What's New and Cool in Windows Server 2003 Active Directory

Gary Olsen
Consultant
WTEC
Global Solutions Engineering
Hewlett-Packard
gary.olsen@hp.com

Books

Windows Server 2003 on ProLiant Servers

http://www.phptr.com/title/0131467581

Authors: Gary Olsen, Bruce Howard
Publisher: Prentice Hall

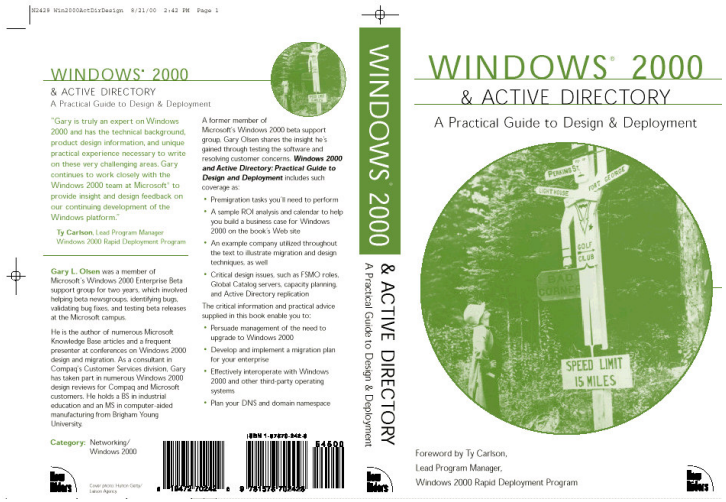
ISBN: 0131467581

Publishing Date: October, 2004

Windows 2000: Active Directory Design & Deployment

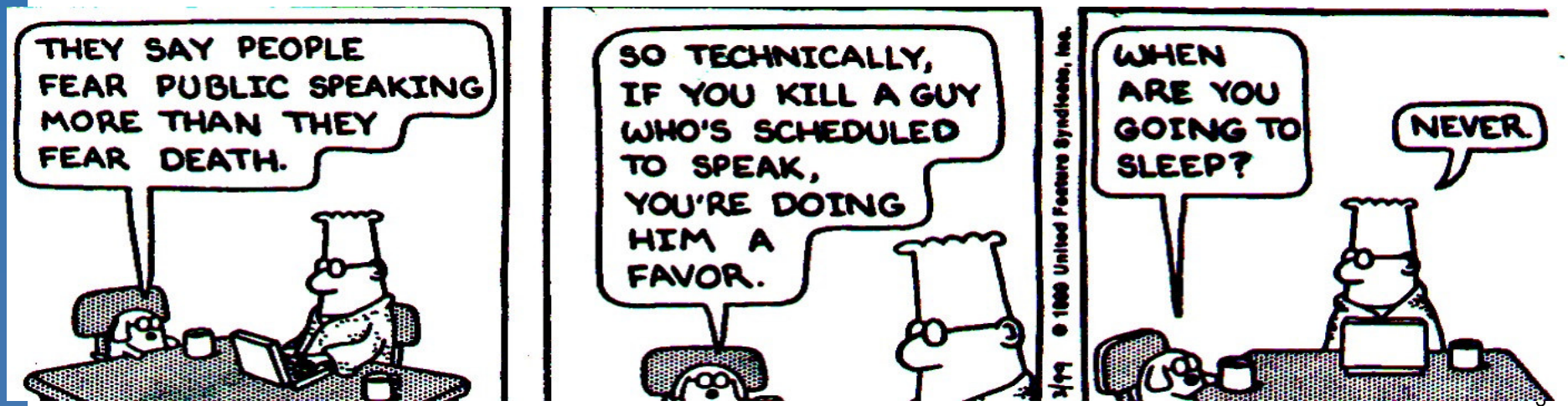
Author: Gary Olsen

Publisher: New Riders
ISBN: 1578702429



Agenda

- Migration Paths
- Improvements and Enhancements
- Deployment and Manageability Improvements
- Removing Fear of Irreversible Decisions
- New Tools

