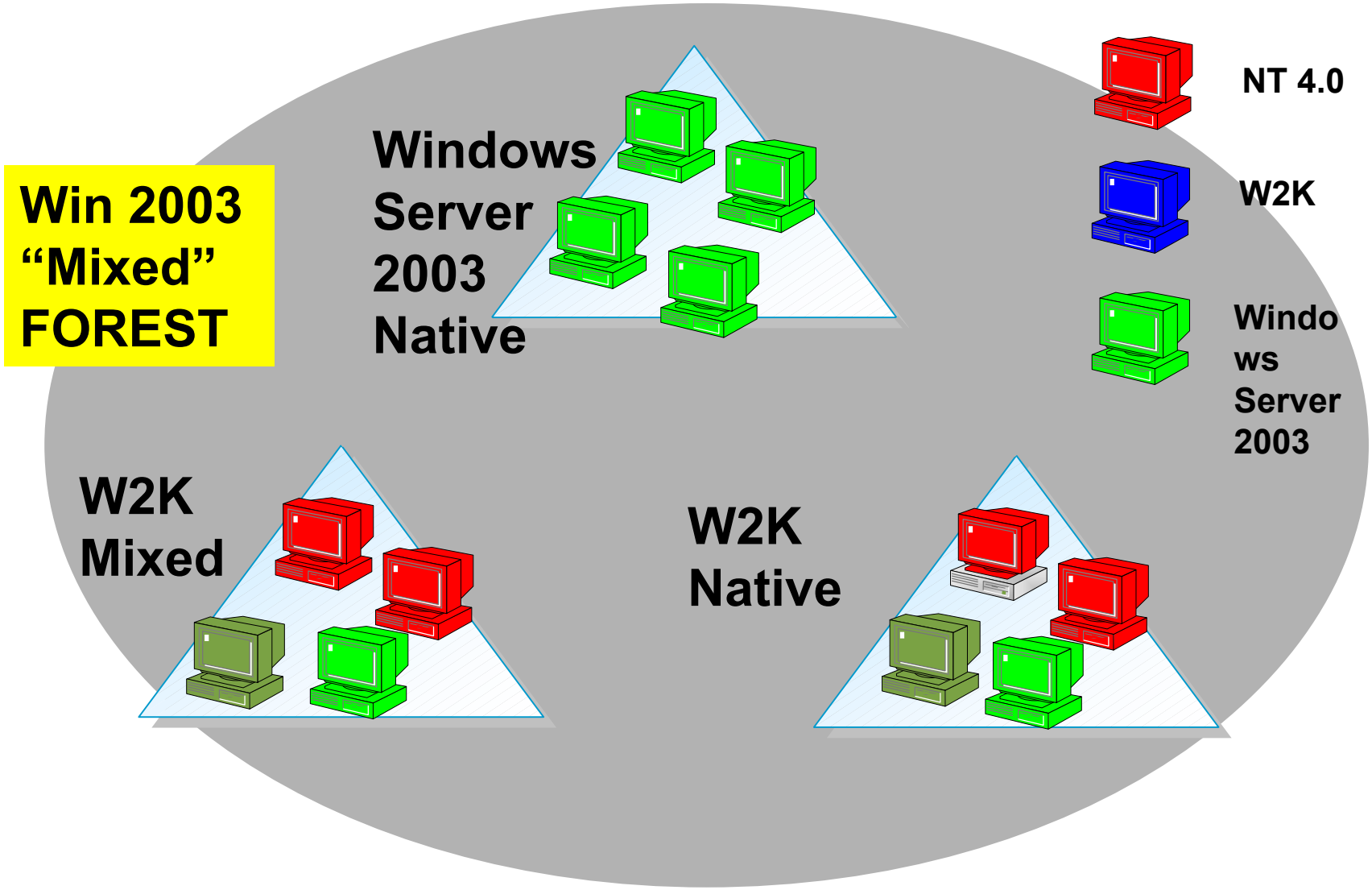
Functional Modes

- **Windows 2000**
  - Mixed
  - Native
- **Windows 2003**
  - Domain
    - Windows 2000 Mixed, Native
    - Windows 2003
  - Forest
    - Windows 2000 Native
    - Windows 2003
- **More on this in the Migration Session #1183**

