



Session 3830

Active Directory Troubleshooting: Problems, Methods and Solutions

Gary L. Olsen

WTEC

Global Services Engineering

Hewlett -Packard

Gary.olsen@HP.com

© 2004 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice



Books



Windows Server 2003 on ProLiant Servers

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

<http://WindowsOnProLiant.com>

Authors: Gary Olsen, Bruce Howard

Publisher: Prentice Hall

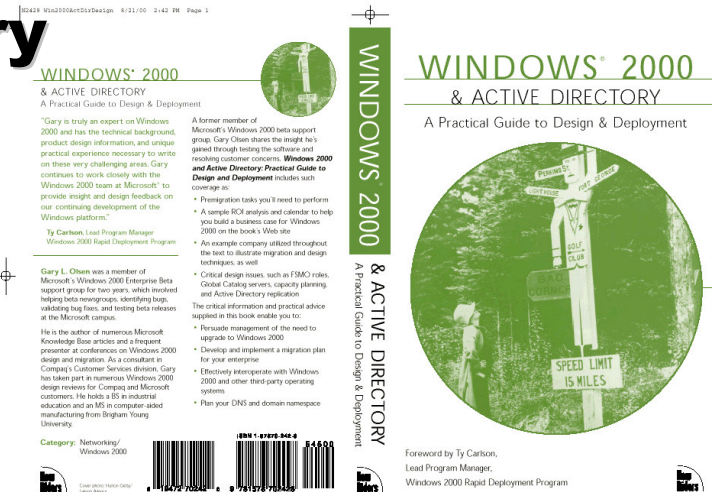
ISBN: 0131467581

Publishing Date: October, 2004

Windows 2000: Active Directory Design & Deployment

Author: Gary Olsen

Publisher: New Riders
ISBN: 1578702429





Topics

- **CLASS EXERCISES!**
 - Troubleshooting Basics
 - Troubleshooting DNS
 - Troubleshooting Replication
 - Troubleshooting FRS Replication
 - Troubleshooting DCPromo
 - Troubleshooting Group Policy



Troubleshooting Basics

Define the Problem
Work the Problem
Collect Data
Action Plan



Define the Problem

Is there one?

- Define the Problem
 - Events are NOT the problem!
 - What exactly is failing?
- Define the Scope
 - One or multiple Machines
 - One or more users
 - Single or multiple sites?
 - Single or multiple DCs? (check logon server env. Variable)
 - Members of same or multiple groups?
 - Group Policy applied (event 1704 in app log)
 - Time of day



Work the Problem

Is there one?

- Impact to the business
 - Urgency
 - Resource allocation
- After Defining the Problem, are there events in the event log related to the failure and time of failure?
- When did you notice it? What conditions?
 - Tie the times to the events, other log entries
- Can the problem be replicated?
 - Start narrowing the variables
 - Identify a savvy user with the problem who can help

Collect Data

- MPSReports
 - Free download (see slide notes)
 - All Event Logs in .txt, evt format
 - Netdiag, DCdiag, Net Accounts, Net Share,
 - Repadmin
 - DCpromo Logs
 - GPOtool, GPreult
 - Run it on all affected machines
- Other
 - Verbose Logging
 - Get status report from Replication Monitor

The Action Plan

- Define the Problem
 - Talk to all admins involved
 - Who is affected? (computers, users)
 - When? Is it reproducible?
 - Area
 - Replication
 - Security
 - Name Resolution
 - Group Policy
 - FRS/DFS
- What data needs to be collected?
- Analyze the Data
 - Errors, warnings, etc
 - Solution
 - Google
 - www.eventid.net
 - Microsoft KB
- Test Solutions

Action Plan Example

Overview: Determine cause of hang of ATL-DC1

Summary:

- analyzing perfmon logs
- implemented contingency plan
- identified support path

Action: Perfmon log analysis.

Why: to compare baseline (current) with Monday's hang events

Priority: Medium

When: March 25

Who: Jim Shoos, Don Juan

Status: In progress

Action: Crash dump analysis.

Why: determine cause of Monday's hang

Priority: Medium

When: March 27

Who: Jack Sprat

Status: In progress



Troubleshooting DNS

Basics

Configuration Issues

Server, Client

Active Directory Integrated Zones (ADI)

Delegation, Forwarding

Quick Checks

Common Problems

Problem Solving Exercises



DNS Basics

- Understand DNS
 - www.microsoft.com/dns (DNS Center)
- Analyze the DNS infrastructure
 - Diagram
 - Details (delegation, forwarding, etc)
- Netlogon registers DNS records
 - Net start Netlogon & Net stop Netlogon
- Zone must contain `_msdcs`, `_sites`, `_tcp`, `_udp` sub zones for SRV records

DNS Resolver Configuration

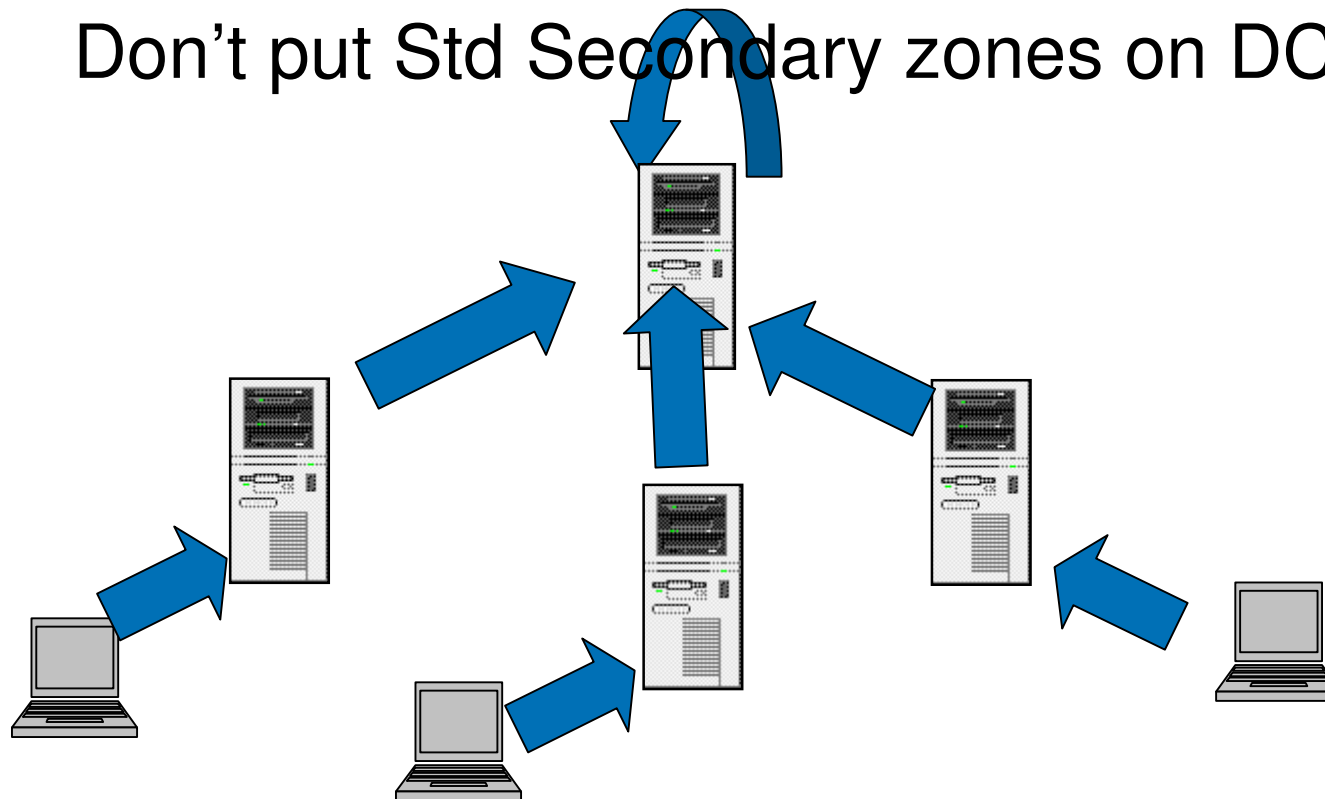
- Workstations, Servers, DCs point to NS for their domain
 - No reason to point to other name servers like ISP, other internal NS, as “additional DNS servers”
- Std primary zone name server – points to self for DNS
- ADI Zone
 - Only one NS points to self for DNS
 - Other NS point to single “primary”

DNS Server Configuration

- Server Properties
 - Forwarding
 - Zone Transfers
 - Restricted Servers
 - Enable Scavenging
- Delegation
 - Correct server, IP address?
- Resolver (Tcp/IP Properties)