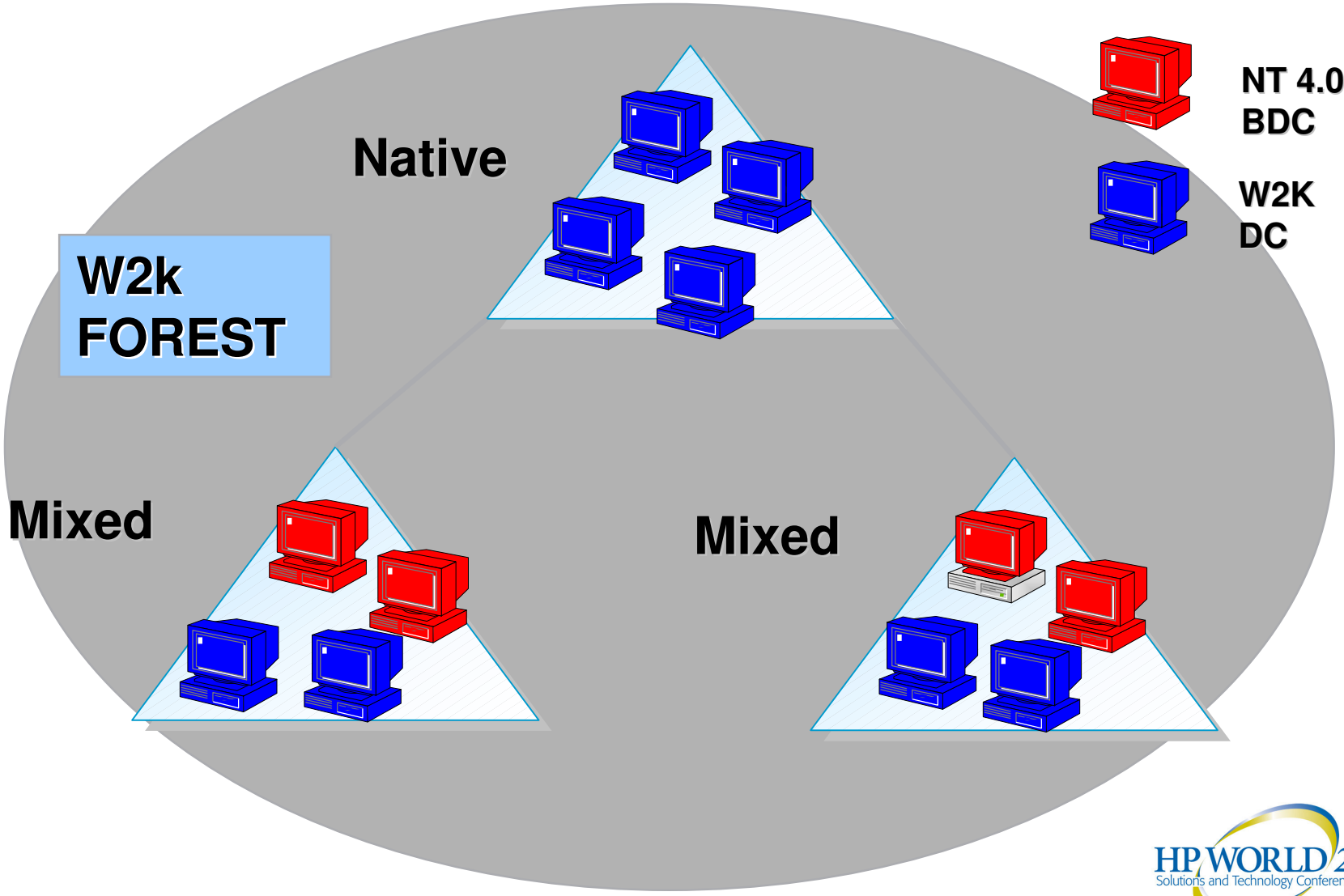


Migration Paths

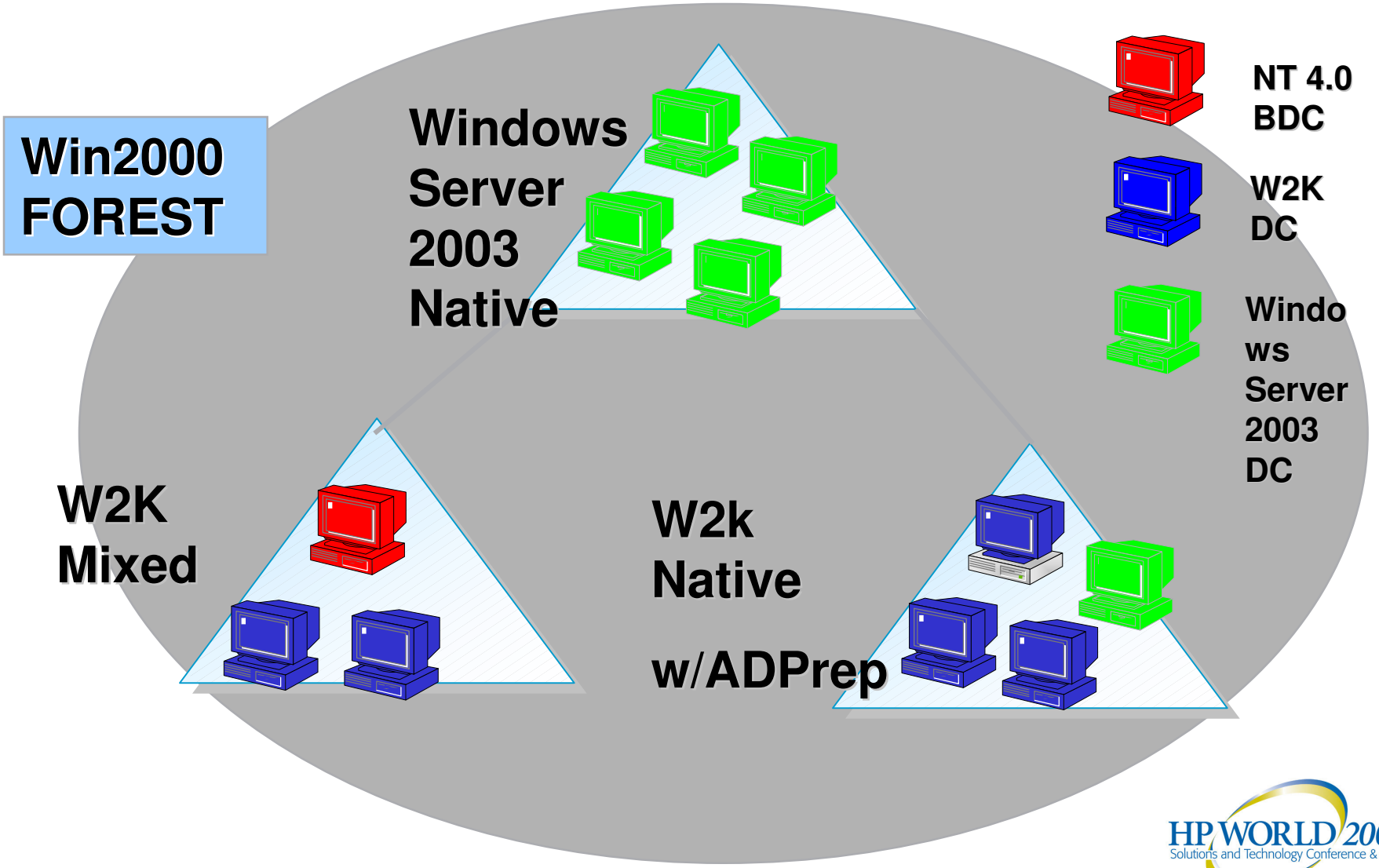
Functional Modes

- 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

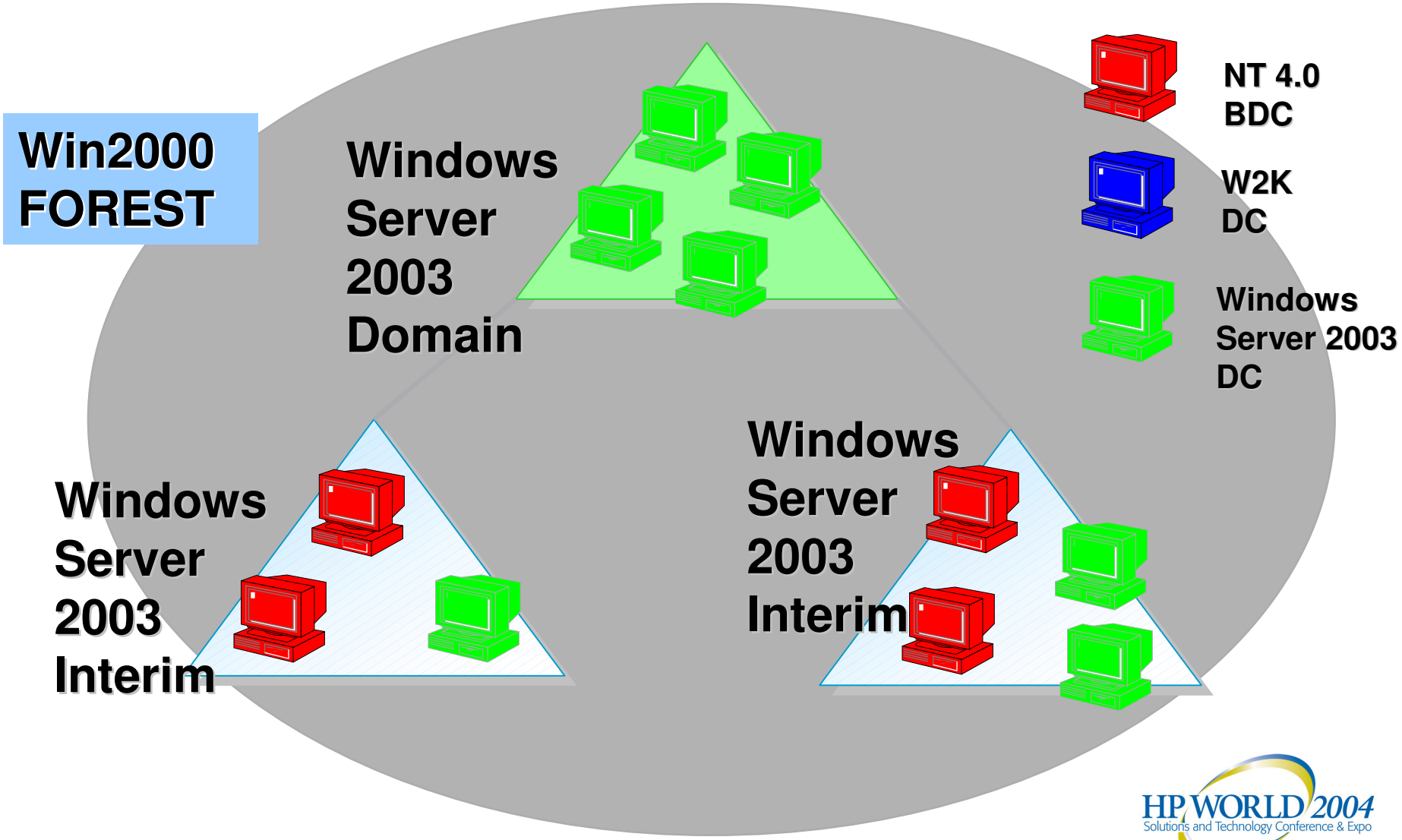
Review:
Win2k Native/Mixed Domains



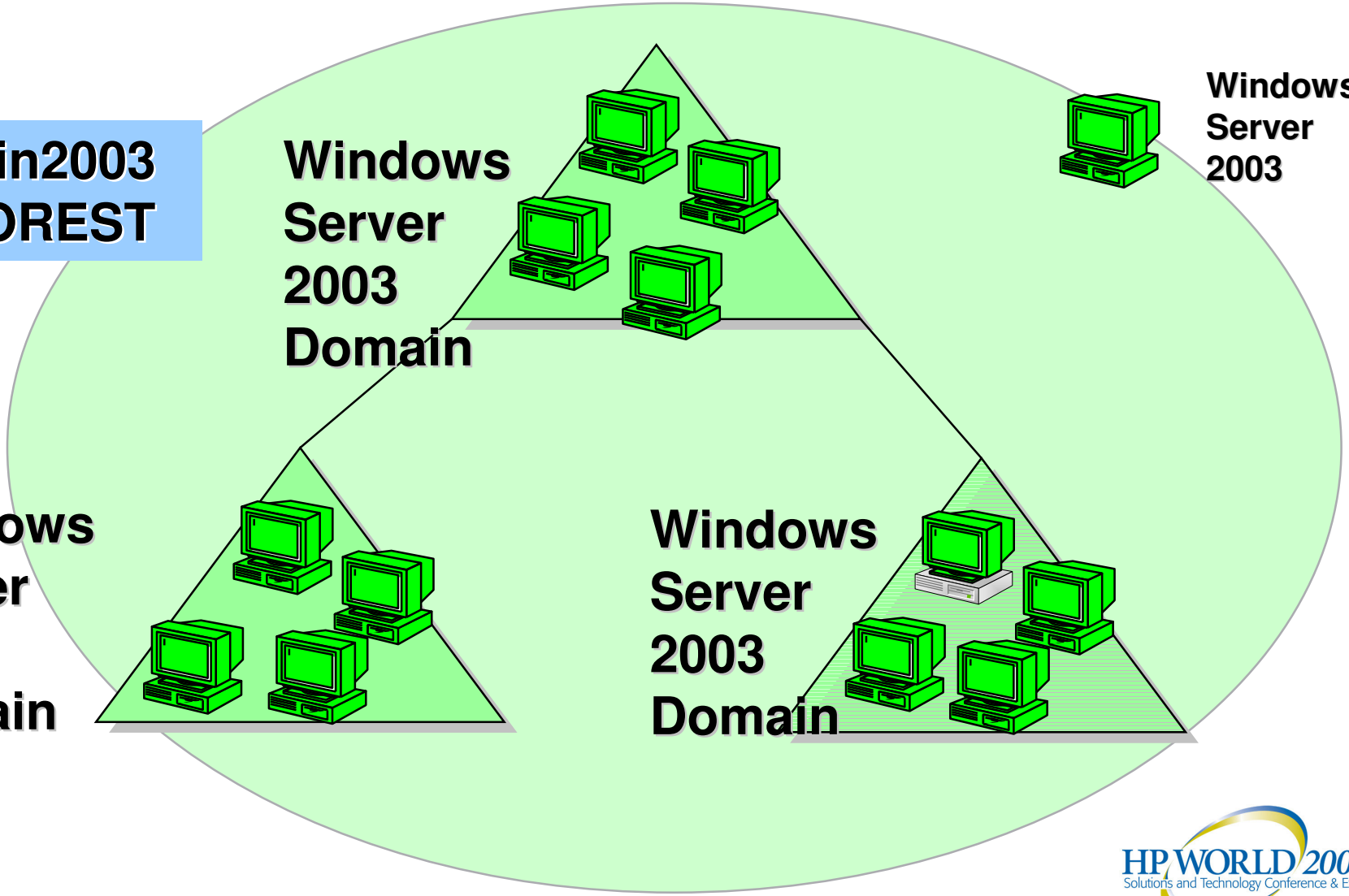
Domain Functional Levels: Windows 2003 Domain in W2K Forest



Domain Functional Levels: Windows Server 2003 "Interim"



Windows 2003 Forest: Full Windows Server 2003 Functionality



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
    - Checks ensure the cache is up to date
    - Interim solution until you can justify GC at the site

No GC Full Synch

- Partial Attribute Set (PAS)
  - Read only context
  - Objects and attributes for other domains in forest
- Windows 2000: Full sync when modifying PAS
  - All GCs do a full sync
  - Inefficient – decrease in performance
  - Increase in WAN Traffic
- Windows Server 2003: Only replicates added attributes.
  - Affects 2003 GCs only – or full sync.