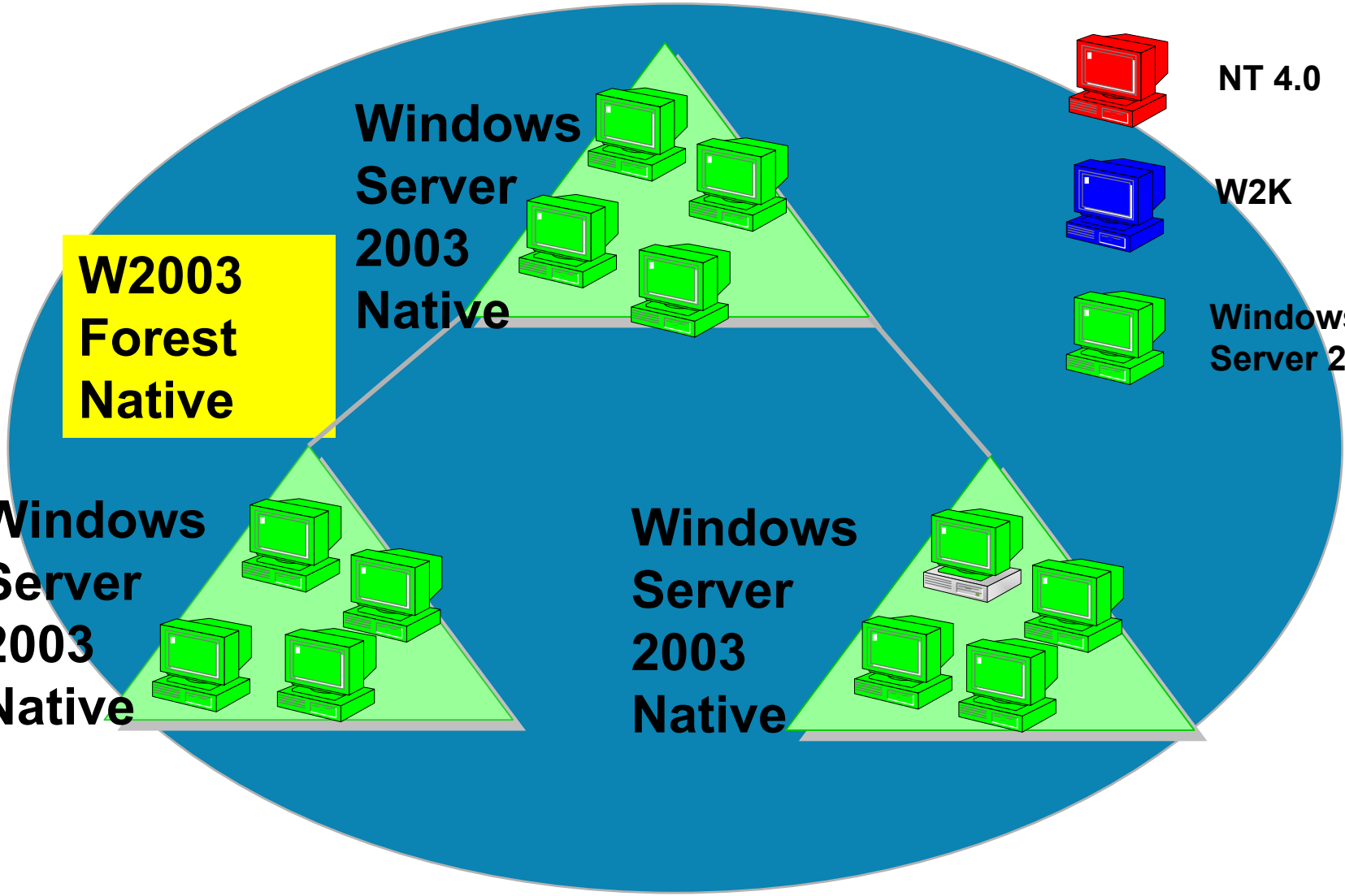
Windows 2000 Native/Mixed Domains



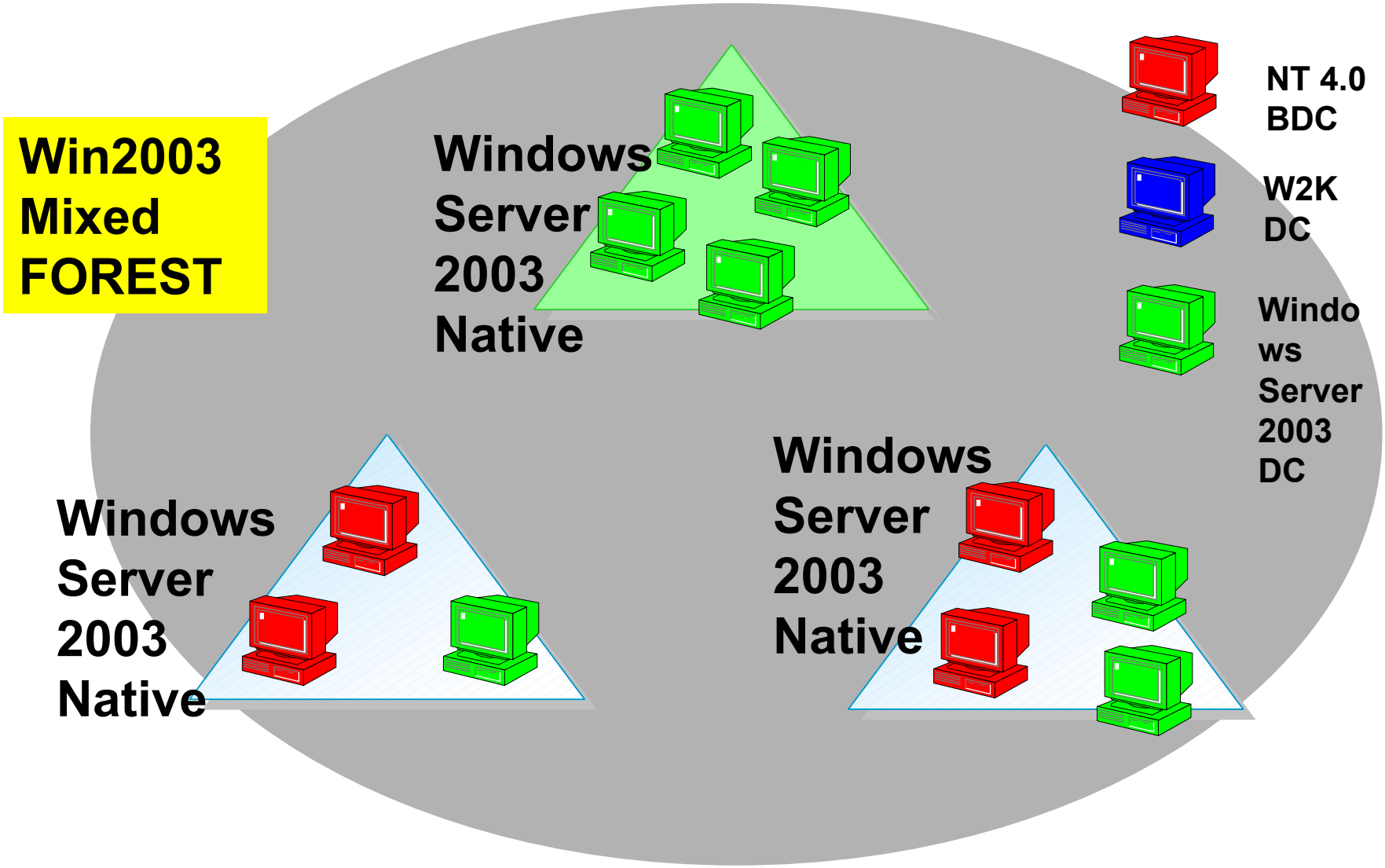
Windows 2003 Mixed Domain Functional Levels



Windows 2003
Forest Functional Level



Domain Functional Levels: Windows Server 2003 "Interim"



Improvements and Enhancements

GC Improvements!

- **No GC logon requirement … sort of…**
  - GC Contact Required in Windows 2000 Native Mode.
    - Dilemma: Put GC in remote sites?
    - Can turn it off (Registry hack)
  - 2003 Solution.
    - Enable GC Caching (by site)
    - First logon: User's group membership cached by LogonServer (DC) (from GC).
    - No GC required for subsequent logons.
    - Group Membership updated via AD Replication by the DC
    - Latency between Group Changes and application to users
      - Users only get Membership from Cache
      - Admin can manually refresh
    - Checks ensure the cache is up to date
    - Interim solution until you can justify GC at the site

GC Improvements!

- **No GC full synch**
  - W2K – Full sync when adding new GC published attributes in Schema
  - 2003 Only replicates added attributes.
  - Affects 2003 GCs only – or full sync.
  - Windows 2003 Native Forest functional level required.

ISTG Performance Enhanced

- **Inter-Site Topology Generator**
  - Responsible for intersite topology generation,
  - Win2K – Practical site limit: 100-300 sites.
  - 2003 Improvement
    - Generates different topology than Win2K ISTG.
    - Limit now about 3,000 sites!
  - Requires 2003 forest functionality

Linked Value Replication (LVR)

- WNT: Object Replication
  - **change to attribute or value**
- W2K: Attribute level replication
  - **Better than NT (more efficient)**
  - **Change to attribute replicates attribute**
  - **Change to value replicates attribute**
  - **Problem: Multi-Valued Attributes**
    - **Group = Attribute**
    - **Member = Value**
    - **Change Member = replicate attribute with all members**
    - **Impacts network traffic**
    - **Limit (per Microsoft) of 5,000 users/group**
- 2003: Linked Value Replication
  - **Replicates values – not attributes**
  - **Eliminates 5,000 user/group limit**

Misc. Replication

- **Permits Undelete of Objects (reanimating tombstones**
  - Permits an application to undelete the object
  - Some attributes missing
- **Improved compression algorithms**
  - Reduction in CPU required on BHS
- **Greater tolerance for demotion/promotion of a DC using the same name**
  - Prevents replication until KCC removes the first name
- **Replication Interval changes**
  - W2K = 5 minutes (Intrasite), 30 second delay
  - W2K3 = 15 seconds and 30 second delay

Change Offline, DS Repair Mode Password While Online!

- **NTDSUtil**
  - Set DSRM Password (main menu)
- **Increases server up-time limited by password change interval in Win2K.**
  - (Had to reboot to DS Repair mode to change.)
  - Q223301 (Win2K limit)
- **Cool error message!**

Setting password failed.

WIN32 Error Code: 0x6ba

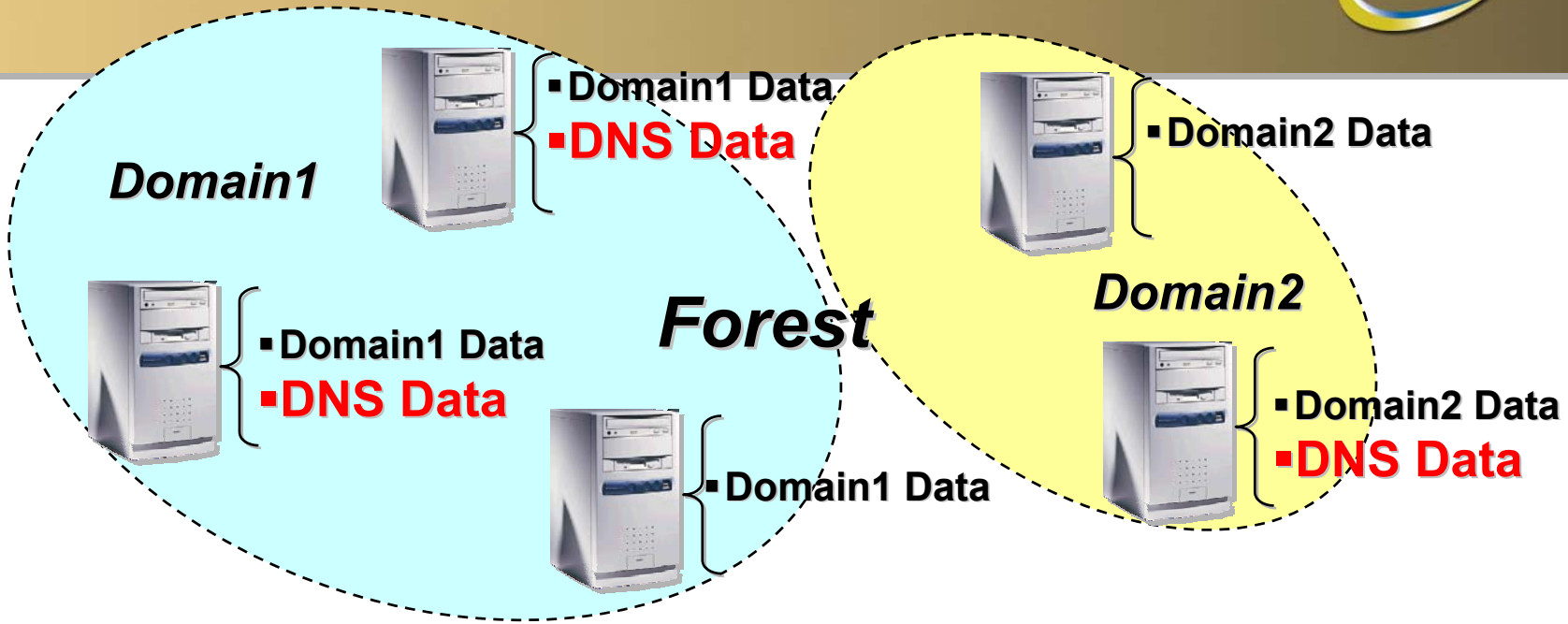
Error Message: The RPC server is unavailable.