ADI Server Configuration

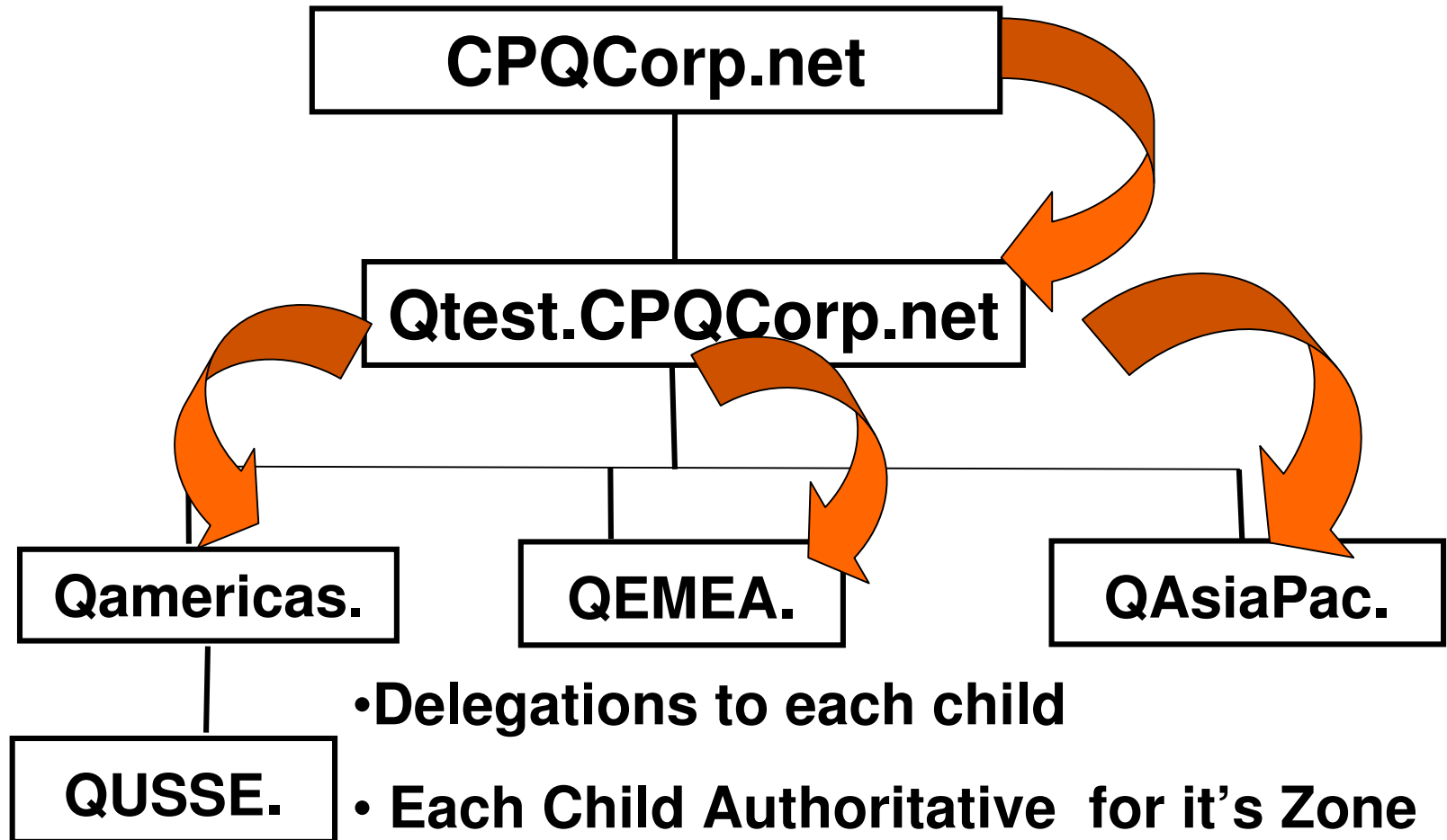
- Best Practice: Select single ADI DNS Server as the “Primary”.
- Fixed in Windows Server 2003
- Don't put Std Secondary zones on DCs!



Qtest DNS Configuration



Delegations

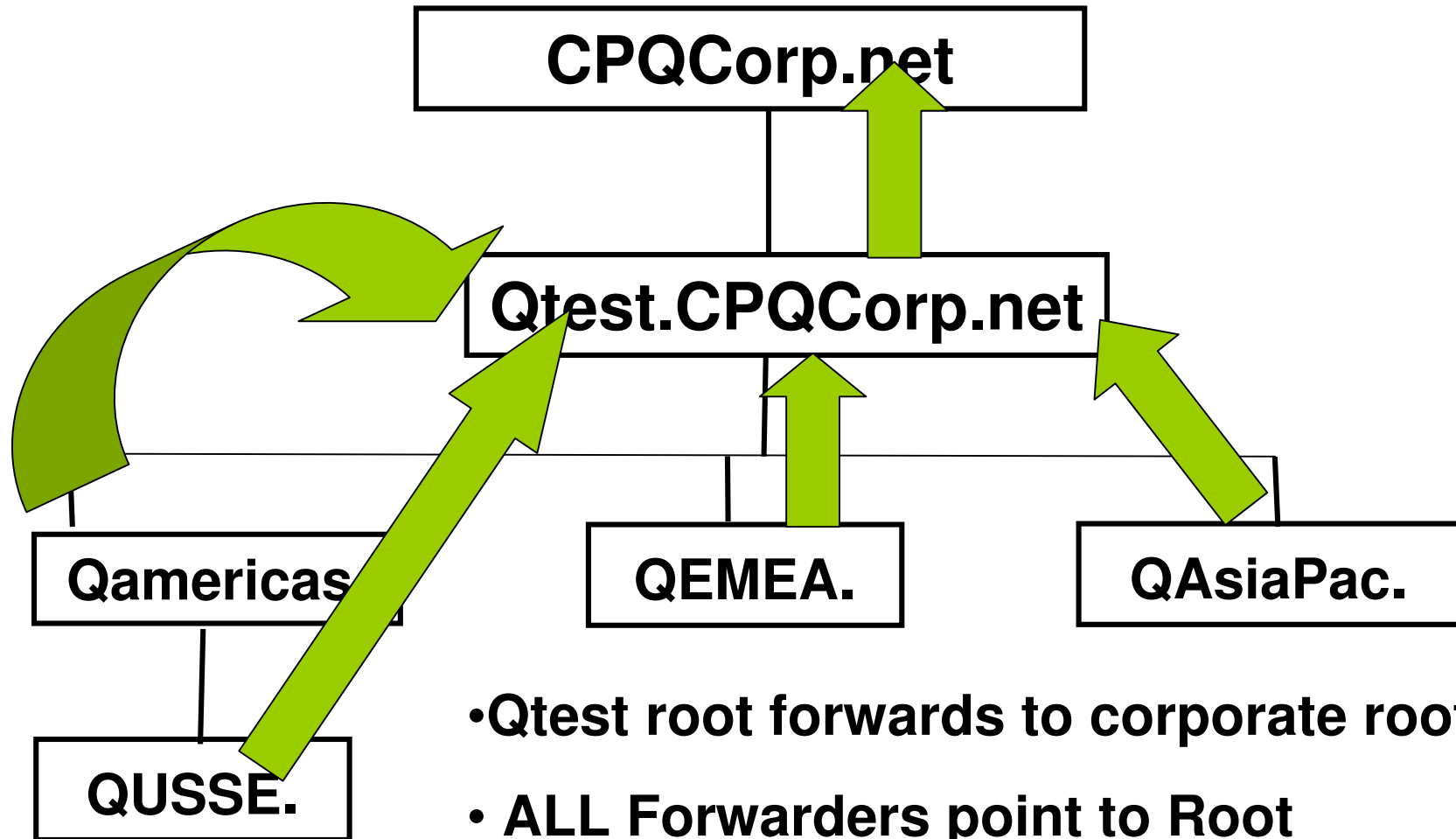


- Delegations to each child
- Each Child Authoritative for it's Zone
- ADI – 2 DNS Servers per Zone

Qtest DNS Configuration



Forwarders



- Qtest root forwards to corporate root
- ALL Forwarders point to Root
- “No Recursion” box checked

Quick Checks

- Access to Internet is different issue
- Clear client and server cache
- Check TCP/IP properties
- Check the DNS topology
 - ADI Zones
- _msdcs zone in root domain only
 - Cname Records
 - GC Records

Quick Checks

- Use Monitor tab in DNS snap-in
 - Test Recursive, simple queries
- Ping
 - Domain name
 - Server Name, address
- NSLookup
 - nslookup gc._msdcs.qtest.cpqcorp.net
- Delete bad records, restart Netlogon svc

Common Problem: Missing sub zones for SRV records



- First DC creates subzones for SRV records
 - _msdcs, _Sites, _TCP, _UDP
- If they aren't there...
 - Check Tcp/ip properties for DNS server
 - Dynamic Updates on
 - Physical connectivity to DNS server
- Bonus Question: What if you delete these zones?