GC Removal Improvements!

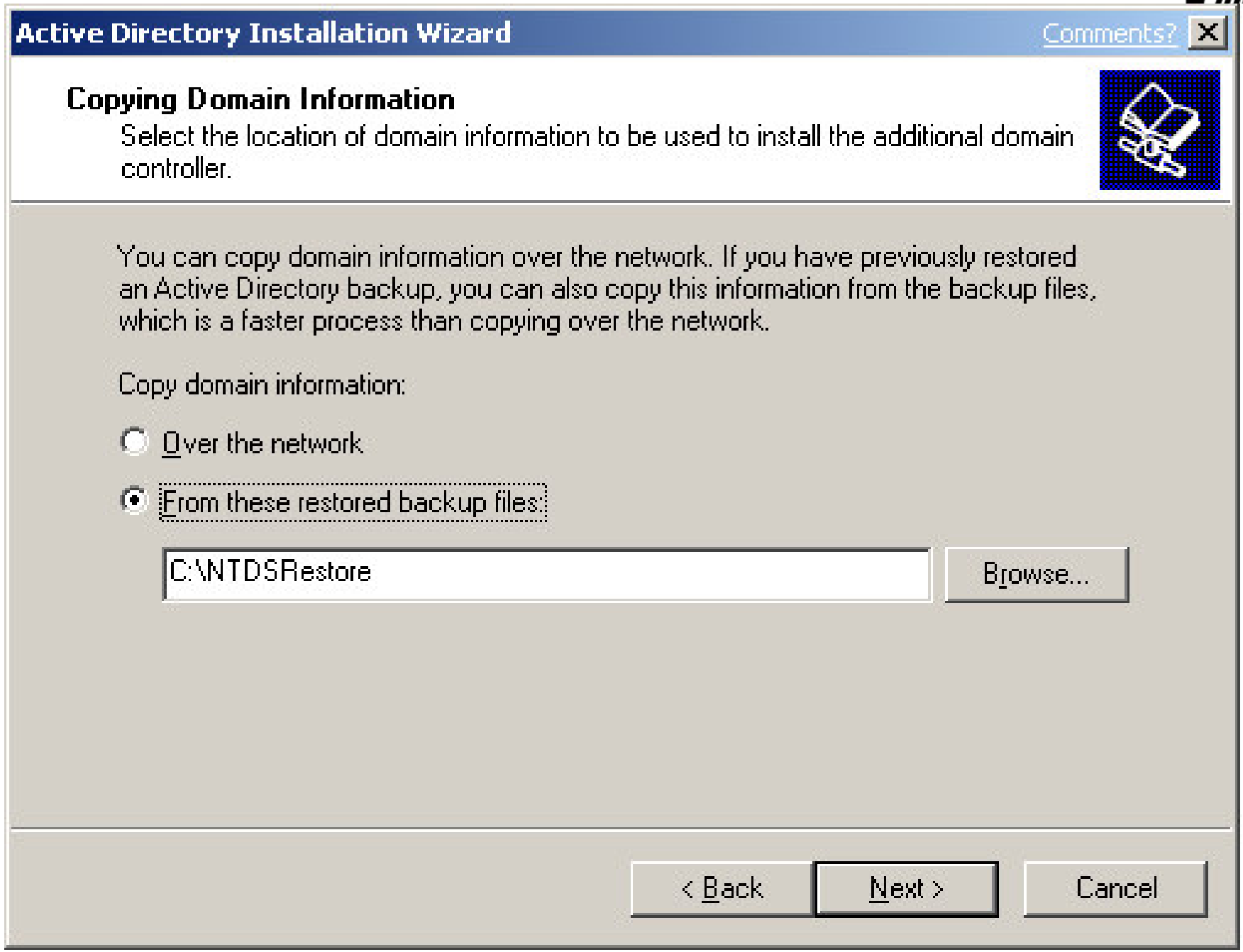
- Windows 2000: Limit of about 500 objects/iteration
  - AD: 4,000 Users 6,000 computers and 500 groups
  - = 10,500 objects / 500 = 21 iterations
  - 21 iterations * 15 minutes = 5 hrs 15 min. to complete
  - + Replication Latency
  - HP: 3-5 days depending on the site.
- Windows Server 2003: No “limit”
  - Continues removal as a low priority task
  - Takes advantage of low bandwidth utilization periods
  - Replaces seti@home for those idle cycles ☺
  - Use with Install From Media for best results