See Microsoft Knowledge Base article Q271641 at http://support.microsoft.com for more information.

Directory Usage Scenarios

- **Win2k AD - Inappropriate to store volatile data.**
  - Only three choices of replication scope:
    - Not replicated
    - Domain-wide (domain NC)
    - Forest-wide (configuration NC)
  - Data may go to places where not used.

Application Partitions



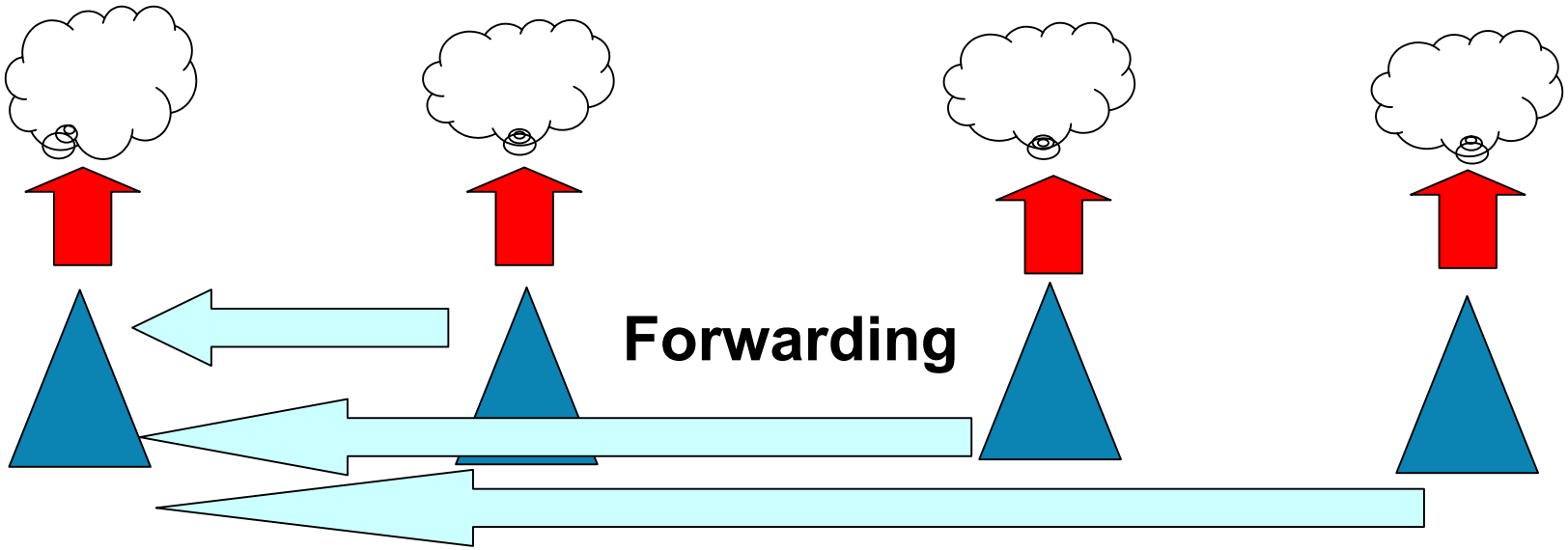
- **Scope: Selected DCs in Forest.**
  - Can cross domain boundaries.
  - As few/many replicas as you want (not replicated to GC).
  - Observes site topology, schedule.
  - Can contain any object type *except* security principals.
  - Named/located via DNS (*e.g.*, mstapi.sales.msn.com).
- **Will be created directly by applications.**
- **Replaced by Active Directory Application Mode (ADAM)?**

DNS Improvements

- **DNS server**
  - **Conditional forwarding and stub zones.**
    - Improved, efficient Name Resolution.
  - **Application Partition.**
    - Puts DNS records only on Name Servers/DCs.
  - **DNS event log now in DNS snap-in.**
  - **WMI provider – MicrosoftDNS.**

- **DNS client**
  - **Control client settings (suffix) via group policy.**
  - **Improved security for non-default naming scenario (“Allowed Suffixes”).**