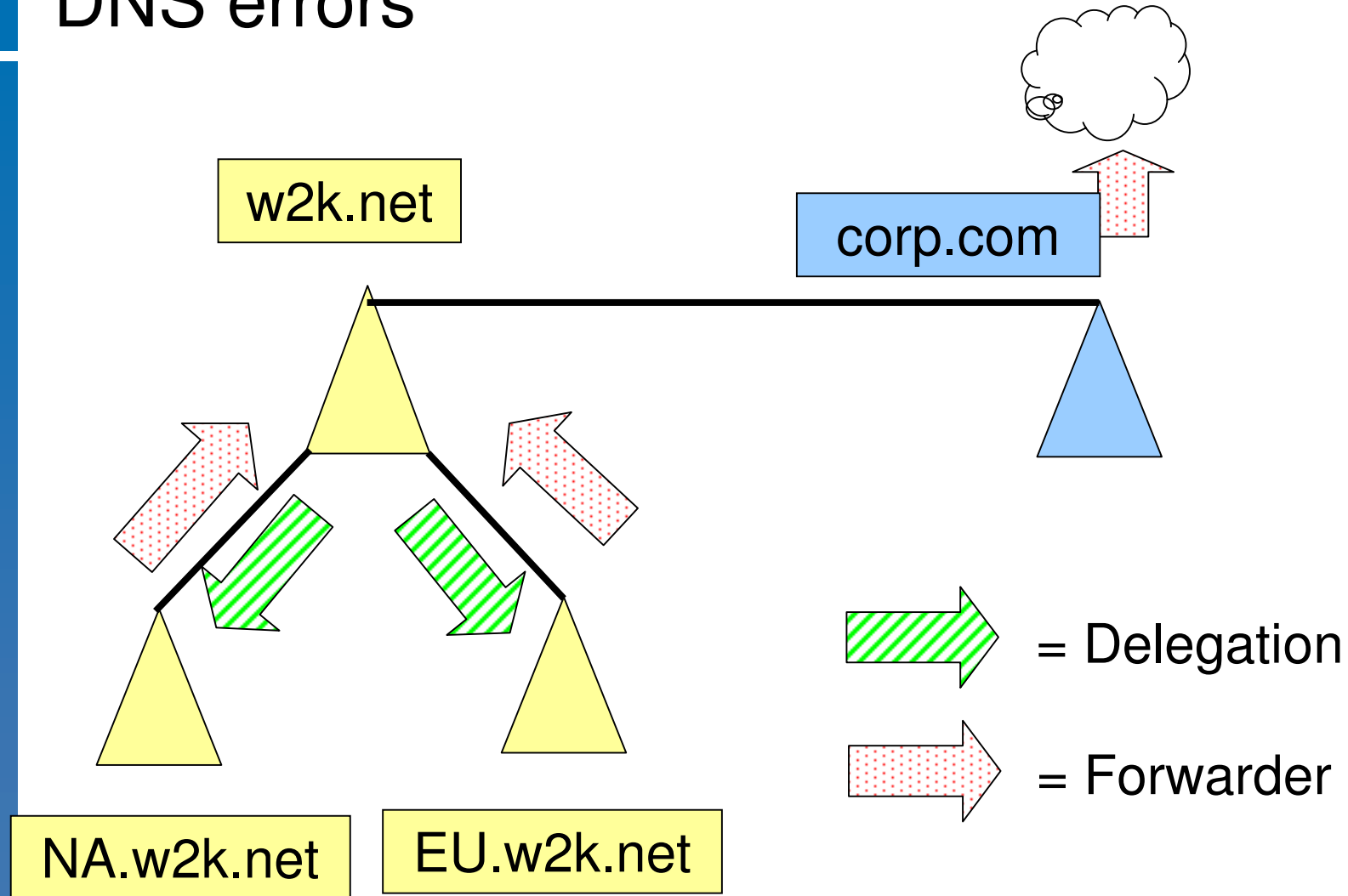


Problem: Promotion of 2nd DC fails: Unable to contact domain

- Just promoted a new DC to create a new forest, company.com.
- Promoting 2nd DC in that domain yields an error saying it can't contact the domain.
- How do you troubleshoot this?

Problem: Replication Broken in child domain

DNS errors





Troubleshooting AD Issues

Tools
MPSReports
Tips
Account Lockout
Problem Solving





XP and Windows 2003 Remote Desktop Resource Redirection

- Client Resources Available when using Terminal Services Remote Desktop
 - **File System** – Local drives and Network drives on Local Machine available on Remote machine
 - **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
 - **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
 - **Terminal Services Virtual Channel Application Programming Interfaces (APIs)** are provided to extend client resource redirection for custom applications.



Windows XP as a Tool!

- Adminpak for Win2K
- Adminpak for Windows 2003
- GResult.exe
 - RSOP, ACL Filters, Policy Priority List,
- Group Policy Management Console
 - Save GPO settings, User application
- Repadmin (new features)
- Remote Desktop

NTDSUtil (Windows 2003)

- Authoritative restore
 - Roll AD back to previous date
 - Entire AD, tree or object
 - Improved in Windows Server 2003 (with LVR)
 - DSRM Mode
- Domain management
 - Create Application Partitions
 - Pre-create domains
- Metadata cleanup
 - Remove Server, domain, site objects
- Roles
 - FSMO Management: See, change all roles
- Semantic database analysis
 - Can repair checksum, inconsistency errors
 - DSRM mode
- Set DSRM Password or account password



ADSIedit.exe Demo

- GUI much like Users & Computers snap-in/Advanced features.
- Graphical view of AD.
- Like LDP.exe but:
 - Easier to browse.
 - Can modify attribute values
 - **Shows ALL attributes**
- Don't confuse with Users & Computers!

LDP.exe Demo

- Takes time to set up:
 - Connect
 - Bind
 - View – Tree
 - Enter DN to start (blank for default)
- Exposes attributes quickly, easy to see.
 - **Only lists DEFINED attributes**
- Faster than ADSIedit – no GUI to traverse.
- LDAP searches.
- Can delete and modify, but not as easy as ADSIedit.
- Can execute remotely.



MPS Reports

- Demo/Exercise – Using MPS Reports for AD Troubleshooting, Health Check

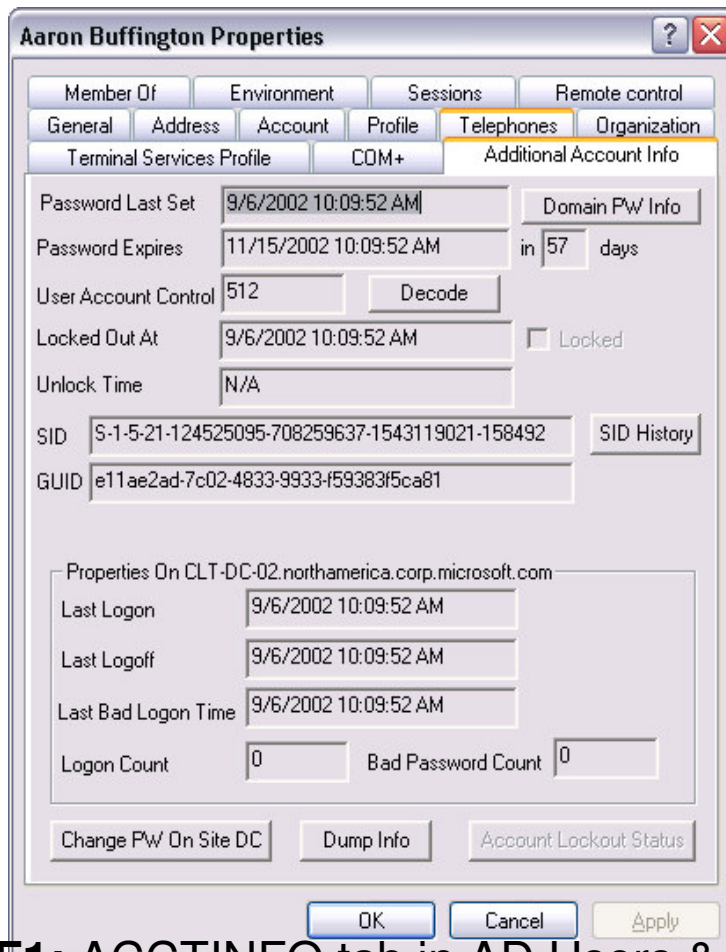
Tip: Tracking Down a GUID

- Problem: GUID referenced in event log. What is it?
- Solution: (Q216359)
 - LDP – search for the GUID
 - **Search: <guid=5d718c23-253b-4310-94f0-9d6c62bea3ad>**
 - Search.vbs in Support tools
- Orphaned Object (will kill replication)
 - Turn up NTDS diagnostic logging
 - Internal processing
 - Replication
 - Find object (GUID) in event logs
 - Delete it via LDP