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=Administrator
Password=MyPassword123
UserDomain=Corp.com
DatabasePath=c:\windows\ntds
LogPath= c:\windows\ntds
SYSVOLPath=c:\windows\sysvol
SafeModeAdminPassword
CriticalReplicationOnly
SiteName=
ReplicaOrNewDomain=Replica
ReplicaDomainDNSName=Corp.com
ReplicationSourceDC=
ReplicateFromMedia=Yes
ReplicationSourcePath=e:\DSrestore
RebootOnSuccess=yes
```

Intersite Topology Generator

- Process of the Knowledge Consistency Checker (KCC)
- Responsible for intersite topology generation
  - Picks Bridgehead Servers
    - Windows 2000: 1 per site, per NC, per IP/SMTP
  - Generate Intersite connection objects
    - Spanning Tree
- Windows 2000 Problems
  - Practical Limit of ~200 sites
  - Practical Limit of ~30 connections to single BHS

Windows Server 2003 Improvements

- Win2K practical limit of ~250 sites
  - (1 + num domains) * num sites ^ 2 * 0.0000075 min
  - 4 domains @ 1,000 sites = KCC takes 45 minutes of 90% cpu
  - KB 244368
- New Spanning Tree Algorithm used in Windows Server 2003 (Kruskal's & Dijkstra's algorithms)
  - (1+ #domains) * #Sites *.0005
  - for 5,000 sites and 1 domain this takes 30 seconds to calculate on a PIII 600 MHZ Single processor machine with Site link Bridging on.
- Windows Server 2003 Forest Mode ONLY!

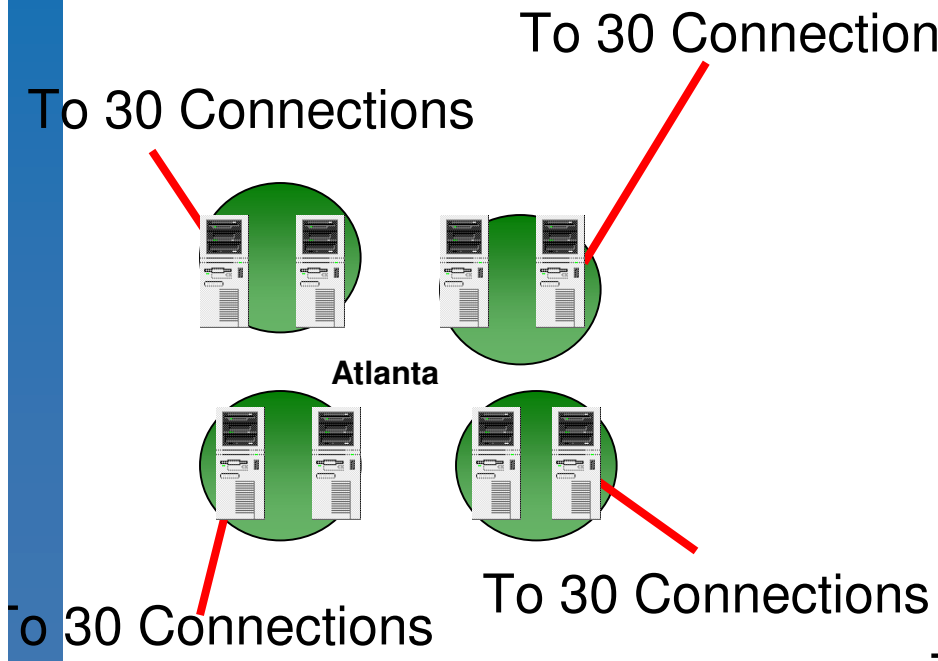
Example – Windows 2000

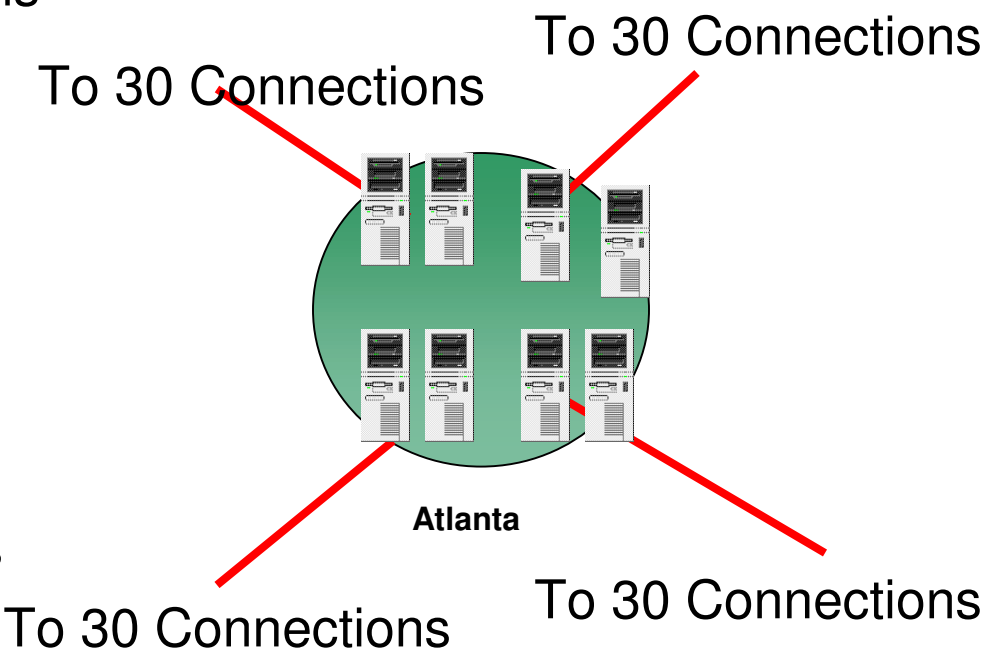
How to support 120 sites to single Hub?

- 10 simultaneous outbound threads
- 1 inbound (serialized) thread
- Too many connections to single BHS:
  - Latency
  - RPC Timeouts
- Baseline of 30 connections per BHS
  - Stagger 10 connections every :30 for 90 min frequency
  - 4 BHS to serve 120 inbound connections

BHS Load Balancing in Windows 2000

- Create multiple hub sites (keep KCC on)
- Create manual connections to >1 DC in Hub site
  - Turn off or Schedule KCC/ISTG





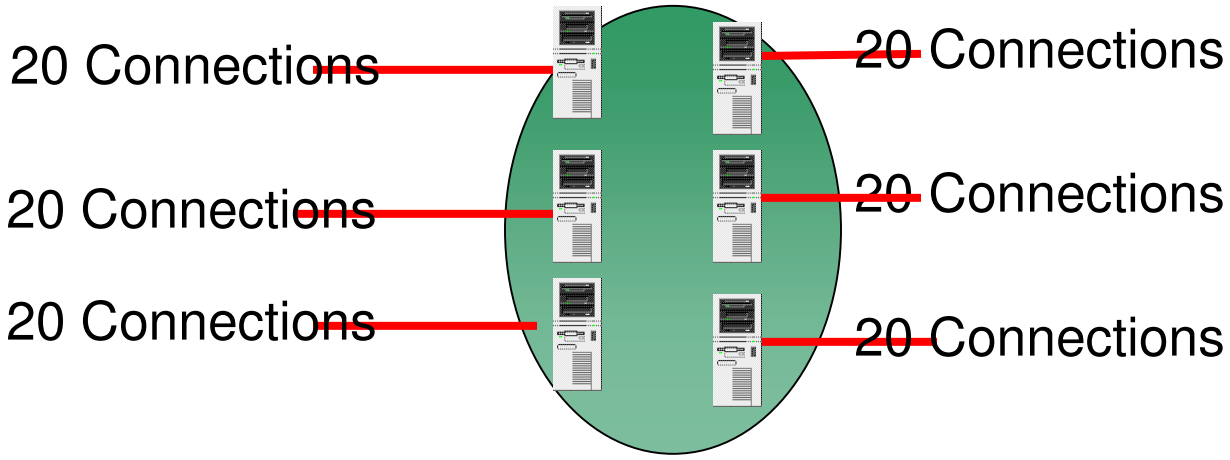
Win2003 BHS Load Balancing

- Every DC is a BHS by default
  - Selected randomly with each new connection
- Outbound Repl Scheduling not staggered
- Start time is randomized in Win2003
  - Replicate 3:00-4:00, selects 3:15, 3:30, 3:45, 4:00 to start