DNS Case Study



corp2003

na.corp2003

sa.corp2003

eu.corp2003

na.corp2003

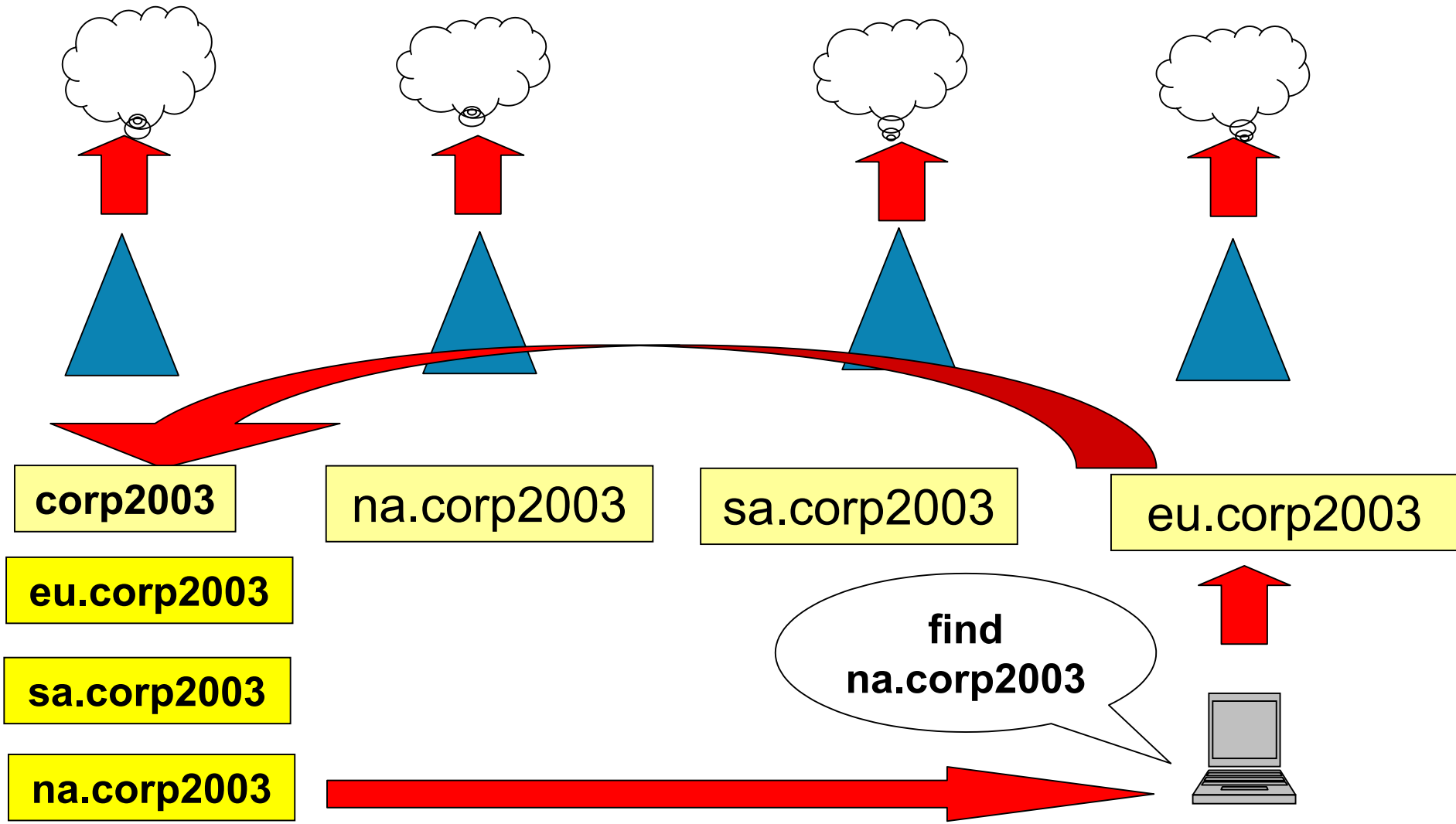
sa.corp2003

eu.corp2003

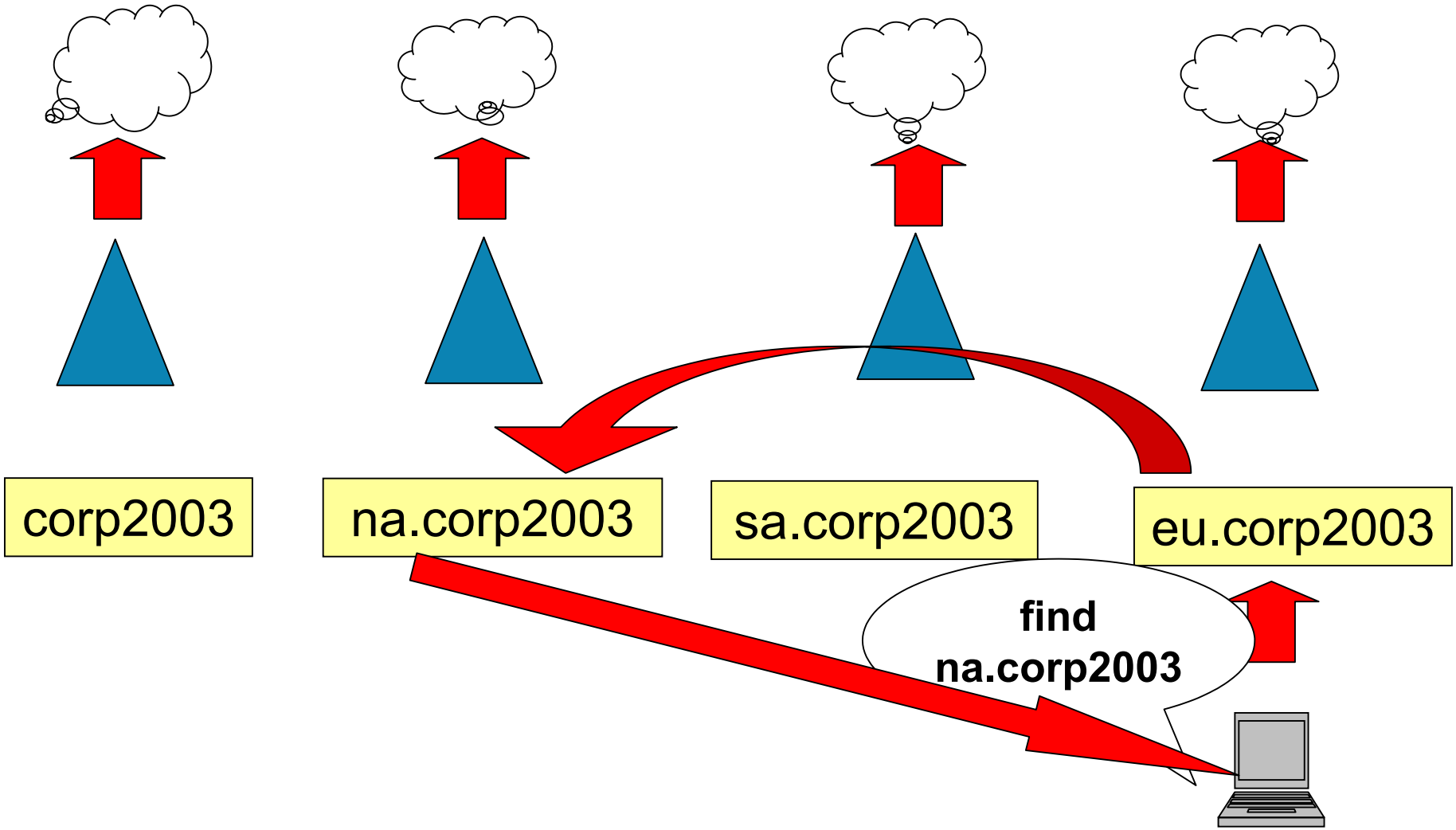
Secondary zones

Zone xfers

DNS Case Study



With Conditional Forwarding…



Errors – Kinder, Gentler ☺

"Lingering Object" Behavior

- **The problem**
  - Replication broken between domains for time >tombstonelifetime (TSL) or GC is offline >TSL.
  - GC comes back on line – replicates object back.
  - Can't create new object with that name (event 1084)
  - Security problem – Deleted acct. from former employee re-animated.
- **Loose behavior**
  - Allows old object to be propagated to DCs that have deleted it.
  - Attempt to create another object with same name results in error (name already exists).
- **Tight behavior**
  - Stops replication on the out-of-date DC until the object is deleted.

"Lingering Object" Behavior

- **Win2k**
  - Permits it by default.
  - Repair: Hot fix WINSE22234 permits deletion on GC.
- **2003 behavior**
  - New Install = Tight: Stops Replication until repaired (Default).
  - Upgrade = Loose (Default) .
- **Registry setting allows Admin to change it.**

  HKLM\System\CurrentControlSet\Services\NTDS\Parameters…
  - Add Value Name = Correct Missing Object
  - Data Type =REG_DWORD
  - Value = 1 (or zero)

Deployment and Manageability Improvements

WMI

- **Computer management**
- **Active Directory**
  - Provider: MicrosoftActiveDirectory
  - Classes:
    - Replication - See replprov.mof %windir%\system32
- **Trust health**
  - Provider: MicrosoftHealthMonitor
  - Classes: see system32\wbem\trusthm.mof
- **DNS**
  - Provider: MicrosoftDNS
  - Classes: system32\wbem\dnsprov.mof
- **Cluster**
  - MSCluster
- **Also look in CIM Studio in MSDN**
- **Book: Understanding WMI – Alain Lissoir (Digital Press)**

Group Policy

>160 New Settings

- **DNS Client Policies**
  - DisableDynamicUpdate
  - SearchList
  - UseDomainNameDevolution
  - DisableReverseAddress Registrations
  - DefaultRegistrationRefreshInterval
  - DisableReplaceAddressesIn Conflicts
  - DefaultTTL
  - UpdateSecurityLevel
  - NameServer
  - Domain
  - EnableAdpaterDomainName Registration
  - RegistrationTtl
  - UpdateSecurityLevel
  - /*AppendToMultiLabelName – this policy is not supported until Blackcomb*/
  - UpdateTopLevelDomainZones
- **Netlogon Parameters**
  - UseDynamicDns
  - DnsAvoidRegisterRecords
  - DnsRefreshInterval
  - LdapSrvWeight
  - LdapSrvPriority
  - DnsTtl
  - AutoSiteCoverage
  - SiteCoverage
  - GcSiteCoverage
  - NdncSiteCoverage
  - ExpectedDialupDelay
  - SiteName
  - NegativeCachePeriod
  - BackgroundRetryInitialPeriod
  - BackgroundRetryMaximumPeriod
  - BackgroundRetryQuitTime
  - BackgroundSuccessfulRefreshPeriod
  - NonBackgroundSuccessfulRefresh Period
  - ScavengeInterval
  - AvoidPdcOnWan
  - AllowSingleLabelDnsDomain