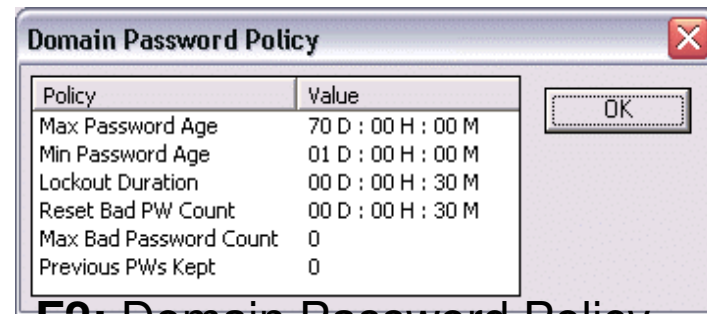
Account Lockout

- Problem: User changes password, account gets locked out
- Causes:
 - User logged in to multiple machines with old credentials (VPN from home, etc.)
 - User has mapped drives with old creds
 - Watch those lab machines!
- MS Solution: Increase retries to 10
- Tools to help...

Tool: Acctinfo.dll Produces new User property tab...



F1: ACCTINFO tab in AD Users & Computers snap-in

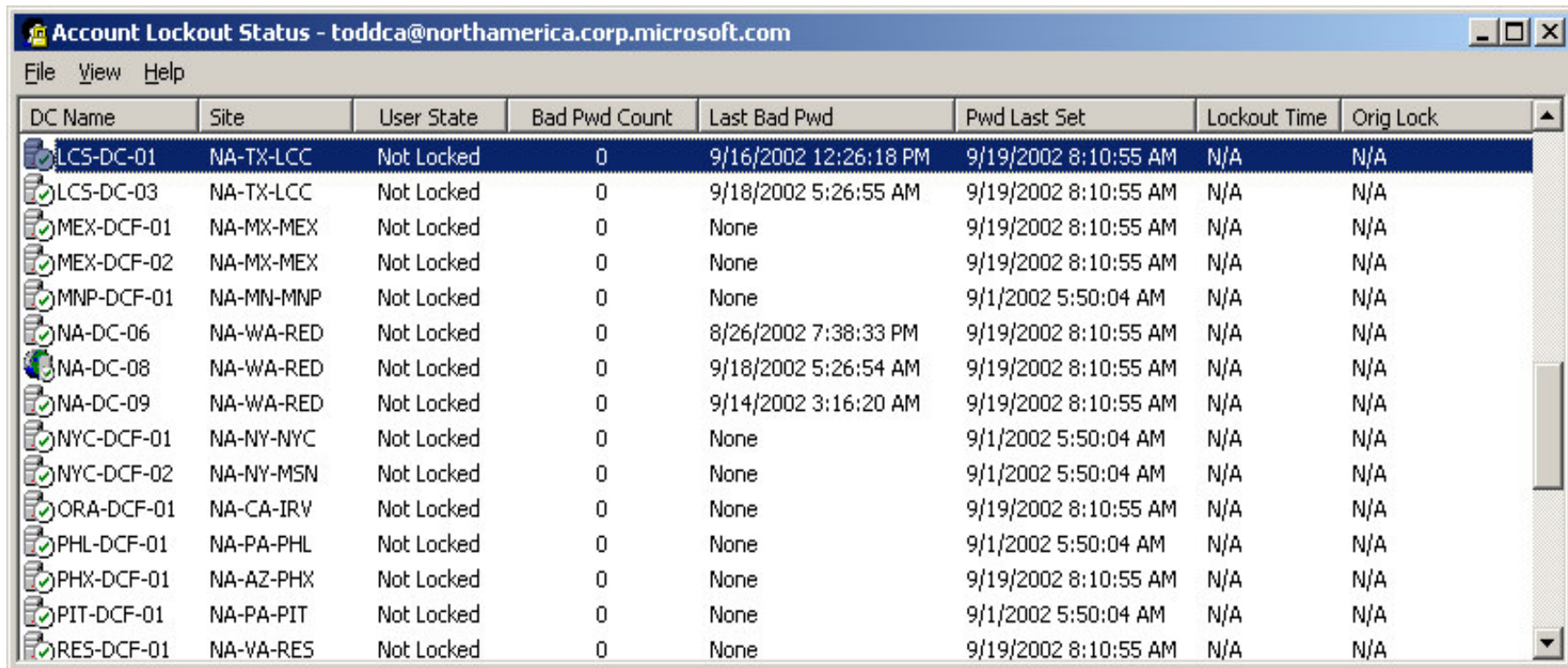


F2: Domain Password Policy

F3: Users computer name used to change p/w on DC in AD same site



Tool: LOCKOUTSTATUS.EXE



Account Lockout Status - toddca@northamerica.corp.microsoft.com

DC Name	Site	User State	Bad Pwd Count	Last Bad Pwd	Pwd Last Set	Lockout Time	Orig Lock
LCS-DC-01	NA-TX-LCC	Not Locked	0	9/16/2002 12:26:18 PM	9/19/2002 8:10:55 AM	N/A	N/A
LCS-DC-03	NA-TX-LCC	Not Locked	0	9/18/2002 5:26:55 AM	9/19/2002 8:10:55 AM	N/A	N/A
MEX-DCF-01	NA-MX-MEX	Not Locked	0	None	9/19/2002 8:10:55 AM	N/A	N/A
MEX-DCF-02	NA-MX-MEX	Not Locked	0	None	9/19/2002 8:10:55 AM	N/A	N/A
MNP-DCF-01	NA-MN-MNP	Not Locked	0	None	9/1/2002 5:50:04 AM	N/A	N/A
NA-DC-06	NA-WA-RED	Not Locked	0	8/26/2002 7:38:33 PM	9/19/2002 8:10:55 AM	N/A	N/A
NA-DC-08	NA-WA-RED	Not Locked	0	9/18/2002 5:26:54 AM	9/19/2002 8:10:55 AM	N/A	N/A
NA-DC-09	NA-WA-RED	Not Locked	0	9/14/2002 3:16:20 AM	9/19/2002 8:10:55 AM	N/A	N/A
NYC-DCF-01	NA-NY-NYC	Not Locked	0	None	9/1/2002 5:50:04 AM	N/A	N/A
NYC-DCF-02	NA-NY-MSN	Not Locked	0	None	9/1/2002 5:50:04 AM	N/A	N/A
ORA-DCF-01	NA-CA-IRV	Not Locked	0	None	9/19/2002 8:10:55 AM	N/A	N/A
PHL-DCF-01	NA-PA-PHL	Not Locked	0	None	9/1/2002 5:50:04 AM	N/A	N/A
PHX-DCF-01	NA-AZ-PHX	Not Locked	0	None	9/19/2002 8:10:55 AM	N/A	N/A
PIT-DCF-01	NA-PA-PIT	Not Locked	0	None	9/1/2002 5:50:04 AM	N/A	N/A
RES-DCF-01	NA-VA-RES	Not Locked	0	None	9/19/2002 8:10:55 AM	N/A	N/A

Runs as Standalone utility or extension to ACCTINFO. Shows bad p/w count and time across all DC's in domain

Downloads...

- Account Lockout Best Practices Whitepaper at <http://www.microsoft.com/downloads/details.aspx?FamilyID=8c8e0d90-a13b-4977-a4fc-3e2b67e3748e&DisplayLang=en>.
- The AcctInfo.dll and LockoutStatus.exe tools can be downloaded from <http://www.microsoft.com/downloads/details.aspx?FamilyID=7af2e69c-91f3-4e63-8629-b999adde0b9e&DisplayLang=en>.