  - Disable by using ADSIedit: Set Options Attribute to 512 on:

    CN=NTDS SiteSettings,CN=<Target-Site-Name>,CN=Sites,
    CN=Configuration,<forest Root domain>

Active Directory Load Balancing Tool

- Windows 2000
  - Dynamically Load balances KCC connection objects between DCs in single site
  - Only runs on XP or W2k3 Server
  - Design Connections per Site, not per Server
  - KCC is running



Linked Value Replication (LVR)

- WNT: Object Replication
- W2K: Attribute level replication
  - Change to attribute replicates attribute
  - Change to value replicates attribute
  - Problem: Multi-Valued Attributes
    - Group = Attribute Member = Value
    - Change Member = replicate all members
    - Limit (per Microsoft) of 5,000 users/group
- 2003: Linked Value Replication
  - Replicates values – not attributes
  - Eliminates 5,000 user/group limit

Linked Value Replication (LVR)

- 2003: Linked Value Replication
  - Replicates values – not attributes
    - Eliminates 5,000 user/group limit
  - Requires Windows Server 2003 Forest level
- Improves Disaster Recovery
  - Authoritative Restore (Windows 2000)
    - User must be replicated before groups
    - Run Authoritative Restore twice
  - Windows Server 2003 Authoritative Restore
    - Run Authoritative Restore once
    - User = value, not a blob as in Windows 2000
    - Only for Windows Server 2003 Forest mode
    - Only for Users created after switch to Forest mode

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
    - 60% of CPU time for replication used for decompression (Windows 2000)
    - Windows 2003: reduced to 20%
  - Can turn off intersite compression
- Replication Interval changes
  - W2K = 5 minutes (Intrasite), 30 second delay
  - W2K3 = 15 seconds and 30 second delay

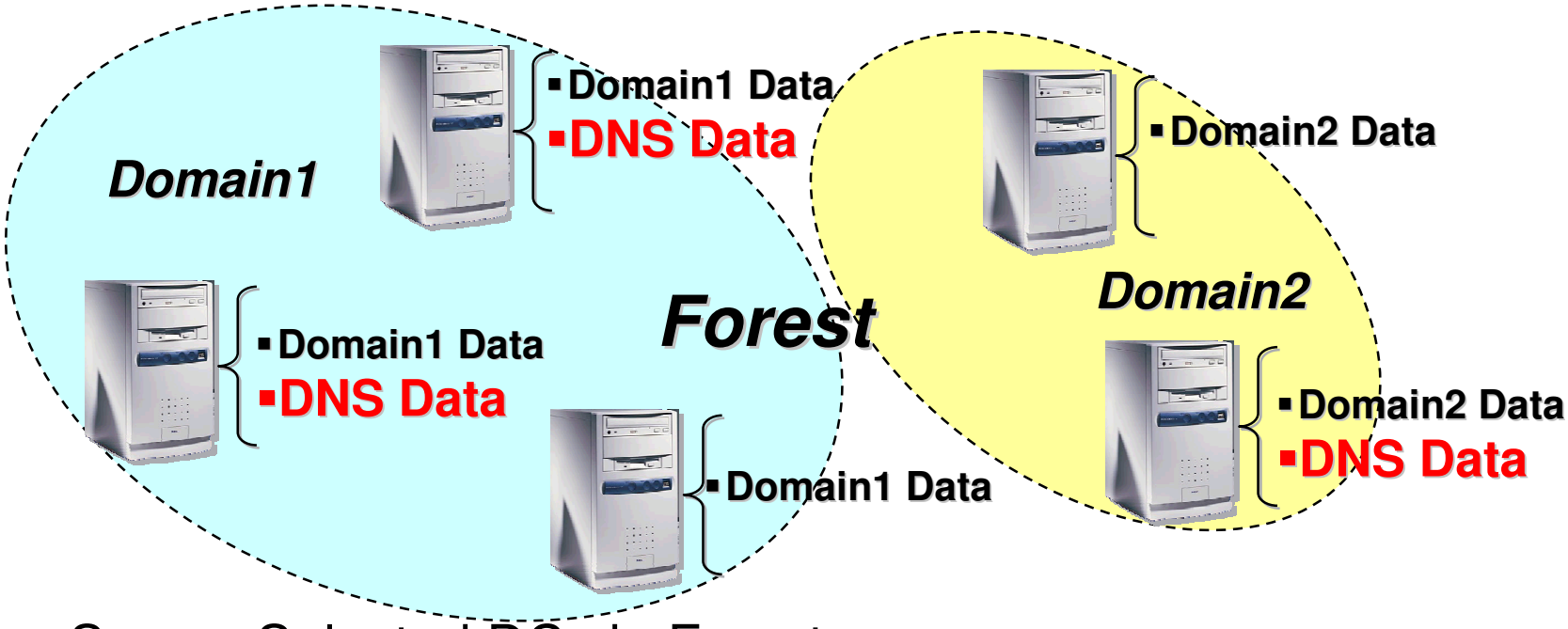
Greater Tolerance for DC Removal

- Demote/Repromote Using the Same Name
  - Two objects with same name, different GUID
  - Graceful
  - Manual
  - Too impatient to wait for Replication Latency
  - Will eventually resolve (64hrs in one case)
- Windows Server 2003: Prevents replication until KCC removes the first name
  - Repromote with same name