Group Policy

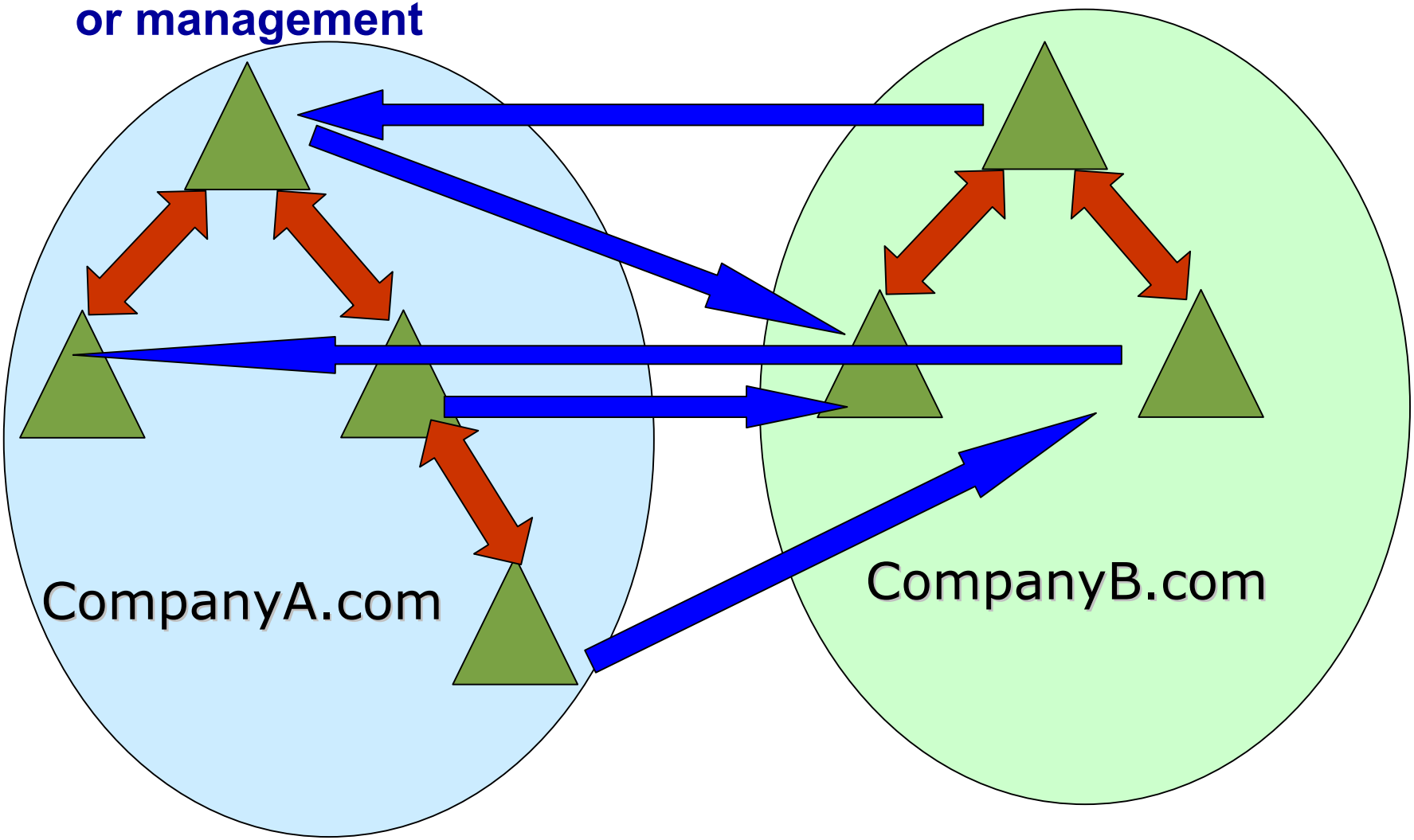
- Software Restriction Policies
  - **FIPS 140-1**
  - **Rules:**
    - **Path**
    - **Hash**
    - **Certificate**
    - **Internet Zone (useless)**
- Tools
  - **GPResult built in to 2003, XP**
  - **Resultant Set of Policies (RSOP)**
    - **Logging – Current settings applied**
    - **Planning – "What if" new policies are applied**
  - **Group Policy Management Console (GPMC)**
    - **Snaping to view, manage all Policies in domain from one spot**

Cross Forest Trust

- **The problem**
  - Forest Level Kerberos Trust Not Available in W2K
    - Only NTLM Authentication via one-way trusts to domains
    - Required NT4 style trust model between domains in forests
- **2003 solution**
  - Kerberos Trust
    - MS Kerberos is now MIT v5 Compliant!
  - Transitive (trust at forest root only)
  - Configurable – not an open door.