Active Directory Problem Diagnosis (Class exercise)

Tried to create a machine account – Error says it already exists, but can't see it in Users and Computers



Troubleshooting AD Replication

Golden Rule
Top 10 Things that Break Replication
Quick Checks
Tools





Golden Rule of Replication Troubleshooting

Always Assume that...

No two domain controllers ever have the same AD information at the same point in time





Top 10 Things That Break Replication

10. Failure by System Architect to Design the topology properly
 - This isn't rocket science!
9. Failure by Administrator to understand Replication
8. Failure by Administrator to monitor AD
7. DNS problems
 - Duplicate connection objects
 - Bad Cname record
 - SRV Records not registered
6. KCC doesn't clean up (by design in Windows 2000)

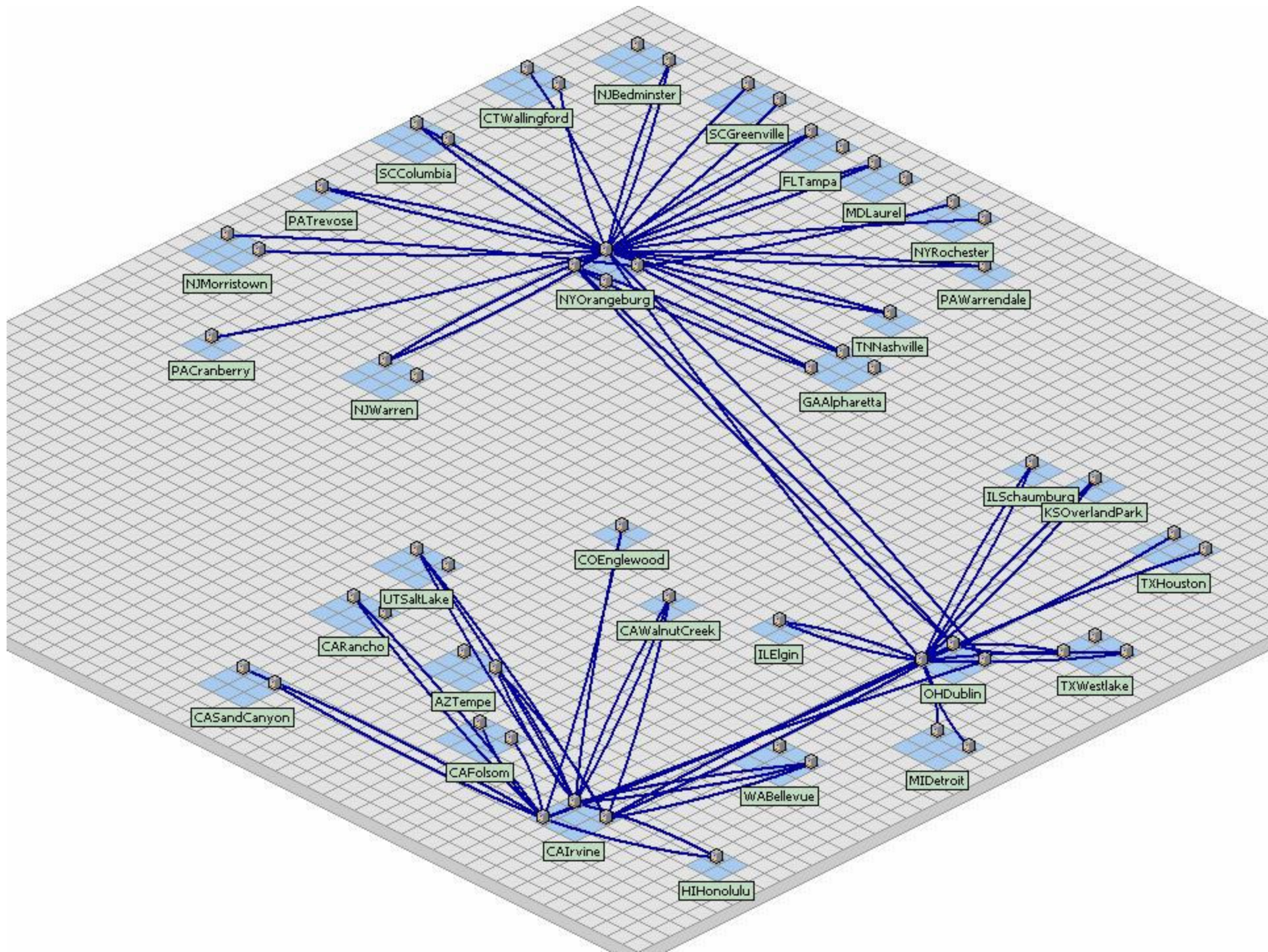


Top 10 Things That Break Replication

5. Orphaned objects, Lingering Objects
4. Poorly routed, IP address changes
3. Messing with schedules, costs, etc.
2. Physical connectivity fails
1. Topology misconfigured
 - Poor design & implementation (see #9,10)
 - Failure to reconfigure DefaultIPSiteLink

Quick Checks

- Who isn't replicating with who?
- MPS Reports (DS)
 - Repadmin
 - /Showreps (Win2K)
 - /replsum bydest bysrc /sort:delta
 - Event Logs
- Map out topology (HP OpenView)





Quick Checks

- Force Replication (snap-in)
 - Returns different error
- Create user, site on broken DC
 - See if Inbound/outbound replication working
- ReplMon – Status Report
 - Not included in MPS Reports

Check Cname DNS Records

- In root `_msdcs` zone (only), alias record mapping DC's FQDN to its server GUID.
 - Only one record per server.
 - Delete duplicates.
 - Match GUID in alias record to GUID reported by `Repadmin /showreps`.
 - If in doubt, delete DC's Alias record(s) and re-start netlogon on broken DC to re-register .
 - Ping `<guid>._msdcs.domain.com`
- OR... Use DNSLINT



Replication Monitor

- Status report (replication health report)
- List of all GCs, BHS, Trusts
- List of all replication errors on all DCs in domain
- Changes not replicated
- Replication partners
- Force push/pull replication
- Group Policy Object status
- FSMO validation

Common Replication Problems

• Event 1311

– Physical

- GC or DC can't be contacted (see event 1722)
- Network Failure
- Improper routing
- Changes in routing, addressing, etc.

– Logical

- Sites w/o site links
- Site Link Bridges covering dial up networks
- Site Links not Interconnected
 - Site link A-B and C-D (no common site)
- Preferred BHS offline

Common Replication Problems

- Logical (cont'd)
 - BHS swamped
 - Undersized
 - Too many satellite sites to single BHS (fixed in W2k3)
 - Site Link Schedule
 - DNS Lookup Failure
 - KCC didn't clean up properly (Windows 2000)
- 1311 Repair
 - Look at the topology (HP OpenView)
 - Review the design and implementation
 - Poor design = lots of 1311s!
 - Are 1311's forest wide, domain wide, or site specific?
 - Repadmin /istg
- 1772 – RPC Server is unavailable.

Common Replication Problems

- Logical (cont'd)
 - BHS swamped
 - Undersized
 - Too many satellite sites to single BHS (fixed in W2k3)
 - Site Link Schedule
 - DNS Lookup Failure
 - KCC didn't clean up properly (Windows 2000)
- 1311 Repair
 - Look at the topology (HP OpenView)
 - Review the design and implementation
 - Poor design = lots of 1311s!
 - Are 1311's forest wide, domain wide, or site specific?
 - Repadmin (see Repadmin slide)



Common Replication Problems

1311 Repair

- Look at the topology (HP OpenView)
 - Review the design and implementation
 - Poor design = lots of 1311s!
- SLB only in fully routed networks
- Preferred BHS: Just say NO! (or upgrade to w2k3)

Common Replication Problems

- 1772 – RPC Server is unavailable.
 - Physical connectivity.
 - DNS.
- DefaultIPSiteLink
 - Failure to treat this as a normal site link after topology is implemented
 - All Sites in here + in other Links (forgot)
 - Treat it as any other link
 - Rename, don't delete... just in case
 - Causes Replication to break, poor performance
 - Test later... ☺
- Time Skew (must be within 5 minutes)
 - W32tm –sync (Windows 2000)
/config /syncfromflags:DOMHIER (Windows 2003)



“Lingering Object” Problem

- The problem
 - Replication broken or DC/GC offline
>tombstonelifetime (TSL)
 - Loose behavior (Windows 2000 pre-sp3)
 - Allows old object to be propagated back to the AD
 - Security Problem (possibly)
 - Kills replication – chokes on orphaned objects
 - GC: propagates read-only objects (can't delete)