  - New name not propogated until old one is removed.

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



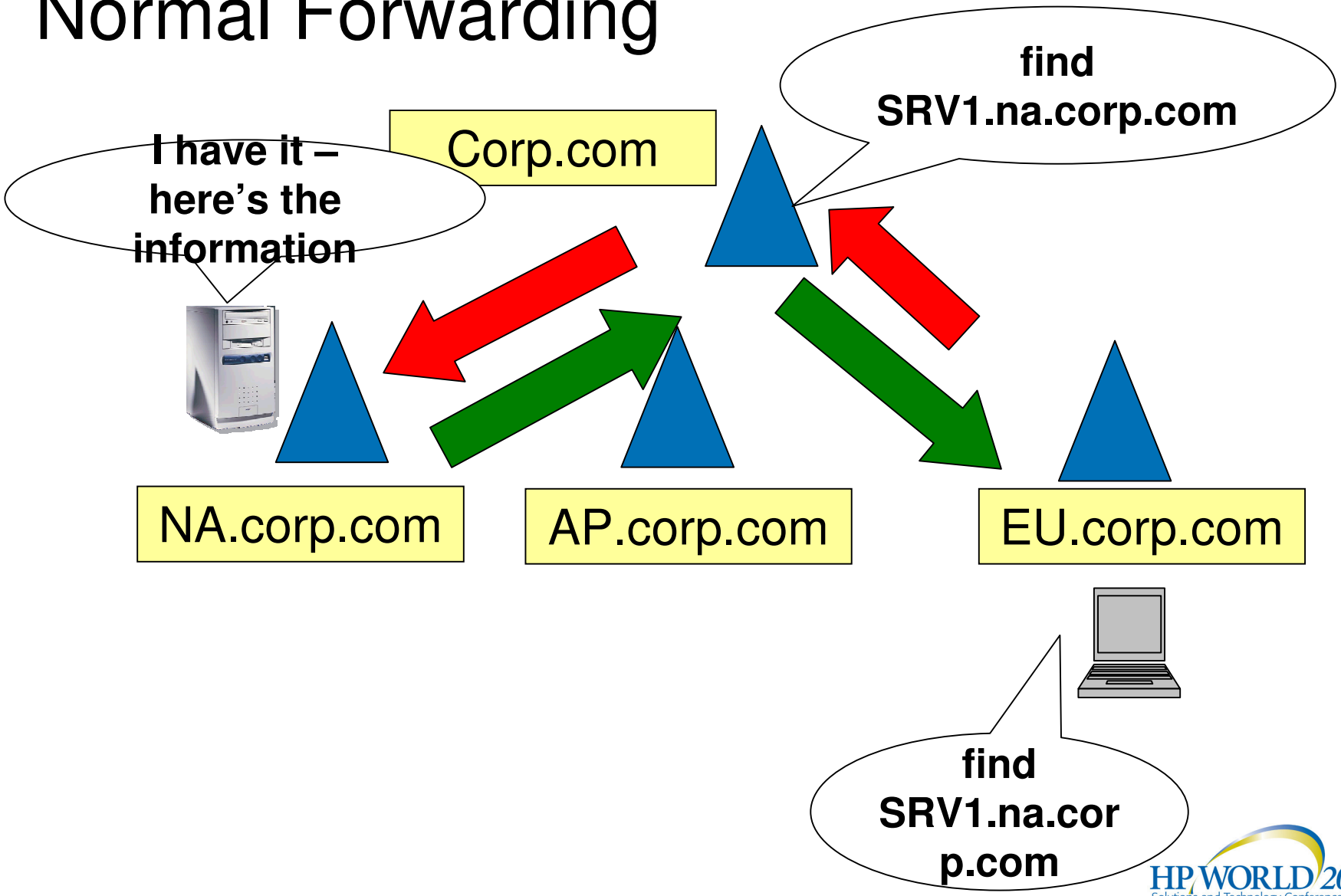
- Scope: Selected DCs in Forest.
  - **Can cross domain boundaries.**
  - **As few/many replicas as you want (not replicated to GC).**
  - **Observes site topology, schedule.**
  - **Can contain any object type *except* security principals.**
  - **Named/located via DNS (*e.g.*, mstapi.sales.msn.com).**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

DNS Improvements

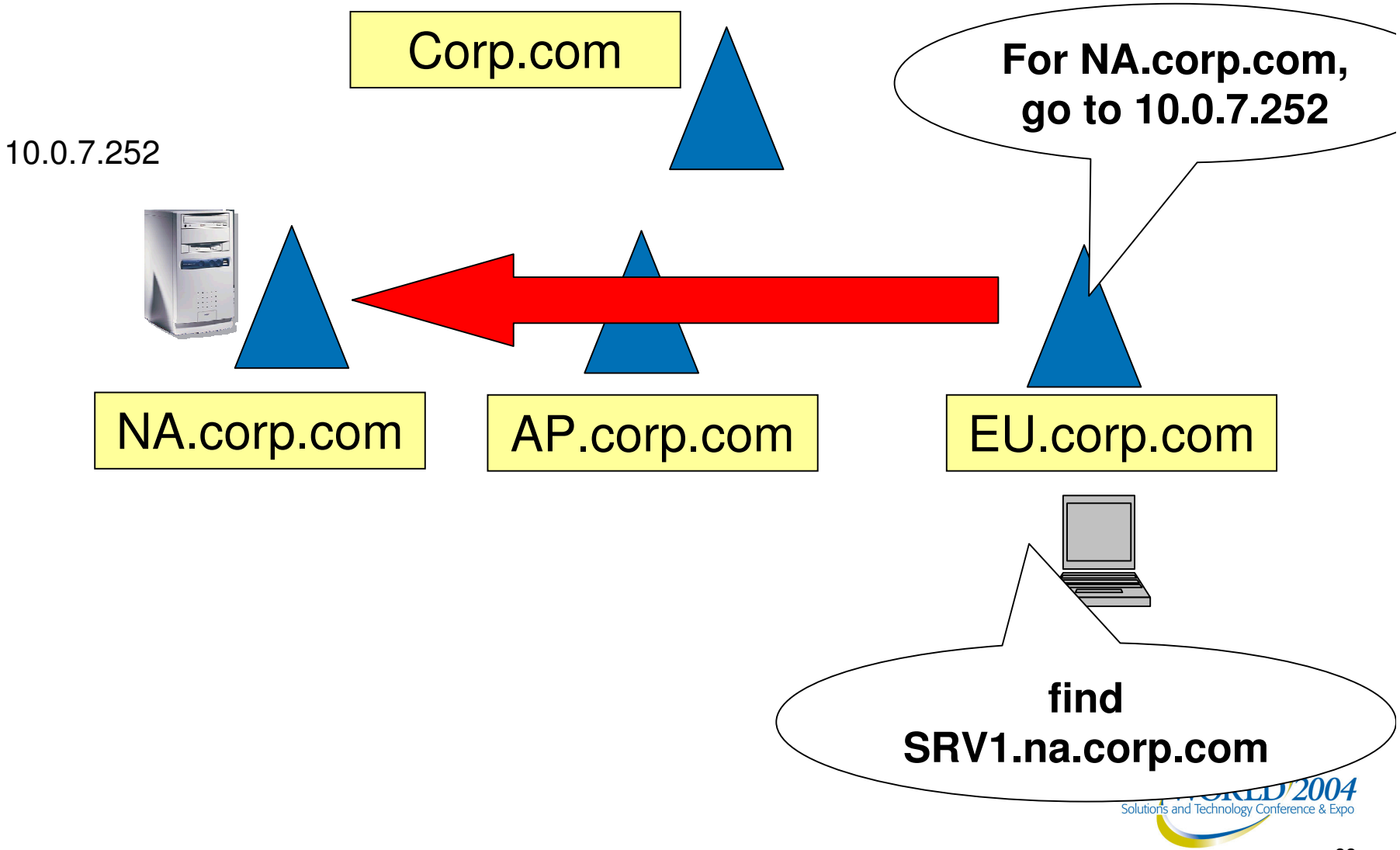
- DNS server
  - **Conditional forwarding and stub zones.**
    - Improved, efficient Name Resolution.
  - **Application Partition.**
    - Puts DNS records only on Name Servers/DCs**.**
  - **DNS event log now in DNS snap-in.**
  - **WMI provider – MicrosoftDNS.**

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

Normal Forwarding



With Conditional Forwarding



“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” Solution

- Win2k
  - Permits it by default.
  - SP 3+ permits deletion of read only objects (GC).
- 2003 behavior
  - New Install = Tight: Stops Replication until repaired (Default).
  - Upgrade = Loose (Default) .
- Registry setting allows Admin to change it
- Windows Server 2003 Cleanup:
  - Repadmin /removelingeringobjects
  - See Repadmin /experthelp
  - Windows Server 2003 Repadmin only!

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

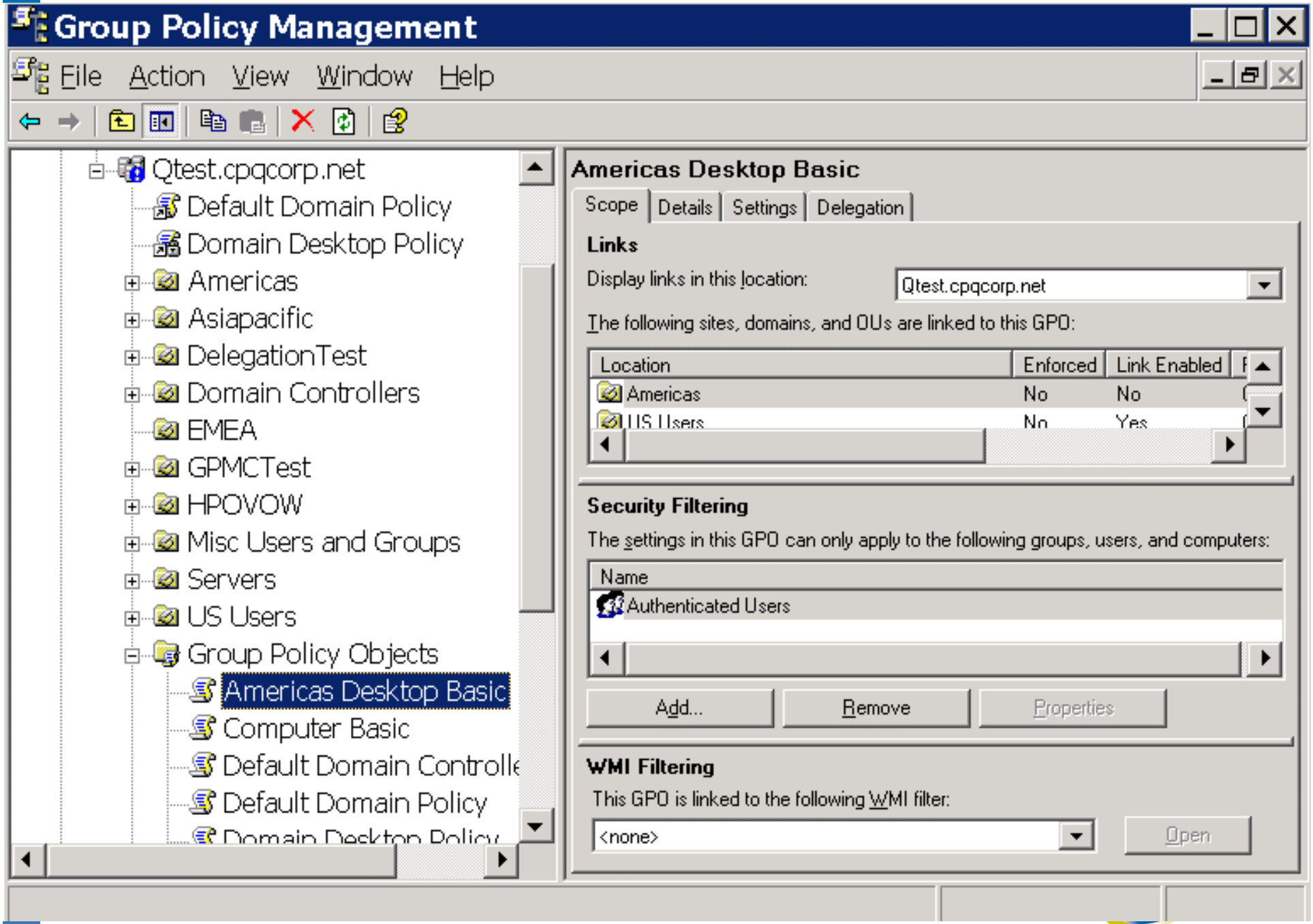
- **Software Restriction Policies**
  - **FIPS 140-1**
  - **Rules:**
    - **Path**
    - **Hash**
    - **Certificate**
    - **Internet Zone (useless)**
- **Tools**
  - **GPResult built in to 2003, XP**
  - **Resultant Set of Policies (RSOP)**
    - **Logging – Current settings applied**
    - **Planning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

New! GPResult

- GPresult
  - Built in to Windows 2003 Server, XP
  - RSOP
    - Security settings displayed
    - Account settings
    - User Right Settings
    - Audit Settings
  - ACL Filters applied
  - Filtered GPOs (and reason)
  - Admin Template (registry) settings
  - Works in a Windows 2000 domain but only from an XP or Windows Server 2003 client.