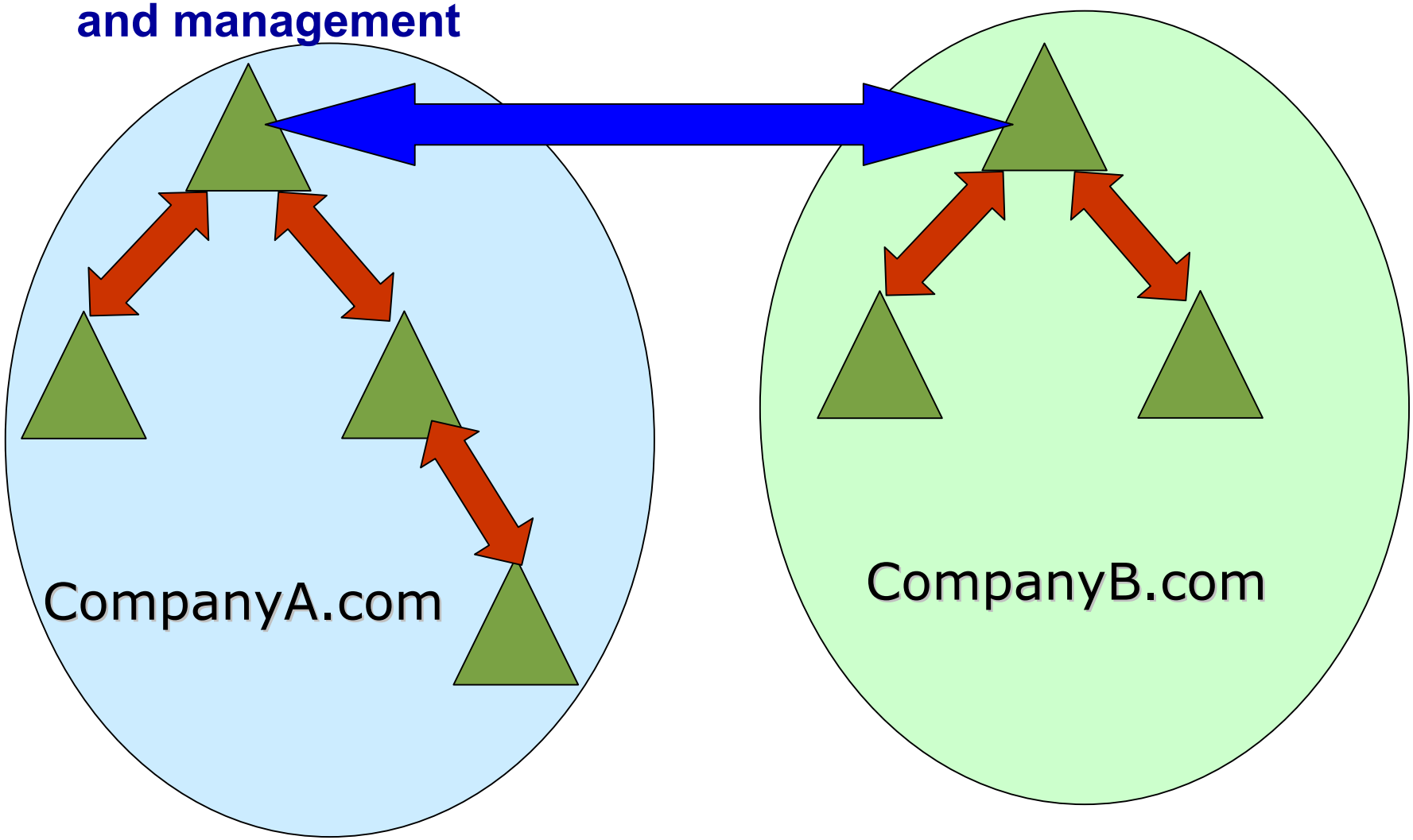
Windows 2000 Inter-Forest Trust

- No Inter-Forest Transitivity or management
- NTLM Based



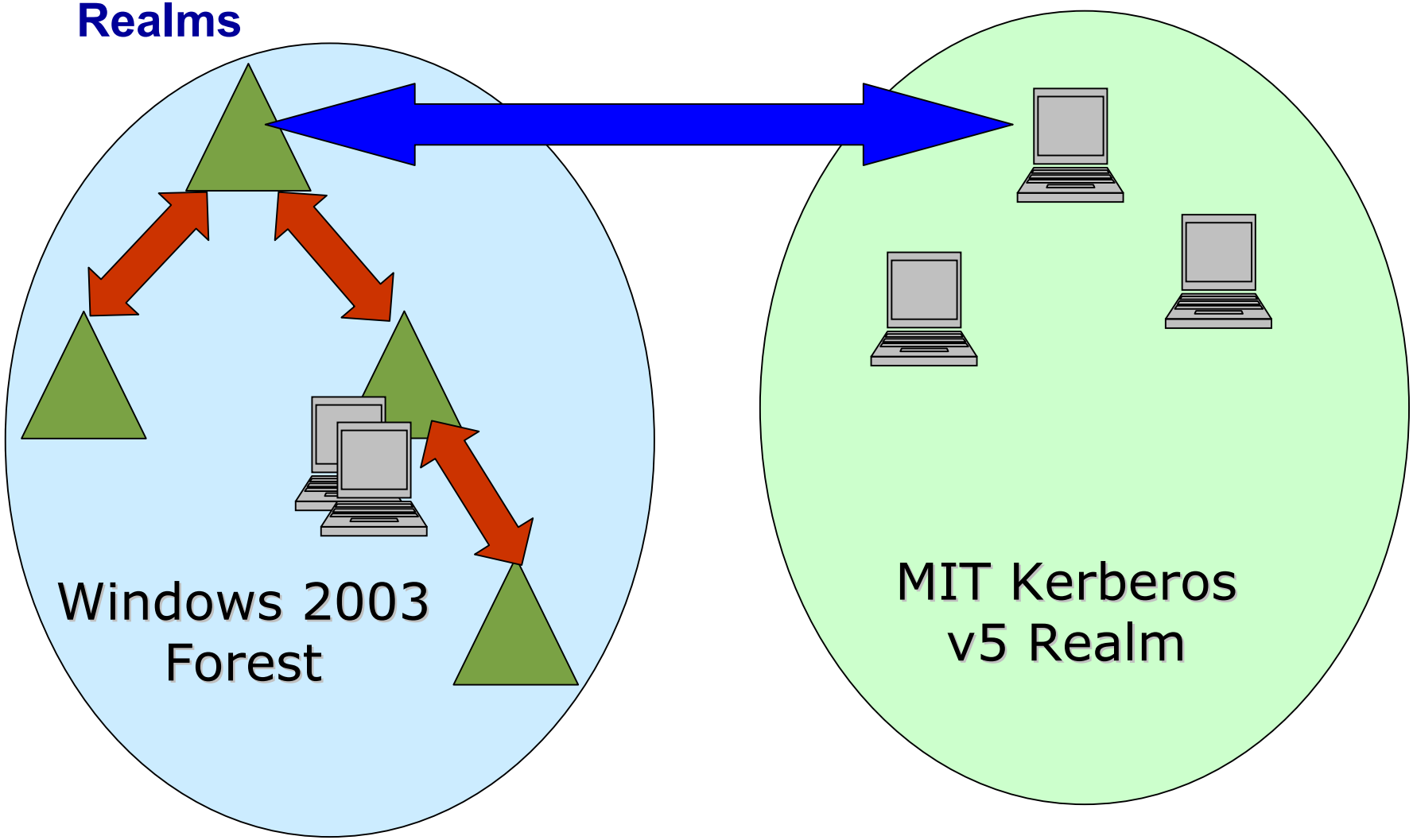
Windows 2003 Inter-Forest Trust

- Full Inter-Forest Transitivity and management
- Kerberos Based



Windows 2003 – Kerberos Realm Trust

- Interoperability between Windows 2003 Forest and Kerberos Realms

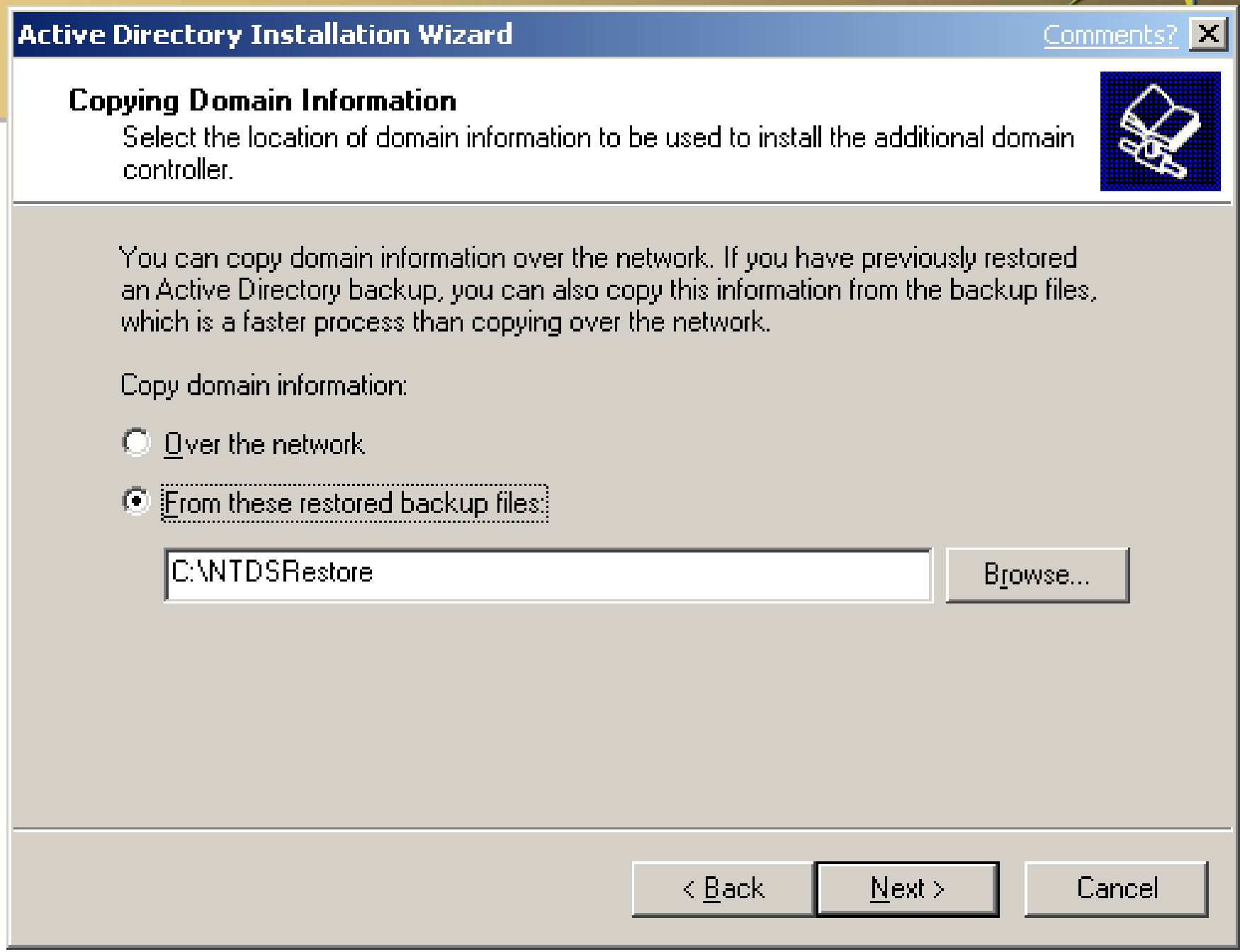


Install From Media (IFM)

- Source Replica AD from Media in DCPromo
  - GCs or DCs (Replica only).
  - No initial replication from a DC.
    - Faster (no searching for a DC).
    - Less network impact (No full sync on the WAN).
    - Easy branch office installation.
  - After initial load, replicates changes.
  - Network connectivity still required.
  - Unattended Answer File Support:
    - ReplicateFromMedia
    - ReplicationSourcePath

Install From Media (IFM)

- **Media must be local drive.**
- **Media useful life < 60 days.**
- **How?Use Backup Files/Media**
  - Create first DC in domain.
  - Back up DC.
  - Restore to Media (local disk, CD, …).
  - C:>dcpromo /adv.
  - Wizard produces an additional screen…


Active Directory Installation Wizard
Comments?
Copying Domain Information
Select the location of domain information to be used to install the additional domain controller.
You can copy domain information over the network. If you have previously restored an Active Directory backup, you can also copy this information from the backup files, which is a faster process than copying over the network.
Copy domain information:
Over the network
From these restored backup files:
C:\NTDSRestore
Browse...
< Back
Next >
Cancel

DCPromo Answer File


```
[DCINSTALL]
UserName
Password
UserDomain
DatabasePath=c:\windows\ntds
LogPath=c:\windows\ntds
SYSVOLPath=c:\windows\sysvol
SafeModeAdminPassword
CriticalReplicationOnly
SiteName=
ReplicaOrNewDomain=Replica
ReplicaDomainDNSName=globalpro.com
ReplicationSourceDC=ReplicateFromMedia
ReplicationSourcePath=e:\DSrestore
RebootOnSuccess=yes
```