“Lingering Object” Fix

- The Fix:
 - Tight behavior (default in Windows Server 2003 clean install)
 - Stops replication until the object is deleted.
 - Q317097
- Cleanup:
 - Repadmin /removelingerobjects
 - See Repadmin /experthelp

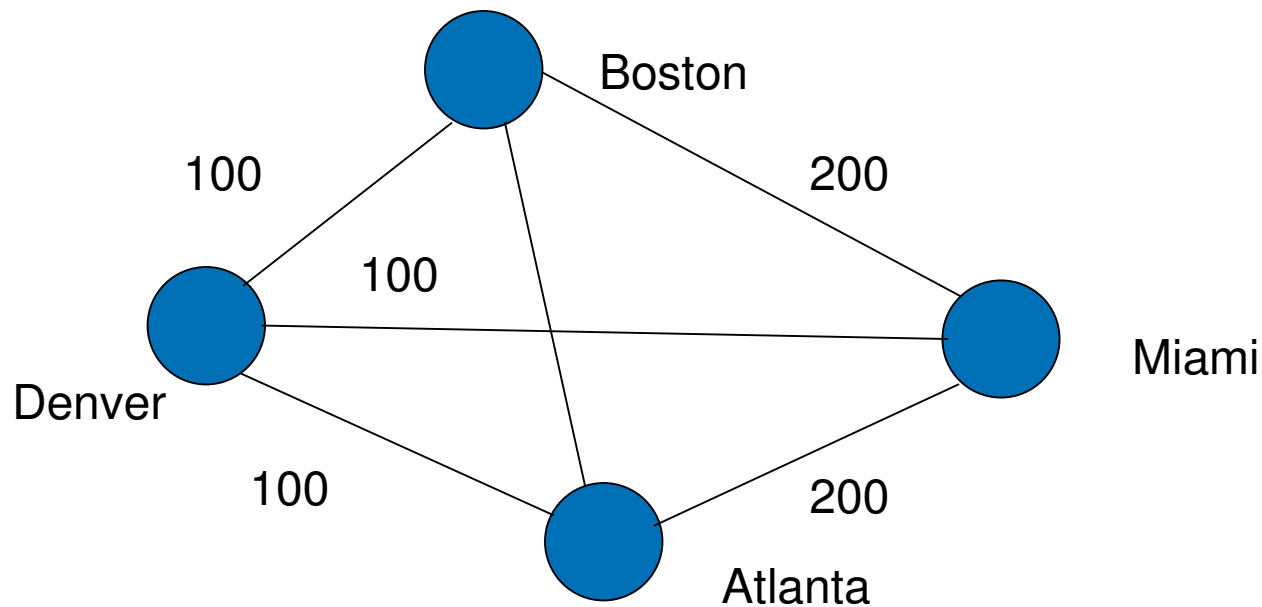
If all else fails, try demoting...

- Normal or Manual Demotion of a DC then repromote to clean up problems
 - Microsoft loves this!
 - Only if problem is isolated to one DC.
 - If replication isn't working, demotion won't work.
 - Can manually demote a DC in Win2K SP3 and Windows 2003.
 - **DCPromo /forceremoval** Then clean up the AD
 - **KB 332199**
- **Warning:** If this is an Exchange Server, manual demotion will break Exchange

Replication Problem Diagnosis (Class exercise)





- Problem 1: Takes twice as long to replicate from Denver to Atlanta as from Denver to Miami. Network bandwidth not an issue.

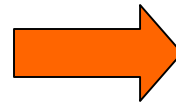


Replication Problem Diagnosis (Class exercise)



- Problem 2: Replication topology automatically changes after a DC becomes unavailable then recovers.
 - 3 tier hierarchy
 - Forcing replication thru certain DCs in each hierarchy (by geography)
 - After DC recovery, KCC reconstructs the topology for that region – ignoring manual design

-  Sites Linking Level 1 and Level 2 "hubs"
-  Sites Linking Level 2 and Level 3 "hubs"



Desired Replication Path

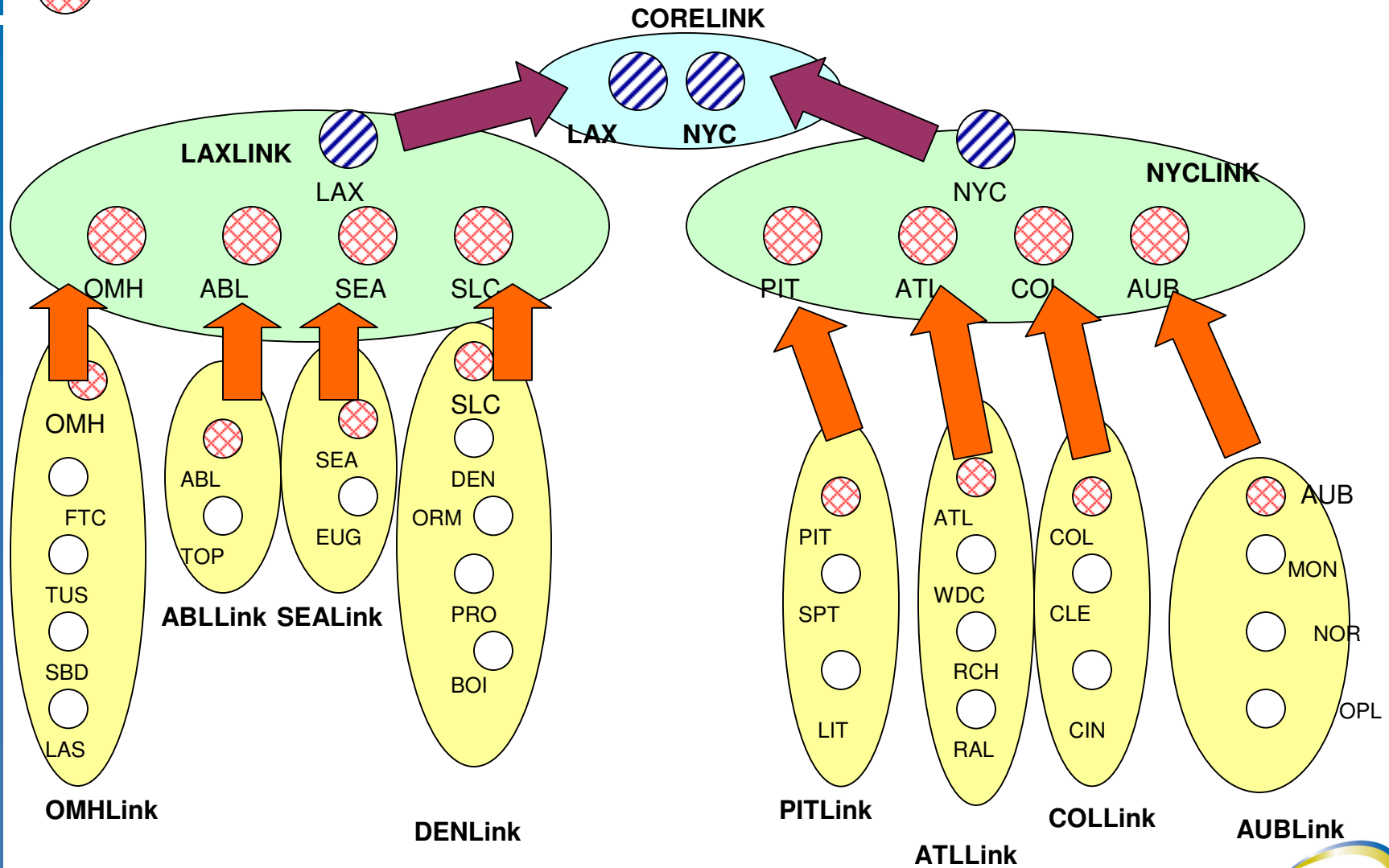
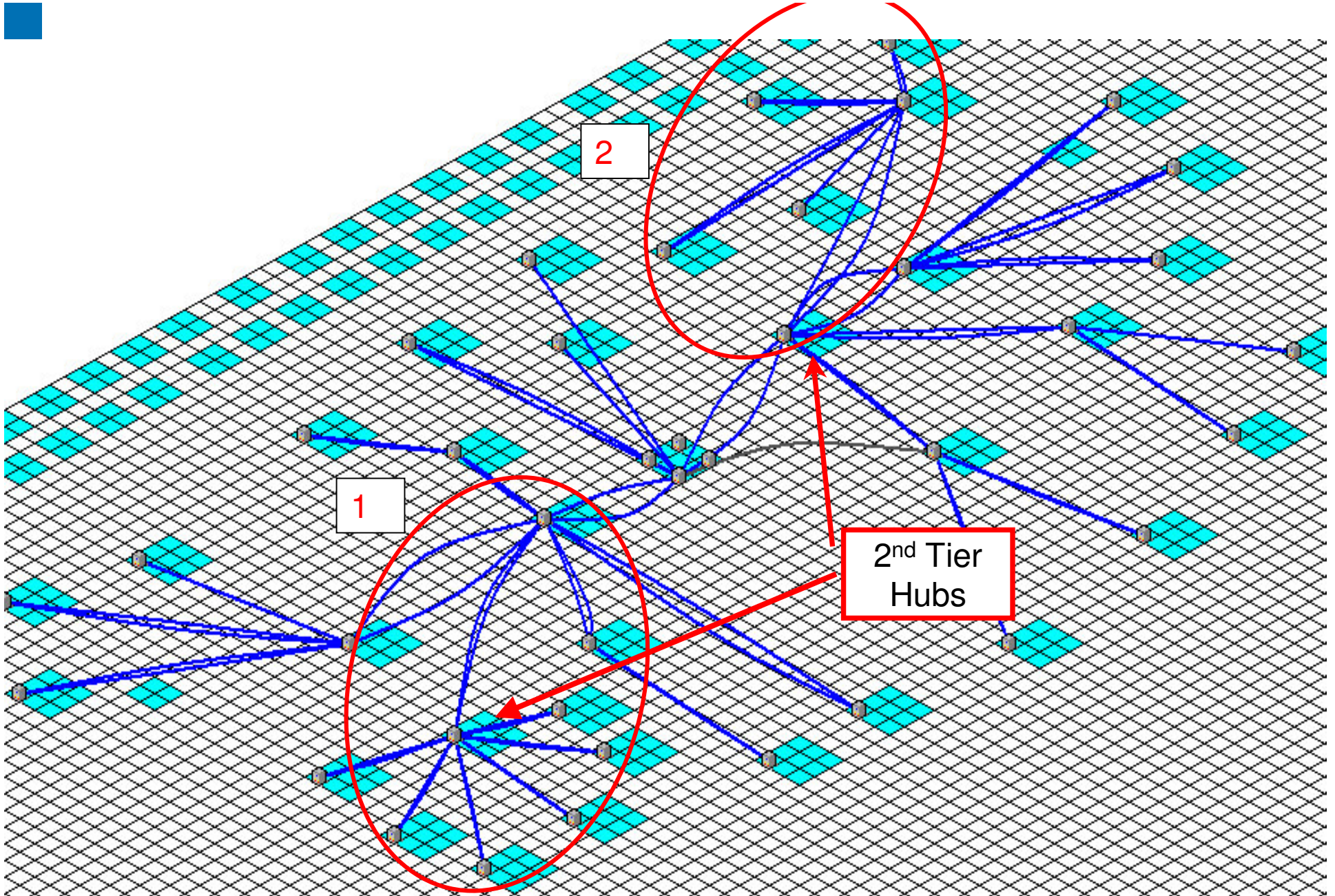