Group Policy Management Console

- Manage all policies for all Domains, all OUs in forest with one GUI based tool
- Run GPResult to see policy apply for any user on any machine – without bothering the user or the machine.
- Save GPO and GPResults in HTML format
  - Off-line analysis
  - Send to Support Engineers for analysis
- Troubleshooting
  - GPOs applied, not applied and why
  - Easily see all settings applied without wading thru gpedit
- Backup/Restore policies

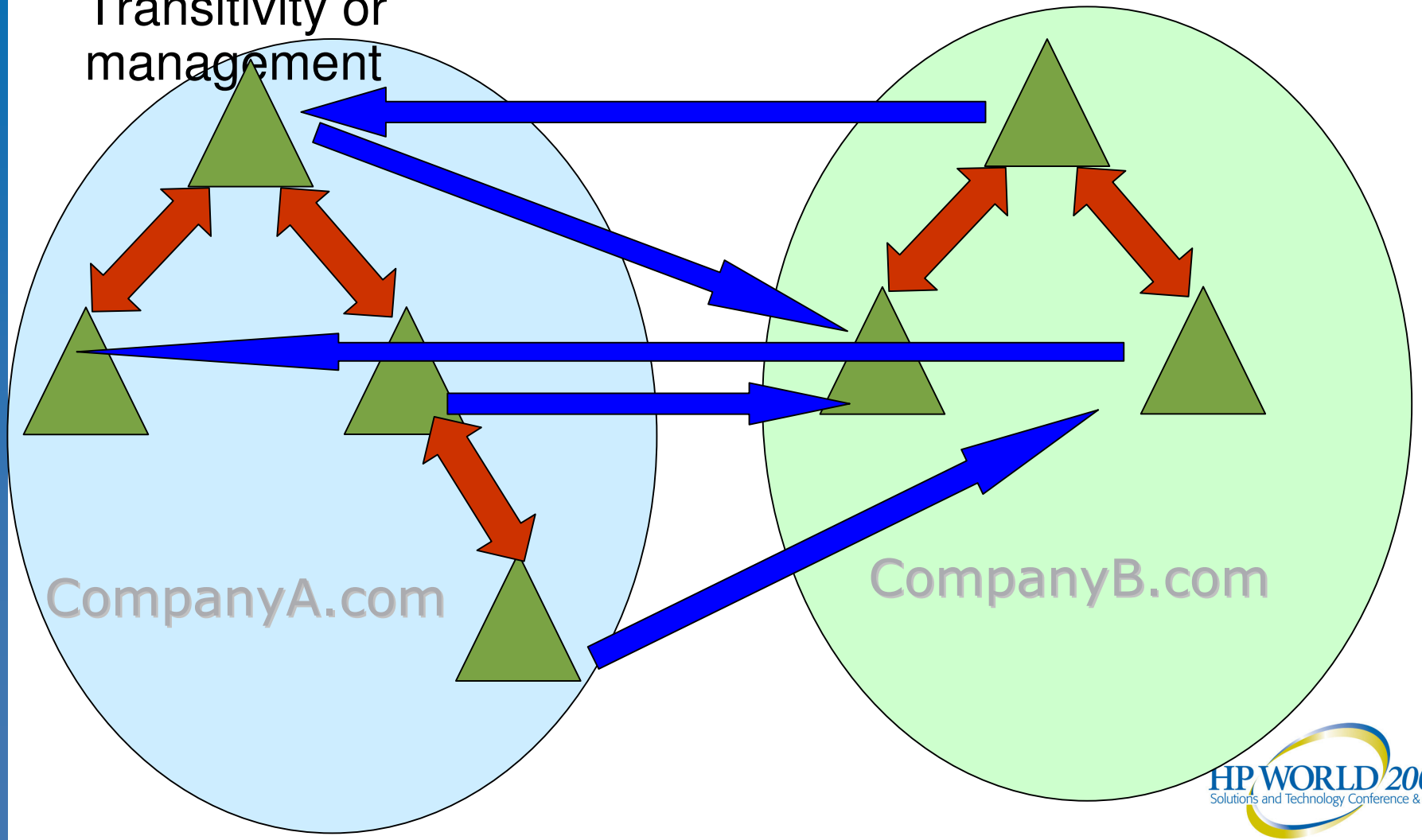

Group Policy Management
File Action View Window Help
Qtest.cpqcorp.net
Default Domain Policy
Domain Desktop Policy
Americas
Asiapacific
DelegationTest
Domain Controllers
EMEA
GPMCTest
HPOVOW
Misc Users and Groups
Servers
US Users
Group Policy Objects
Americas Desktop Basic
Computer Basic
Default Domain Controlle
Default Domain Policy
Americas Desktop Basic
Scope Details Settings Delegation
Links
Display links in this location:
Qtest.cpqcorp.net
The following sites, domains, and OUs are linked to this GPO:
Location Enforced Link Enabled
Americas No No
US Users No Yes
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Authenticated Users
Add... Remove Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open

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.

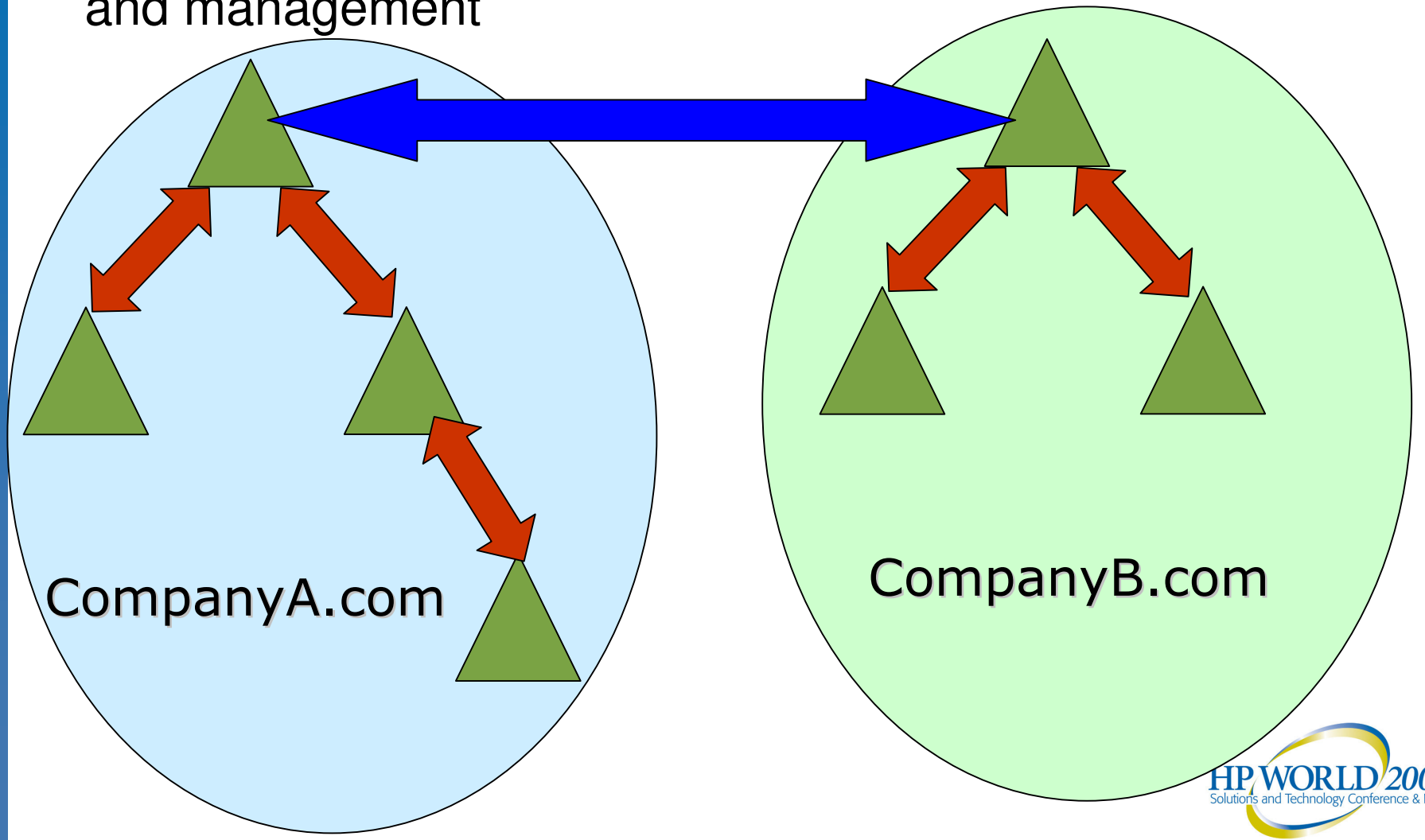
Windows 2000 Inter-Forest Trust

- No Inter-Forest Transitivity or management
- NTLM Based



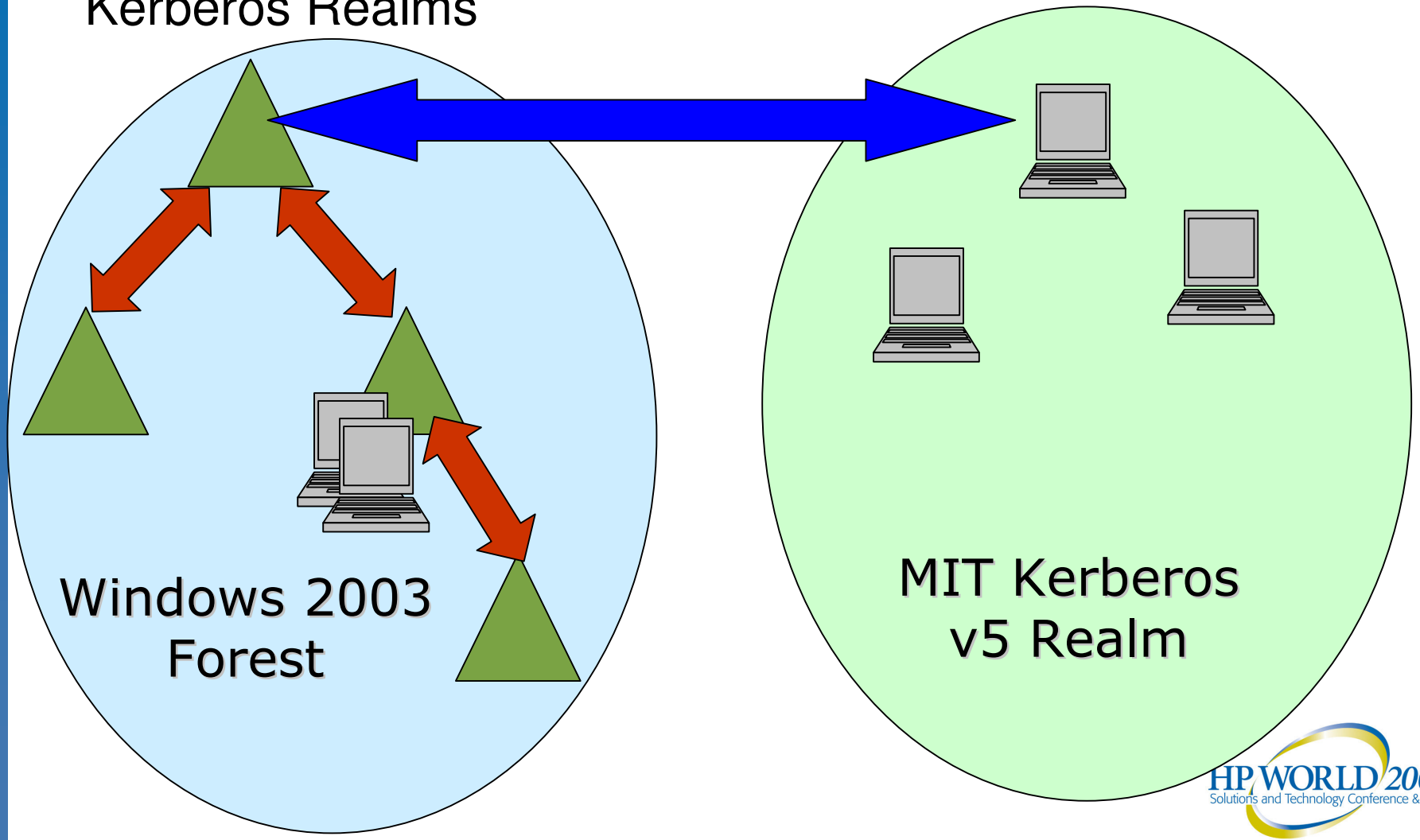
Windows 2003 Inter-Forest Trust

- Full Inter-Forest Transitivity and management
- Kerberos Based



Windows 2003 – Kerberos Realm Trust

- Interoperability between Windows 2003 Forest and Kerberos Realms

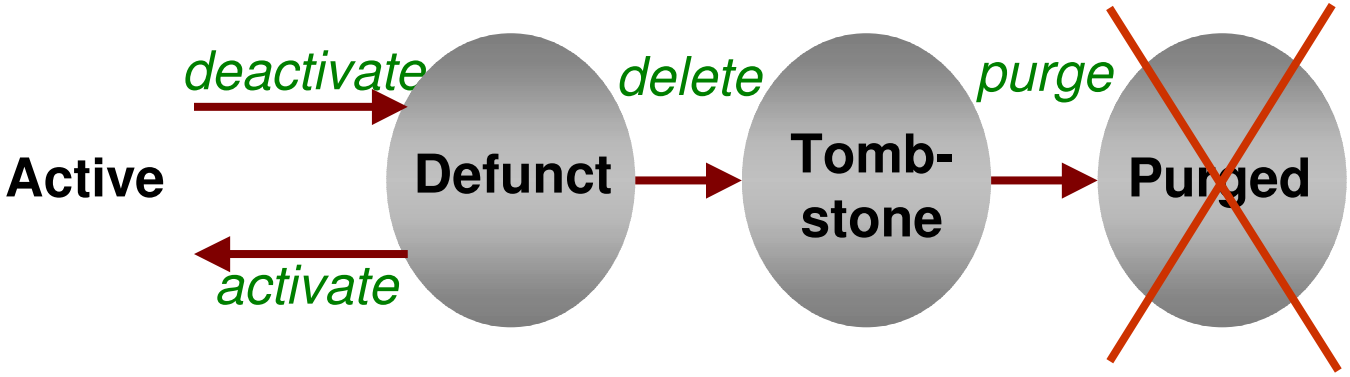


Remote Desktop Features

- 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



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:
  - Exchange 2003 SP1
  - Forest Native mode
  - No “Grafting” or merging of Forests!
  - **Application Compatability**
    - **No compatability list (even of MS products)**
    - **Shares, printers**
    - **Think of how many components use domain name**

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.