Remote Desktop Features

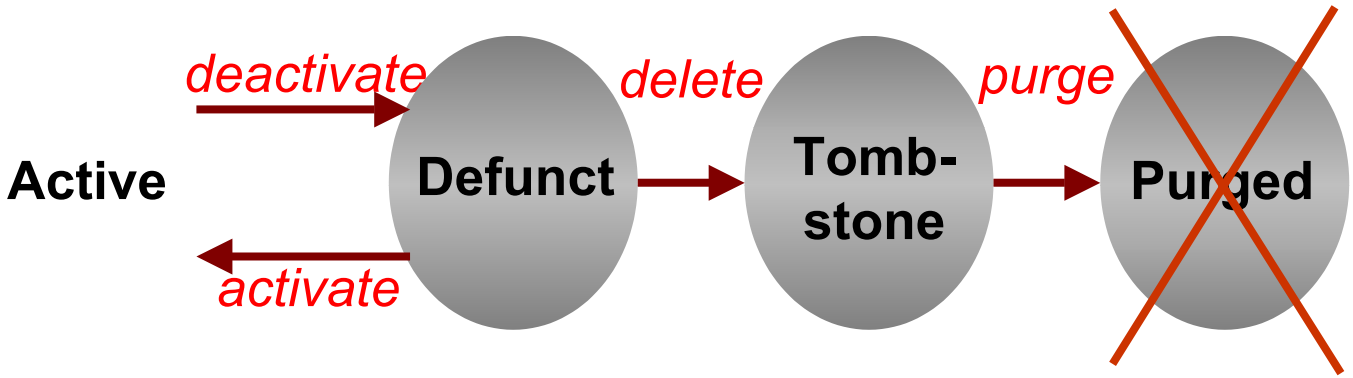
- Replaces Terminal Services Admin Mode
- File System – the client file system is accessible through the Remote Desktop
- Audio – Audio streams such as .wav and .mp3 files can be played through the client sound system.
- Port – Applications have access to the serial and parallel ports on the client
- Printer – The default local or network printer on the client becomes the default-printing device for the Remote Desktop.
- Clipboard – The Remote Desktop and client computer share a clipboard that allows data to be interchanged..

Removing Fear of Irreversible Decisions

Schema Delete

- **Core of the problem:**
  - Immutable association between the *identity* of a class/attribute in the schema and certain properties.
  - Identities cannot be reused (W2K).
  - Old classes/Attributes cannot be Purged

Schema Delete



Deactivate	**Set isDefunct= TRUE with *ldap_modify()***
Activate	**Set isDefunct=FALSE (or remove the attribute) with *ldap_modify()***
	Not Implemented in 2003:
Delete	**Delete with *ldap_delete()***
Purge	**Garbage collect tombstones**

Domain Rename

- **White paper and tools:**
  - **www.microsoft.com/WINDOWS2000/downloads /tools/domainrename/default.asp**
- **Not for the faint of heart…**
- **Why would you want to?**
  - DNS Namespace changes.
  - Changes in environment since deployment.
- **Other options**
  - Migrate using third-party tool or ADMT.
  - Tear down and start over.

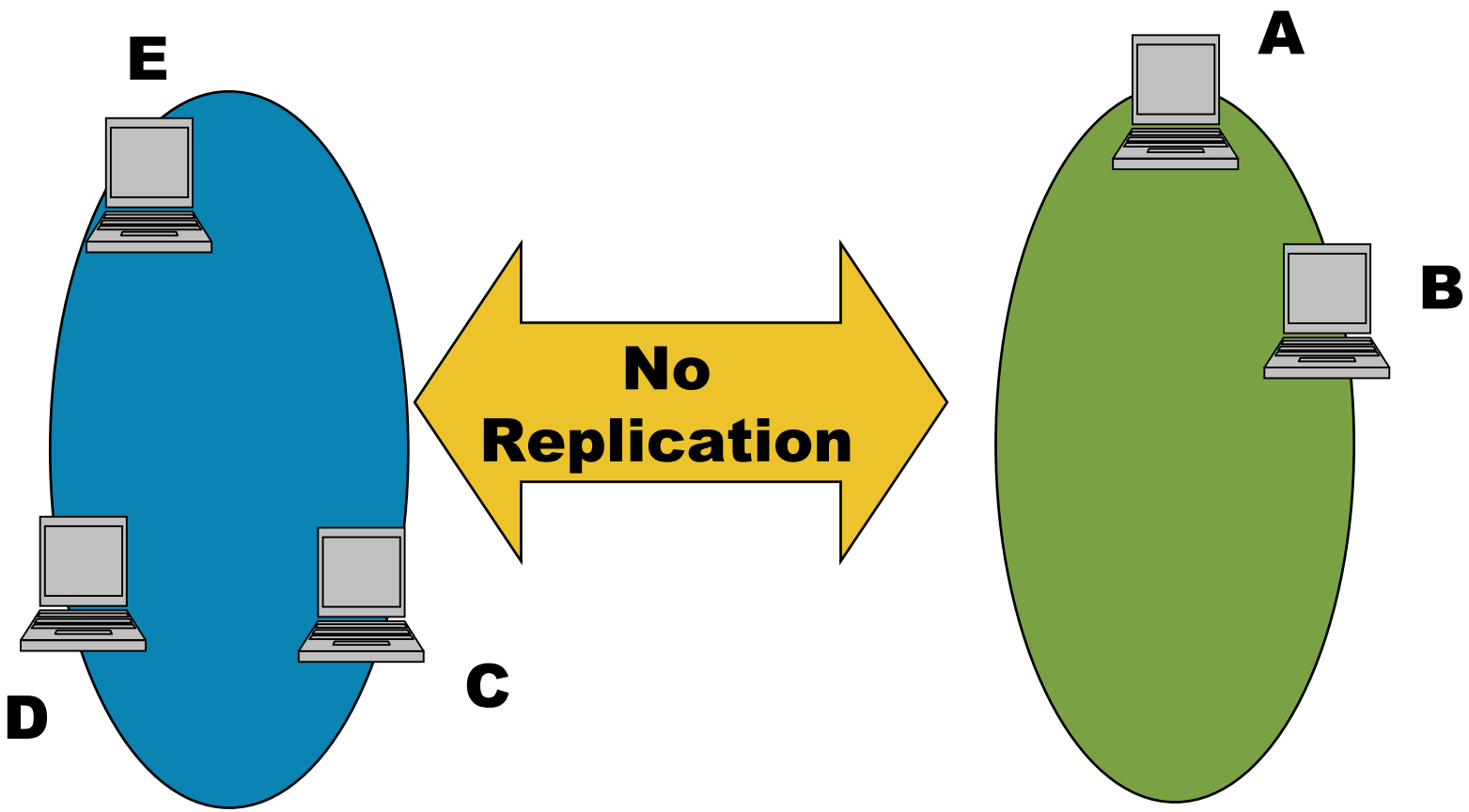
Domain Rename

- **What you can do (The Good):**
  - Rename a DC.
  - Rename a domain: DNS or NETBios or both!
  - Rename and restructure domains in a forest.
- **Restrictions (The Bad):**
  - **Can't do it if Exchange is deployed in forest**
  - **No earlier than Exchange 2003 SP1**
    - Workaround: Put Exchange in a "resource forest."
  - Forest Native mode: Only 2003 DCs in all domains in Forest
  - Can rename root domain but can't change domain that is forest root.
  - **No "Grafting" or merging of Forests!**

Domain Rename

- **Gotchas**
  - Must be in pure 2003 Forest /Domain functionality mode
  - MUST LOCK DOWN THE ENTIRE FOREST DURING DOMAIN RENAME PROCESS
  - DCs in renamed domain won't replicate with DCs in original domain.
    - Replication limbo - Two replication topologies
    - What happens to password, other changes?
    - DFS/FRS
  - Applications that depend on the name (registry)
  - Secure Channels: Clients, trusts, etc.

Domain Rename "Limbo State"



New Tools

Admin Tool Improvements

- **Users and Computers snap-in**
  - Drag and drop.
  - Multi-select and edit user objects.
  - Heavily revised object picker.
  - Saved queries.
  - Viewing Saved DS, DNS, FRS eventlogs on non-DCs!
- **Improved Gpresult.exe (more verbose!)**
- **Command-line tools**
- **2003 Adminpak (only on XP)**

Command Line Tools

- **GPresult**
  - Enhanced reporting
- **DCDiag**
  - DCPromo Test
- **Repadmin – enhanced reporting**
- **Netdom – *computername* for DCrename**
- **Others**
- **Shipped on**
  - Service Pack 2 CD (install manually)
  - 2003 Server, AdvSvr CD

