



PRESENTS

**NETWORLD INTEROP**



# Deploying Active Directory Lesson's Learned

---

Richard Puckett

Senior Systems Administrator

Core Distributed Services Group

September 2001

# Cisco's Move to The Active Directory

---

- We “Dog Food” What Our Customer’s Use
- Next Generation Product Reliance on AD
  - Call Manager/Unity/Exchange 2000
  - Internal Directory Enabled Application Development
- Time for a Paradigm Shift in Administrative Models
  - Move Towards a More Centralized, Global Model
- Better Control Over Cisco’s Assets
  - Asset Tracking, Updates, Software Management
  - Remote Control, Help Desk Support
- Convergence Issues/Futures
  - Single Sign-On, PKI, Metadirectory Services

# Now... the Dilemmas

---

- “Who’s Gonna Build/Own This Thing?”  
Building Consensus for the Active Directory
- “What’s It Going to Look Like?”  
Design, Configuration & Deployment
- “Correcting the Sins of the Past”...  
What it Takes to Collapse an NT 4.0 Environment
- “The Sheer Logistics of It All...”  
Re-Architecting the Way Systems are Managed
- “This is Not Your Father’s NT...”  
Implementation Pitfalls

# “Who’s Gonna Build/Own This Thing?”

---

Building Consensus for the Active Directory

# “Who’s Gonna Build/Own This Thing?”

---

Welcome to Layer 8 of the OSI Model...

... the Political Layer.

- Don’t Underestimate Planning Requirements
- Anticipate the Political & Turf-Related Issues
- Cisco’s Departmental & Control Boundaries Blurred...
  - LDAP/Directory Services/White Pages Application Support
  - DNS/Networking Requirements
  - NOS Authentication & Access Control Administration
  - Application & Development Teams
  - Regional & Theater Ownership Issues
- Convergence of Two Internal IT Houses (ECS & IS)

# “What’s It Going to Look Like?”

---

Design, Configuration & Deployment

# “What’s It Going to Look Like?”

---

- Evaluate Requirements Thoroughly
  - Your Environment Will, in Part, Dictate Design
  - Make Sure You Understand the Pros/Cons of AD
- Don’t Overarchitect the Solution
  - Build Only What You Need/Start Simple
  - Leverage Partnerships/Talk to Others
- Run An Extensive Pilot
  - Be Sure to Thoroughly Test the Intended Model
  - DNS/Network Topology Will Play Heavily in the Design
- Phase Your Migration
  - Segment Migration Stages to Reduce Complexity
  - Leverage W2K’s Increased Support for Automation

# “Correcting the Sins of the Past...”

---

What it Takes to Collapse an NT 4.0 Environment



# “Correcting the Sins of the Past...”

---

- Complexities of a Multi-Master Domain Model
  - Moving from LoB Segmentation & Regional Affiliations into a Single Global Forest Model
- Resource Domain Collapse
  - Identifying Owners, Requirements for OUs, etc.
- ACL Cleanup
  - Rooting out Improper ACEs on Resources
- Creating a New Group Model
  - Mapping User-Group-ACL Relationships
- Restructuring Administrative Mechanisms
  - User & Workstation Management
  - Schema & Object Management

# “The Sheer Logistics of It All...”

---

## Re-Architecting the Way Systems are Managed

# “The Sheer Logistics of It All...”

---

- Leveraging the Web for Administration
  - Intranet-Based Services/No MMC
  - Proxied Interfaces for Greater Access Control/Auditing
  - Platform-Independent Management Interfaces
  - Feature-Rich COM Object Models for Administration (ADSI, ADO, WMI, CDO & CDOEXM)
- Health & Well-Being of AD
  - Highly Restricted Access to Administrative Functions
  - Leverage Terminal Services for Administrative “Nodes”
  - Procedures for Schema Injection, Database-Managed
  - Use of a Schema Review Board
  - Use of DEV & STAGE mirror environments for Testing
  - Replication Monitoring is \*Essential\*

# “This is Not Your Father’s NT...”

---

## Implementation Pitfalls

# “This is Not Your Father’s NT...”

---

- This is NOT an Upgrade...
- Don’t Underestimate the Political Elements
- Leverage Pilots/Challenge Designs
- Talk to Others/Share AD Experiences
- Don’t Overarchitect Your Solution
- Use a Strong Project Manager/Team
- Clean Up Your NT 4.0 Environments
- If Possible, Build Development Forests for Testing
- DNS a Critical Element to a Successful Deployment
- Protect the Schema!