- Group Policy Management Tool
- Ultrasound, and Ultrasound Help File for FRS
- Support Tools
  - Shipped on Windows Server 2003 CDs
- More info at the Active Directory Troubleshooting Session #3830 8:00 – 12:00 Tuesday (4 hrs of fun and games)

New! Netdom

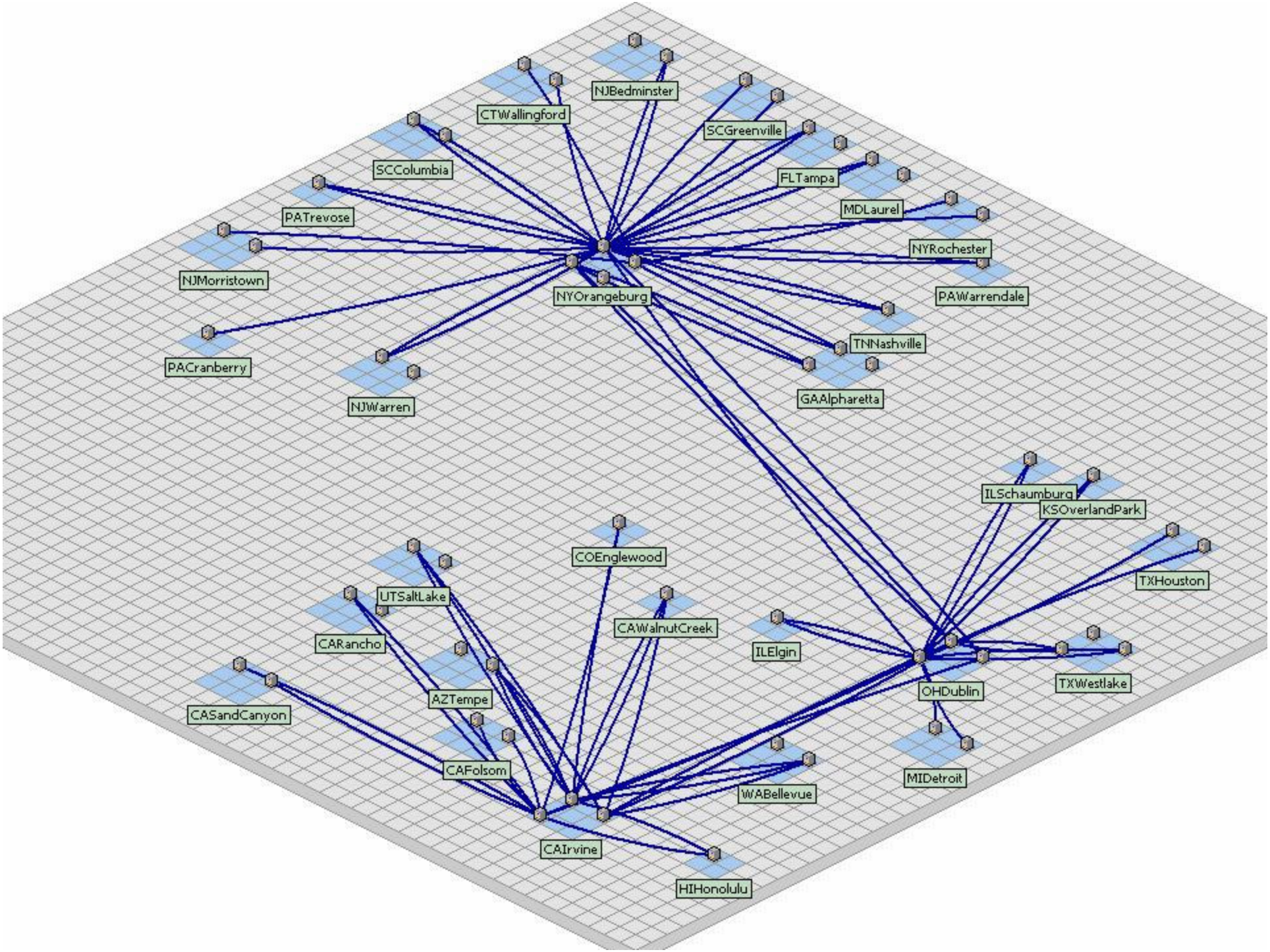
- Netdom
  - RenameComputer (rename workstation, server)
  - Computername (rename DC)
    - This can be done in the UI
      - My Computer-Properties-Computername tab – just like any workstation or server.
    - Netdom version allows rename of DNS name, NetBIOS name separately
  - MoveNT4BDC (move NT BDC to new Windows 2003 domain)

New! Repadmin

- Repadmin
  - /experthelp
  - /RemoveLingeringObjects
  - /replsum /bysrc /bydest /sort:delta
    - Current replication status of all DCs in forest
    - Replicating within schedule?
  - /bridgehead
    - Lists all BHS in forest
  - /istg
    - Lists all ISTGs in forest
  - /latency
    - Shows delta since last successful replication
    - Latency of each DC in the forest.
    - Good way to identify machines that are way out of sync

OpenView for Windows

- Windows 2000 and 2003
- Active Directory Monitoring
- Active Directory Topology Viewer
- Root Cause Analysis

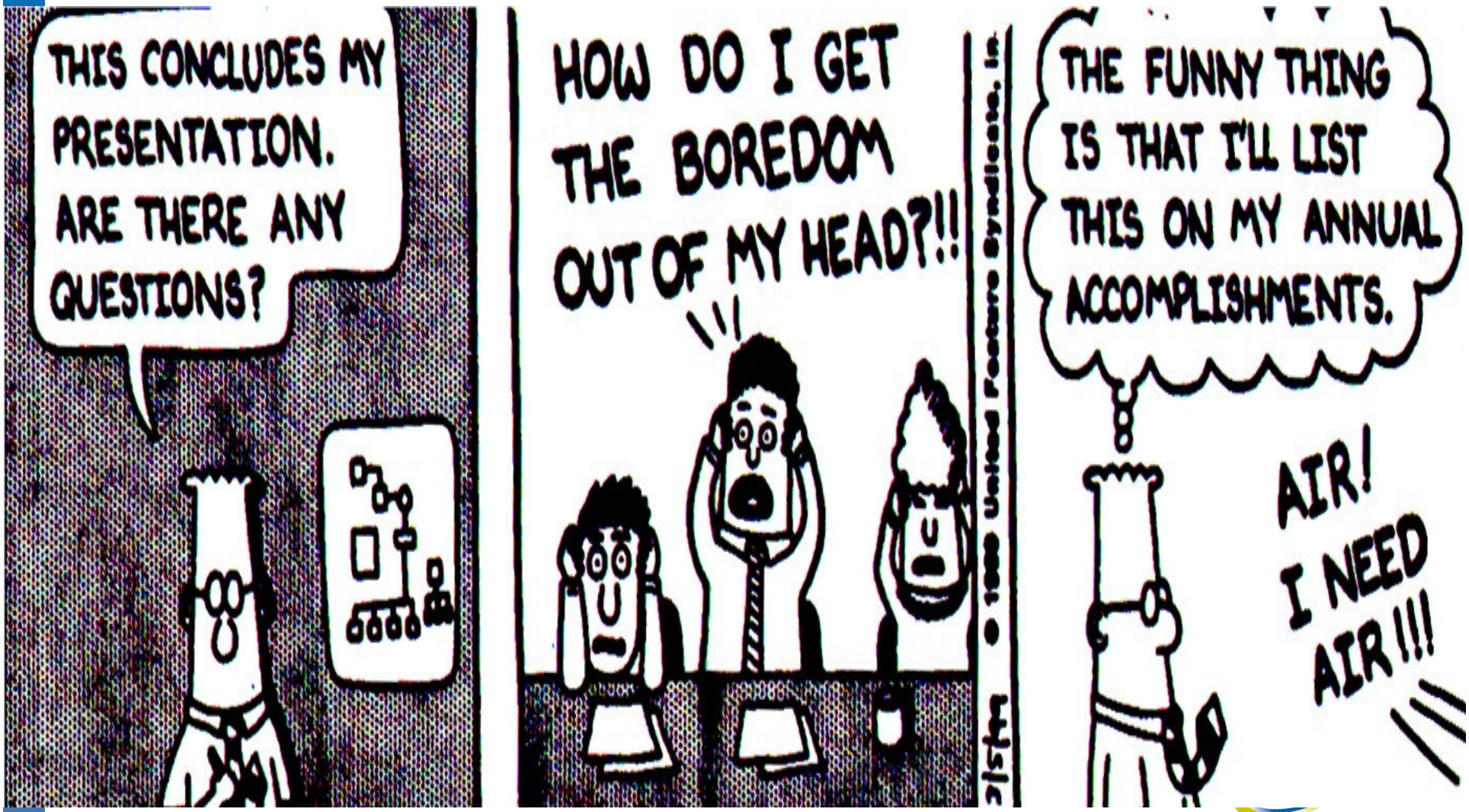

NJBedminster
CTWallingford
SCGreenville
SCColumbia
FLTampa
PATrevose
MDLaurel
NJMorristown
NYRochester
NYOrangeburg
PAWarrendale
TNNashville
PACranberry
NJWarren
GAAlpharetta
ILSchaumburg
KSOverlandPark
COEnglewood
TXHouston
UTSaltLake
CAWalnutCreek
CARancho
ILElgin
TXWestlake
OHDublin
CASandCanyon
AZTempe
MIDetroit
CAFolsom
WABellevue
CAIrvine
HIHonolulu

Should I Upgrade to Windows Server 2003?

It Depends…

- NT4 is at end of life June, 2004
  - There is a program to extend MS Support
    - Pay $50K to HP or $400K to Microsoft
    - Pay $40K per QFE
    - Must submit migration plan to Microsoft
  - Eventually you'll have to (or go to Linux ☺)
- Upgrade from Windows 2000
  - No redesign
  - Simple upgrade (unless you need to change things)
  - When?
    - Analyze the benefits of new features
    - HP: IFM, efficient database, etc. justified upgrade.

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!!!