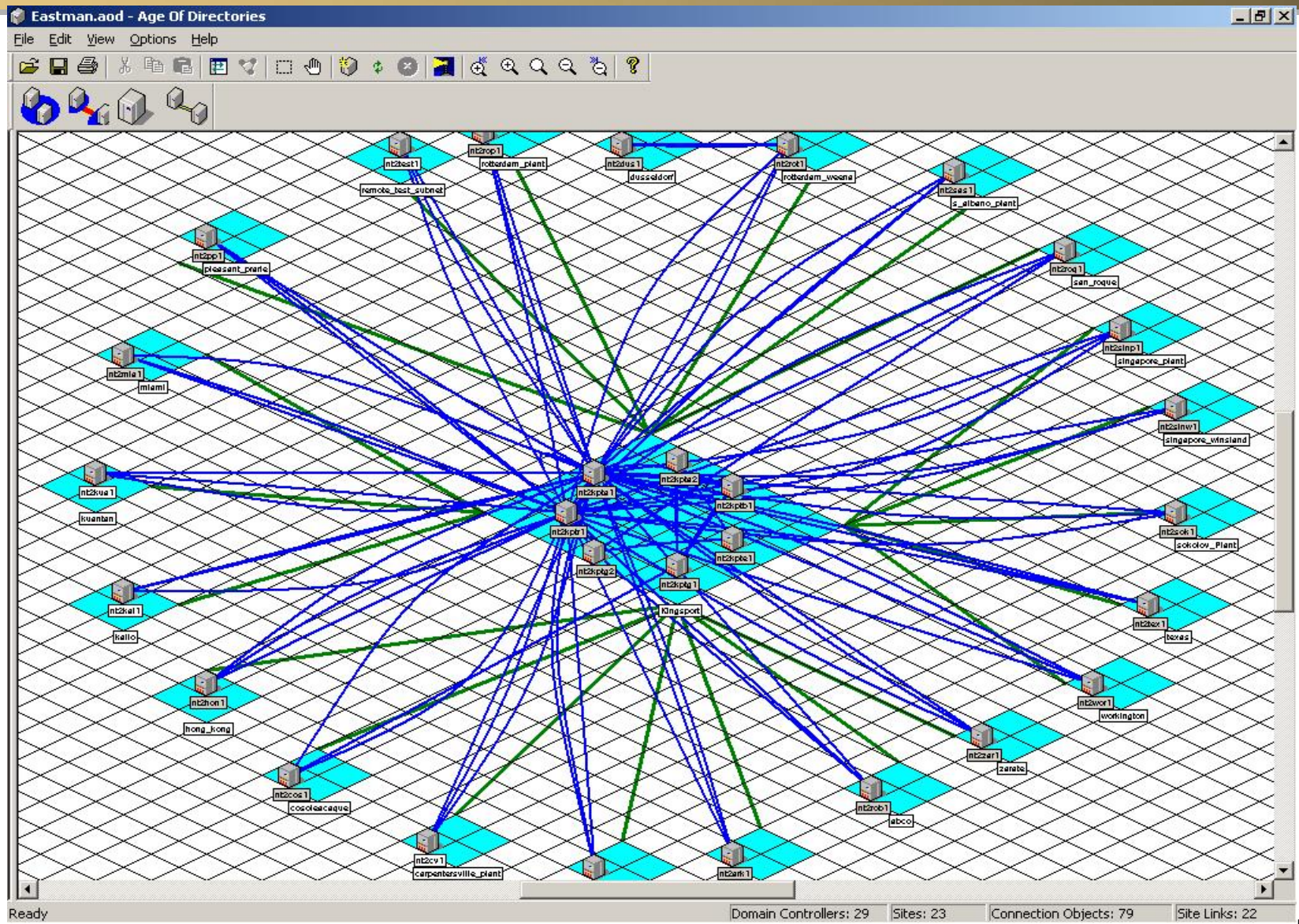
Active Directory Load Balancing Tool

- **Does the job of branch office deployment.**
  - KCC chooses BHS for connection objects – choose the same one.
  - Tool allows you to spread the load to other DCs in the site (that have that NC).
  - ADLB tool modifies the Hub DC's replication schedules to spread it out over time.
  - Generates a log – like replmon's status log.
  - For Deployments with hundreds of branch offices all replicating to a single hub..
  - Tool=no benefit to sites with only one DC per domain.

OpenView for Windows

- Windows 2000 and 2003
- Active Directory Monitoring
- Active Directory Topology Viewer

Tools: HP OpenView for Windows Demo

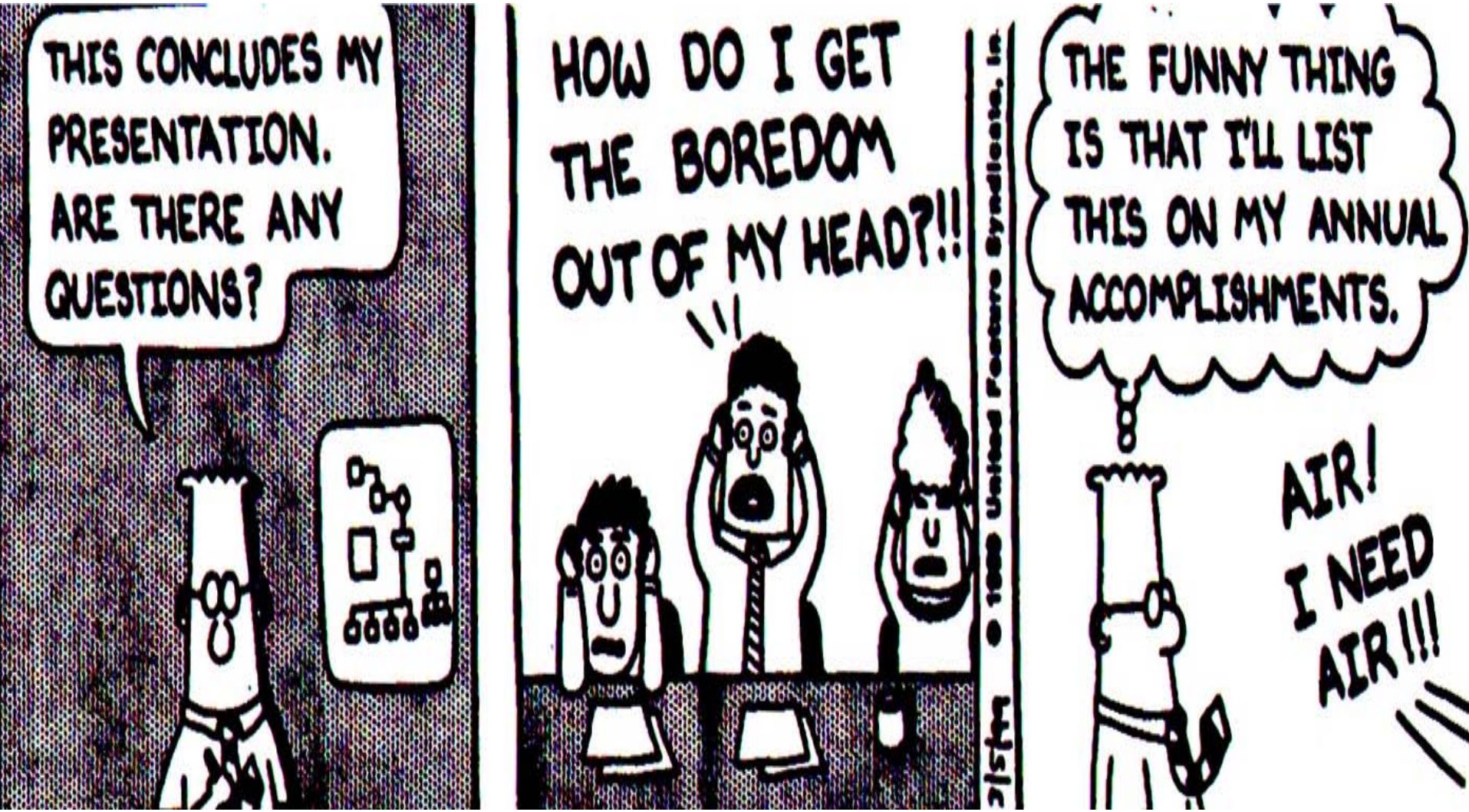


HP Internal: Qtest and Qnet

- **Qtest**
  - Win2k
  - Testing and Learning – everyone is an admin
  - Since Beta 2
  - Will be adding 2003 DCs
  - Contact: Ken Punshon (EMEA)
    - **Gary Olsen, Dung Hoang Khac**
    - **http://ps.inet.cpqcorp2003/ent/Qtest.htm**
- **QNet**
  - Native 2003 forest
  - Contact: Daragh Morrissey, Kim Mikkelsen

- **KBs on joining Qtest and Qnet**

QUESTIONS?


THIS CONCLUDES MY PRESENTATION. ARE THERE ANY QUESTIONS?
HOW DO I GET THE BOREDOM OUT OF MY HEAD?!!
THE FUNNY THING IS THAT I'LL LIST THIS ON MY ANNUAL ACCOMPLISHMENTS.
AIR! I NEED AIR!!!

Interex, Encompass and HP bring you a powerful new HP World.