Figure 7.40



Replication Problem Diagnosis (Class exercise)

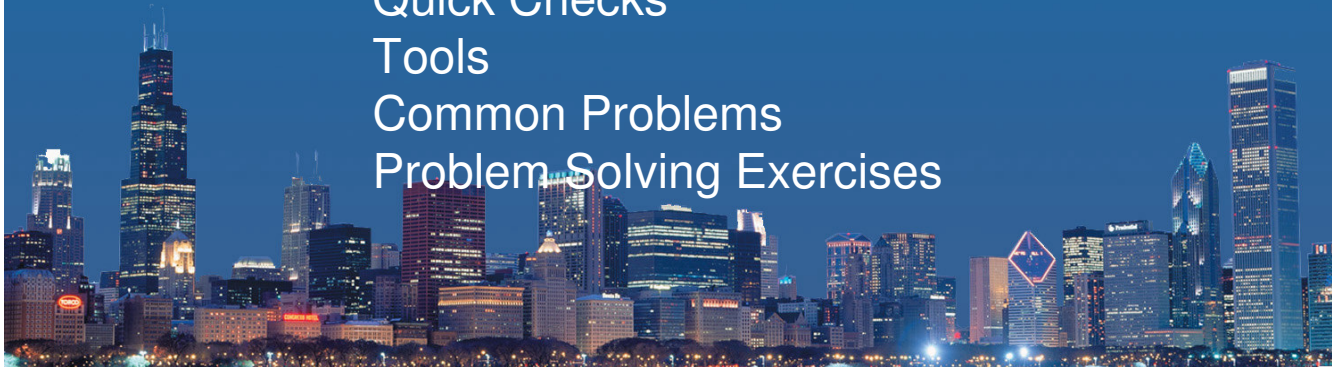


- Problem 3: Event 1311 Source: NTDS
 - The Directory Service consistency checker has determined that there is not enough physical connectivity published via the Active Directory Sites and Services Manager to create a spanning tree connecting all the sites containing the Naming Context DC=mycorp,DC=com. Where do we start?
- Where do we start?



DCPromo Troubleshooting

Basics
Quick Checks
Tools
Common Problems
Problem Solving Exercises



DCPromo Basics

- 1st DC in Forest doesn't need DNS
 - DNS failure will show up with #2 DC
 - DNS “_” zones must exist
- DCPromo will configure DNS
 - First DC in Forest
 - W2k: NO! W2k3: Yes!
- W2K33 – Nice DNS check
- DCPromo isn't successful until SYSVOL and Netlogon shares are created
 - No Sysvol share = Replication failure

DCPromo Basics

- Able to contact a functional existing DC.
 - DNS must be working
 - Dcpromo /replicationsourceDC=
 - NLTest /test:DCPromo (tests DNS)
- Creates/moves Machine acct (DC1\$)
- UserAccountControl Attribute set
 - 4096 (1000 hex) = Workstation/Server
 - 532480 (82000 hex) = DC

Quick Checks

- DNS Set up properly?
 - TCP/IP properties set to correct DNS
 - “_” zones exist
- Proper Credentials?
- Is the DC a DC?
 - Inbound/Outbound Replication
 - SYSVOL and NetLogon shares
 - If no, then no Outbound Replication
 - UserAccountControl = 532480 (82000 hex)

DCPromo tools

- %windir%\debug
 - DCpromo.log (appended)
 - DCpromoui.log (renamed)
- Set verbosity on dcpromoui.log
- Netdiag /v
- DCDiag /v
- Directory Service Event Log

Common Problems

- Missing Sysvol and NetLogon shares
- KB 257338 good but...
 - Create Manual connection object
 - Force Replication
 - Works well for any connection failure
 - Force KCC to “Check Replication Topology”
- Repadmin /add and /sync
 - Adds a low level link and syncs across it
 - Works very reliably
 - **See my article on the CD**

Common Problems

- Errors accessing the machine account (DC1\$)
 - Q250804
 - If server is in a workgroup, join the domain, then Dcpromo (cuts the troubleshooting in half)
 - Account is moved.
 - Error: DC1\$ not found, access denied, etc.
 - Credentials of account running Dcpromo
 - Source must have security policy applied to itself.
 - Q250874
 - Dcdiag /test:MachineAccount
 - /test:FixMachineAccount
 - /test:RecreateMachineAccount

Poor WAN Performance

- Install From Media (W2k3)
 - Source Replica AD from Media in DCPromo
 - GCs or DCs (Replica only).
 - No initial replication from a DC.
 - After initial load, replicates changes.
 - Unattended Answer File Support:
 - ReplicateFromMedia
 - ReplicationSourcePath
- Media useful life < 60 days (or TSL)

DCPromo Problem Diagnosis (Class Exercise)



- Attempting to promote 1st DC in a remote site – fails with specified domain does not exist or cannot be contacted
 - RPC Server Unavailable



File Replication Service (FRS)



Fixes in Windows 2000 SP3 and Windows Server 2003



- FRS Detects and Suppresses Excessive Replication
- FRS Performs Serialized Version Vector Joins
- FRS Does Not Stop Replicating If the Staging Area Is Filled
- Increase in NTFS Journal Size
- Changes to the Automatic Non-Authoritative Restore Functionality



Top FRS Issues

- Morphed Directories
 - Upgrade to SP3 + FRS hotfix
 - Don't use Authoritative Restore
- Excessive replication
 - Get FRS friendly AV software
 - Upgrade to SP3 +FRS hotfix



Top FRS Issues

- Improper design & implementation
 - Topology
 - Staging area space
 - USN Journal size
 - Insufficient hardware
- Missing FRS objects in Active Directory
 - Usually easiest to demote/promote



#1 FRS Issue

- Accidental Bulk Delete of Sysvol or DFS trees
 - Oops!
- Solutions:
 - Authoritative Restore/ Disaster Recovery
 - Watch who you give Admin rights to!



FRS Troubleshooting Tools

- Sonar
- Ultrasound
- FRSDiag
- Ultrasound Help File



File Replication Service

- **Journal Wrap errors + Journal Sizing**
 - Q292438 Troubleshooting Journal_Wrap Errors on SYSVOL and DFS Replica Sets
 - Q315070 Event 13568 Is Logged in the File Replication Service Event Log
- **Staging Directory Sizing & Placement**
 - Q329491 Configuring Correct Staging Area Space for Replica Sets
 - Q265085 Moving FRSStagingPath Requires Non-Authoritative Restoration (RTM,SP1,SP2)
 - Q291823 How to Reset the File Replication Service Staging Folder to a Different (SP3)
- **Staging Directory accumulation**
 - Q307777 Possible Causes of a Full File Replication Service Staging Area
- **Repairing AD Objects used by FRS**
 - Q296183 Overview of Active Directory Objects That Are Used by FRS
 - Q312862 Recovering Missing FRS Objects and FRS Attributes in Active Directory
- **File and Folder filters in FRS**
 - Q229928 Design Decisions, Defaults and Behavior for FRS File and Folder Filters



File Replication Service

- **FRS entries in the registry**
 - Q221111 Description of FRS Entries in the Registry
- **FRS Debug Log Configuration**
 - Q221112 NT File Replication Service Log File Size and Verbosity
- **Morphed or Conflicted Directories**
 - Q328492 Folder Name Is Changed to "FolderName_NTFRS_<xxxxxxx>"
- **QuadZero Service Assertion**
 - Q328800 superceded by Q811217
- **Excessive Replication of FRS content**
 - Q279156 The Effects of Setting the File System Policy on a Disk Drive or Folder
 - Q284947 Antivirus Programs May Modify Security Descriptors and Cause Excessive
 - Q282791 Disk Defragmentation Causes Excessive FRS Replication Traffic
 - Q315045 FRS Event 13567 Is Recorded in the File Replication Service Event Log
- **Sharing violations**
 - Kixstart, real-time antivirus programs, interactive logon scripts, dynamic data

FRS Problem Diagnosis (Class Exercise)

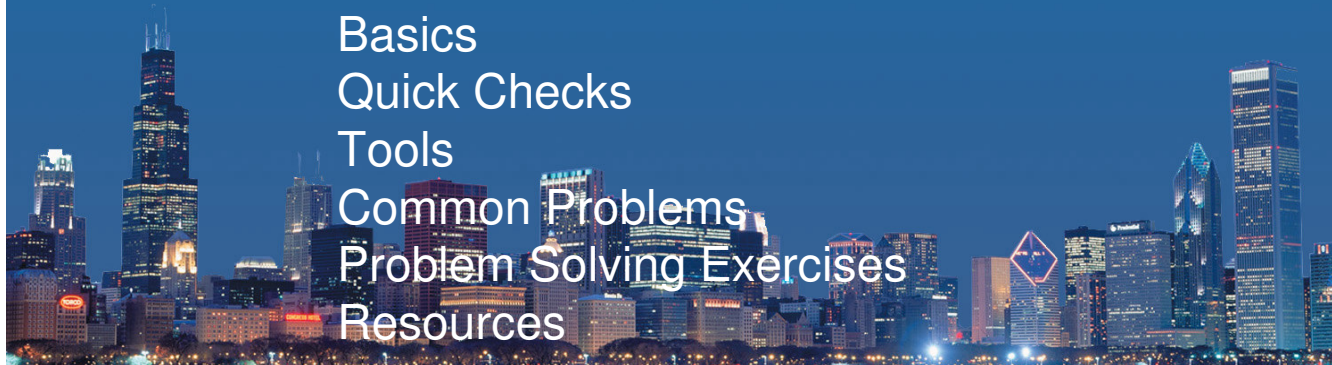


- Problem: Group Policy not being propagated because FRS not working
 - Created txt file in sysvol – didn't make it to some DCs
- Examine NTFSUtl logs using Perl Scripts



Group Policy Troubleshooting

Basics
Quick Checks
Tools
Common Problems
Problem Solving Exercises
Resources



GPO Basics

- Powerful and dangerous
 - ~700 in Windows 2000
 - ~900 in Windows Server 2003
- LSDOU Ordering
 - Apply to Local Machine, Site, Domain, OU
 - Windows Server 2003 Software Restriction Policies don't follow this.
- User must have Read, Apply Group Policy rights



GPO Basics

- Removing the GPO will modify the dynamic registry settings, return to pre-GPO state
- Watch for
 - Inheritance Blocking
 - No Override
 - ACL filtering
 - Loopback



GPO Basics

- GPO only applies to domain/OU where user or computer account reside
 - Won't apply to OU with just groups
- Multiple GPOs cost in logon performance
- Test them before implementing

Quick Checks

- Policy isn't getting applied
 - Computer, user in domain or OU policy is defined for?
 - ICMP disabled or blocked in the network
 - Filtered, Overridden, Blocked, disabled?
 - Not refreshed yet?
 - GPUpdate (replaces secedit /refreshpolicy)
 - FRS or Replication Problem
 - Look for event 1704



New! Gpresult.exe

- Use the XP/2003 version
 - Run on XP client in the domain
 - Built-in
 - Gpresult /V (verbose)
- Returns:
 - Filtered GPOs (and reason)
 - Security Details
 - Account policies
 - User Rights
- Remember
 - Policy is cached – reboot / login to clear
 - Note who authenticating server is
 - Environmental Variable “logon server”



New! GPMC

- Group Policy Management Console
 - Free Download
- Manage all Policies in domain
 - See all options: No Override, blocking, etc
 - Applied GPOs / Denied GPOs (and why)
- Save GPO settings, User Applied Settings
- Modeling (“what if scenario”)



New! GPRresult

- GPRresult
 - 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

← → [Icons]

- 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
 - Domain Desktop Policy

Americas Desktop Basic

Scope | Details | Settings | Delegation

Links

Display links in this location:

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled
Americas	No	No
IIS 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

Userenv.log

- Located: %systemroot%\debug\usermode
- User environment info:
 - Group policy (registry)
 - Client side extensions
- Increase verbose logging (Q221833)
 - (enhanced in Windows 2003)
- Take time – read and study and you may be surprised at what you can find!
- **Sample Userenv.log**



Additional User Mode Logs

- Client-side extensions
 - Registry (demo) Q216357
HKLM\software\Microsoft\WindowsNT\currentversion\winlogon\ GPExtension
 - Errors created in %windir%\debug\user mode
 - Named after the CSE .dll
 - Q245422
 - Produced automatically on error (except winlogon.log)
 - Invaluable in debugging. Use them!
 - **Sample gptext.dll**

Common Problem

- Need to restore Default Domain, Default Domain controllers policies
- Best Practice – Don't mess with these 2 policies
- If you do...
- DCGPOFix
 - Replaces Default Domain Policy
 - Replaces Default Domain Controllers Policy
 - One or both
 - Wipes out old settings like EFS –

Group Policy Problem Diagnosis (Class exercise)



- Problem: Group Policy settings not applied to some clients
 - **User settings made to Users OU GPO**
 - **Some users get them, some don't**
 - **USE GPMC!**

- **Problem: Policy Applies some user settings, but logon script doesn't work.**

Security Problem Diagnosis (Class exercise)



Problem: Set Password Length to 6, History to 24.
However, when user changes password, it forces
length of 8 and History of 5.

- 4 sites, 30 DCs - Affects all users and admins
- Checked all GPOs – none have 8/5 set
- Noticed 2 default domain policies
- 16 GPOs at domain level
- Default Domain policy lowest priority
- Users OU, Computers OU



Group Policy Resources

All Group Policy Resources: <http://www.microsoft.com/gp>
Server 2003 Group Policy Infrastructure

<http://www.microsoft.com/downloads/details.aspx?FamilyId=D26E88BC-D445-4E8F-AA4E-B9C27061F7CA&displaylang=en>

Troubleshooting Group Policy:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=B24BF2D5-0D7A-4FC5-A14D-E91D211C21B2&displaylang=en>

Administering Group Policy with GPMC:

http://www.microsoft.com/windowsserver2003/gpmc/gpmc_wp.msp

